

bullx S6000

Console matérielle

Guide utilisateur

extreme computing



REFERENCE
86 F1 50FD 06

bullx S6000 Console matérielle

Guide utilisateur

Matériel

Septembre 2011

Bull Cedoc
357 avenue Patton
BP 20845
49008 Angers Cedex 01
FRANCE

REFERENCE
86 F1 50FD 06
V11.07.13

L'avis juridique de copyright ci-après place le présent document sous la protection des lois de Copyright qui prohibent, sans s'y limiter, des actions comme la copie, la distribution, la modification et la création de produits dérivés.

Copyright ©Bull SAS 2011

Imprimé en France

Marques déposées

Toutes les marques citées dans ce manuel sont la propriété de leurs détenteurs respectifs.

Tous les noms de marques ainsi que les noms de produits matériels et/ou logiciels sont régis par le droit des marques et/ou des brevets.

La citation des noms de marques et de produits est purement informative et ne constitue pas une violation du droit des marques et/ou des brevets.

Des corrections ou des modifications au contenu de ce document peuvent intervenir sans préavis. Bull SAS ne pourra pas être tenu pour responsable des éventuelles erreurs qui pourraient y être contenues dans ce manuel, ni pour tout dommage pouvant résulter de son application.

Table des matières

Information juridique	vii
Déclarations de conformité	vii
Déclaration du fabricant ou de l'importateur	vii
Avis de conformité aux normes de sécurité	vii
Directives de la CEE	vii
Avis de conformité de la FCC	viii
Déclaration de conformité pour le Canada	viii
Déclaration du VCCI	viii
Avis de conformité laser (si applicable)	ix
Informations de sécurité	x
Définition des consignes de sécurité	x
Sécurité électrique	x
Informations sur la sécurité des rayons laser (si applicable)	xi
Intégrité et vérification des données	xi
Maîtrise des déchets	xi
Recommandations de sécurité	xii
Préface	xv
Public visé	xv
Conventions typographiques	xv
Bibliographie	xvi
Chapitre 1. Présentation du serveur	1-1
1.1. Vue d'ensemble	1-2
1.2. Composants, contrôles, voyants et ports	1-4
1.2.1. serveur bullx S6030	1-4
1.2.2. serveur bullx S6010	1-8
Chapitre 2. Mise en route	2-1
2.1. Démarrage de la console matérielle	2-2
2.2. Présentation de la console matérielle	2-4
2.3. Arrêt de la console matérielle	2-8
2.4. Configuration initiale	2-8
2.5. Installation de l'utilitaire KiraTool	2-9
Chapitre 3. Gestion de l'alimentation	3-1
3.1. Présentation des fonctionnalités de gestion de l'alimentation	3-2
3.2. Vérification de l'état d'alimentation	3-4
3.3. Démarrage du serveur depuis la console	3-6
3.4. Arrêt du serveur depuis la console	3-8
3.5. Arrêt forcé / Réinitialisation du serveur	3-10

Chapitre 4.	Utilisation de la console système distante	4-1
4.1.	Configuration de la console système distante	4-2
4.1.1.	Configuration des paramètres spécifiques utilisateur	4-2
4.1.2.	Configuration du clavier et de la souris	4-6
4.1.3.	Partage des lecteurs locaux	4-8
4.2.	Lancement de la console système distante	4-10
4.2.1.	Présentation de la console système distante	4-11
4.2.2.	Menus de la console système distante	4-12
4.2.3.	Barre d'outils de la console système distante	4-14
4.3.	Virtualisation de médias	4-15
4.3.1.	Virtualisation d'un lecteur local	4-15
4.3.2.	Virtualisation d'un fichier image	4-17
4.3.3.	Virtualisation d'un dossier local	4-19
4.4.	Arrêt de la console système distante	4-20
Chapitre 5.	Surveillance du serveur	5-1
5.1.	Configuration initiale de la messagerie et des alertes	5-2
5.2.	Vérification des capteurs de surveillance	5-2
5.3.	Vérification et effacement du journal SEL	5-4
5.4.	Vérification du journal des messages Board & Security	5-6
5.5.	Téléchargement et suppression du journal BIOS	5-7

Chapitre 6.	Configuration du contrôleur de gestion intégré du serveur	6-1
6.1.	Configuration des paramètres d'identification de la plateforme	6-2
6.2.	Configuration du nom du serveur géré	6-3
6.3.	Modification des paramètres du profil fonctionnel	6-4
6.4.	Configuration des paramètres réseau pour l'accès à distance	6-6
6.5.	Modification des paramètres de l'horloge interne	6-10
6.6.	Configuration du journal des messages Board & Security	6-12
6.7.	Gestion des utilisateurs	6-14
6.7.1.	Création d'un compte utilisateur	6-14
6.7.2.	Affichage des détails des comptes utilisateurs	6-17
6.7.3.	Modification d'un compte utilisateur	6-18
6.7.3.1.	Mise à jour des détails	6-18
6.7.3.2.	Changement de groupe	6-20
6.7.4.	Désactivation/Activation des comptes utilisateurs	6-20
6.7.5.	Forçage du changement du mot de passe utilisateur	6-21
6.7.6.	Suppression d'un compte utilisateur	6-22
6.7.7.	Déverrouillage manuel d'un compte utilisateur	6-23
6.7.8.	Modification du mot de passe	6-26
6.7.9.	Création d'un groupe	6-27
6.7.10.	Configuration des permissions	6-28
6.7.11.	Visualisation des membres d'un groupe	6-34
6.7.12.	Suppression d'un groupe	6-35
6.8.	Configuration des paramètres de sécurité	6-37
6.8.1.	Forçage des connexions HTTPS	6-37
6.8.2.	Obtention et installation d'un nouveau Certificat SSL	6-40
6.8.3.	Configuration de la politique de connexion	6-41
6.8.4.	Gestion de l'authentification	6-43
6.8.5.	Activation/désactivation du bouton de mise sous tension du LCP	6-47
6.8.6.	Configuration du verrouillage d'un compte d'utilisateur	6-48
6.9.	Configuration des alertes	6-50
6.9.1.	Configuration des serveurs SNMP et SMTP	6-51
6.9.2.	Configuration des destinations LAN	6-52
6.9.3.	Configuration des politiques d'alertes	6-55
6.9.4.	Gestion des filtres d'événements prédéfinis	6-58
6.9.5.	Customisation d'un filtre d'événement	6-60
Chapitre 7.	Utilisation des fonctionnalités de maintenance	7-1
7.1.	Informations sur le contrôleur de gestion	7-2
7.2.	Récupération des informations sur les FRU	7-3
7.3.	Affichage des versions des firmwares	7-4
7.4.	Mise à jour du firmware	7-5
7.5.	Opérations de réinitialisation	7-6
7.6.	Activation/désactivation du voyant d'identification	7-8
7.7.	Exclusion/inclusion des processeurs	7-9
7.8.	Inclusion/Exclusion d'un module du serveur	7-11
7.9.	Affichage des utilisateurs connectés	7-12
7.10.	Sauvegarde des données de configuration	7-13
7.11.	Restauration des données de configuration	7-14

Annexe A.	Dépannage du serveur	A-1
A.1.	Description des filtres d'alertes prédéfinis	A-2
A.2.	Messages du System Event Log (SEL)	A-9
A.2.1.	Messages SEL : External Environment	A-10
A.2.2.	Messages SEL : Power system board	A-11
A.2.3.	Messages SEL : Sub-chassis	A-11
A.2.4.	Messages SEL : Power Supply	A-12
A.2.5.	Messages SEL : Power Unit	A-13
A.2.6.	Messages SEL : ILB	A-15
A.2.7.	Messages SEL : MTB/MXB	A-27
A.2.8.	Messages SEL : Processor	A-30
A.2.9.	Messages SEL : Fan device / Cooling unit	A-41
A.2.10.	Messages SEL : PDB	A-43
A.2.11.	Messages SEL : Ultra Capacitor	A-44
A.2.12.	Messages SEL : LCP (Panneau de contrôle local)	A-53
A.2.13.	Messages SEL : BMC	A-54
A.2.14.	Messages SEL : Memory	A-62
A.2.15.	Etapes de démarrage : BMC	A-62
A.2.16.	Etapes de démarrage : SMC	A-65
Annexe B.	Console Serial-Over-LAN	B-1
B.1.	Présentation de la console SOL	B-2
B.2.	Utilisation de la console SOL avec ipmitool	B-3
B.3.	Utilisation de la console SOL avec telnet	B-5
Glossaire		g-1

Liste des figures

Figure 1-1.	serveur bullx S6010	1-2
Figure 1-2.	serveur bullx S6030	1-2
Figure 1-3.	Série bullx S6000	1-3
Figure 1-4.	Composants du serveur - Vue éclatée	1-5
Figure 1-5.	Boutons et voyants du serveur - Vue avant	1-5
Figure 1-6.	Boutons et voyants du serveur - Vue arrière	1-6
Figure 1-7.	Ports de connexion du serveur - Vue arrière	1-7
Figure 1-8.	Composants du serveur - Vue éclatée	1-8
Figure 1-9.	Boutons et voyants du serveur - Vue avant	1-9
Figure 1-10.	Boutons et voyants du serveur - Vue arrière	1-10
Figure 1-11.	Ports de connexion du serveur mono-module - Vue arrière	1-11
Figure 2-1.	Logon (Connexion)	2-2
Figure 2-2.	Présentation de la console matérielle	2-4
Figure 2-3.	Commandes et options de l'utilitaire KiraTool - Windows	2-9
Figure 2-4.	Commandes et options de KiraTool - Linux	2-10
Figure 3-1.	Présentation des fonctionnalités de gestion de l'alimentation	3-3
Figure 3-2.	Vérification de l'état d'alimentation	3-4
Figure 3-3.	Démarrage du serveur depuis la console	3-7
Figure 3-4.	Arrêt du serveur depuis la console	3-9
Figure 3-5.	Arrêt d'urgence	3-12
Figure 4-1.	Console système distante - Paramètres spécifiques utilisateur	4-5
Figure 4-2.	Console système distante - Paramètres clavier et souris	4-7
Figure 4-3.	Drive Redirection (Redirection du lecteur)	4-9
Figure 4-4.	Prévisualisation de la console système distante	4-10
Figure 4-5.	Présentation de la Console système distante	4-12
Figure 4-6.	Console système distante menus	4-13
Figure 4-7.	Console système distante Barre d'outils	4-14
Figure 4-8.	Media virtuel – Disque local	4-16
Figure 4-9.	Media virtuel – Fichier image	4-18
Figure 4-10.	Media virtuel – Dossier local	4-20
Figure 5-1.	Sensor Status (État des capteurs)	5-3
Figure 5-2.	Journal SEL	5-5
Figure 5-3.	Messages Board & Security	5-6
Figure 5-4.	Journaux du BIOS	5-7
Figure 6-1.	Platform Settings (Paramètres plateforme)	6-2
Figure 6-2.	Managed Server Settings (Paramètres du serveur géré)	6-3
Figure 6-3.	Paramètres des profils fonctionnels	6-5
Figure 6-4.	Paramètres réseau - valeurs d'usine	6-9
Figure 6-5.	Paramètres Date/Heure - valeurs d'usine	6-11
Figure 6-6.	Paramètres de gestion d'événements - valeurs d'usine	6-13
Figure 6-7.	Gestion des utilisateurs – Création d'un utilisateur	6-16
Figure 6-8.	Gestion des utilisateurs - Détails du compte	6-18

Figure 6-9.	User Account Deletion (Suppression d'un compte utilisateur)	6-23
Figure 6-10.	Gestion des utilisateurs - Utilisateur verrouillé	6-24
Figure 6-11.	Password Management (Gestion des mots de passe)	6-26
Figure 6-12.	Gestion des groupes - Création d'un groupe	6-28
Figure 6-13.	Permissions du groupe	6-30
Figure 6-14.	Group Management (Gestion des groupes)	6-34
Figure 6-15.	Gestion des groupes - Suppression d'un groupe	6-35
Figure 6-16.	Gestion du chiffrement - valeurs d'usine	6-39
Figure 6-17.	SSL Certificate Management (Gestion du certificat SSL)	6-41
Figure 6-18.	Gestion de la politique de connexion utilisateur - valeurs d'usine	6-42
Figure 6-19.	Paramètres d'authentification - valeurs d'usine	6-46
Figure 6-20.	Power Button Lockout Management (Gestion du verrouillage du bouton de mise sous tension) . 6-48	
Figure 6-21.	Gestion du verrouillage des utilisateurs - valeurs d'usine	6-49
Figure 6-22.	Paramètres globaux des alertes	6-52
Figure 6-23.	LAN Destination Settings (Paramètres de destination LAN)	6-53
Figure 6-24.	Configuration des alertes : édition de la Destination LAN	6-54
Figure 6-25.	Paramètres des politiques d'alerte	6-55
Figure 6-26.	Paramètres des politiques d'alerte - Modification	6-57
Figure 6-27.	Gestion des filtres prédéfinis	6-58
Figure 6-28.	Modification des filtres prédéfinis	6-60
Figure 6-29.	Personnalisation d'un filtre d'événement	6-61
Figure 6-30.	Filtres configurables - Modification	6-63
Figure 7-1.	Management Controller Information (Informations sur le contrôleur de gestion)	7-2
Figure 7-2.	FRU Information (Informations sur les FRU)	7-3
Figure 7-3.	Affichage des informations sur le firmware - Exemple d'un serveur	7-4
Figure 7-4.	Reset Operations (Opérations de réinitialisation)	7-7
Figure 7-5.	Identification LED Management (Gestion des voyants d'identification)	7-8
Figure 7-6.	Exclusions de matériel	7-9
Figure 7-7.	Exclusion/inclusion des modules	7-11
Figure 7-8.	Connected Users Information (Informations sur les utilisateurs connectés)	7-12
Figure B-1.	Console SOL - Lancement avec ipmitool	B-3
Figure B-2.	Console SOL - Fermeture avec ipmitool	B-4
Figure B-3.	Session telnet	B-5
Figure B-4.	Commandes telnet	B-6
Figure B-5.	Console SOL - Lancement avec telnet	B-6
Figure B-6.	Console SOL - Fermeture avec telnet	B-7

Liste des tableaux

Table 1-1.	Données produit du serveur	1-3
Table 2-1.	Interface features and permissions (Fonctionnalités de l'interface et permissions)	2-8
Table 3-1.	Informations sur l'alimentation - Causes potentielles du dernier redémarrage	3-5
Table 6-1.	console matérielle : Permissions non configurables	6-30
Table 6-2.	console matérielle : Permissions configurables	6-33
Table 6-3.	IPMI : Privilèges hors bande	6-33
Table A-1.	Filtres d'événements prédéfinis	A-8

Information juridique

Déclarations de conformité

Déclaration du fabricant ou de l'importateur

Nous certifions par la présente que ce produit est conforme à la directive :

- 2004/108/CEE de l'Union européenne relative à la compatibilité électromagnétique, en respectant les normes EN55022 (Classe A) et EN55024, ainsi qu'à la directive 2006/95/EEC relative à la basse tension, en respectant la norme EN60950
- Directive internationale IEC 60297 et directive US ANSI EIA-310-E

Avis de conformité aux normes de sécurité

- UL 60950 (États-Unis d'Amérique)
- IEC 60950 (Internationale)
- CSA 60950 (Canada)

Directives de la CEE

Ce produit est conforme aux directives du conseil des Communautés Européennes (CE) :

Compatibilité électromagnétique

- 2004/108/CE

Basse tension

- 2006/95/CE

Conformité CE

- 93/68/EEC

Équipement terminal de télécommunications

- 1999/5/EC

Ni le fournisseur ni le fabricant ne peuvent être tenus responsables du non-respect des directives de protection résultant d'une modification non autorisée du produit.

La conformité à ces directives requiert :

- Une déclaration de conformité CE fournie par le fabricant
- Une étiquette CE sur le produit
- Une documentation technique

Structures mécaniques

- IEC 60297
- EIA-310-E

Avis de conformité de la FCC

Cet équipement est conforme à l'article 15 de la réglementation FCC. Son utilisation est soumise aux deux conditions suivantes : (1) L'appareil ne doit pas provoquer d'interférences et (2) doit supporter les interférences reçues, notamment les interférences qui peuvent perturber le fonctionnement.

Déclaration FCC

Cet équipement a été testé et déclaré compatible avec les limites des appareils numériques de la classe A, conformément à l'article 15 de la réglementation FCC. Ces limites visent à fournir une protection raisonnable contre les interférences lorsque le produit est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre des ondes radioélectriques qui peuvent perturber les communications radio s'il n'est pas utilisé et installé conformément aux instructions du manuel. L'équipement utilisé dans une zone résidentielle peut créer des interférences que l'utilisateur doit supprimer à ses propres frais.

Des câbles et des connecteurs blindés et correctement mis à la terre doivent être utilisés conformément à la législation relative aux limites d'émission FCC. En aucun cas le fournisseur ou le fabricant ne peut être tenu responsable de l'émission d'interférences radioélectriques provoquées par l'utilisation de câbles et de connecteurs inappropriés ou résultant de la modification de l'équipement. Toute modification non expressément approuvée par le titulaire de cet appareil peut entraîner l'interdiction d'utiliser l'équipement.

Conformément à l'article 15.21 de la réglementation FCC, tout changement ou modification à cet équipement non expressément approuvé par le fabricant peut entraîner des interférences nuisibles et annuler l'autorisation FCC d'utiliser cet équipement. Une étiquette réglementaire FCC est apposée sur l'équipement.

Déclaration de conformité pour le Canada

Cet appareil appartient à la classe A des appareils numériques, il est conforme à la réglementation canadienne sur les équipements pouvant causer des interférences.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Ce produit est conforme aux normes de protection suivantes :

- ICES-003
- NMB-003

Déclaration du VCCI

Cet équipement est conforme aux conditions du VCCI V-3/ 2008-4.

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI- A

C'est un produit de classe A basé sur le standard du Voluntary Control Council for Interference by Information Technology Equipment (VCCI). Si cet équipement est utilisé dans un environnement domestique, des perturbations radioélectriques peuvent survenir. Si de tels troubles apparaissent, il peut être demandé à l'utilisateur de prendre des actions correctives. Une étiquette réglementaire VCCI est apposée sur l'équipement.

Avis de conformité laser (si applicable)

Ce produit utilisant la technologie laser est conforme aux prescriptions des dispositifs laser de classe 1.

Une étiquette PRODUIT LASER DE CLASSE 1 figure sur le dispositif laser.

Class 1 Laser Product Luokan 1 Laserlaite Klasse 1 Laser Apparat Laser Klasse 1
--

Informations de sécurité

Définition des consignes de sécurité



DANGER

La mention *Danger* indique l'existence d'un risque potentiel de blessure grave ou mortelle.



ATTENTION

La mention *Attention* indique l'existence d'un risque potentiel de blessure modérée ou de faible gravité.



AVERTISSEMENT

La mention *Avertissement* indique l'existence d'un risque potentiel d'endommagement d'un programme, d'une unité, du système ou de données.

Sécurité électrique

Les consignes de sécurité suivantes doivent être observées lors de chaque connexion ou déconnexion de périphériques au système.



DANGER

Le client doit s'assurer que l'alimentation électrique du secteur est compatible avec les recommandations, la réglementation, les normes et les pratiques nationales et locales. Un mauvais câblage de la prise de courant peut provoquer une mise sous tension dangereuse des parties métalliques du système ou des unités qui lui sont raccordées. Il est impératif de débrancher les câbles des prises électriques avant tout déplacement du système.



ATTENTION

Ce système est équipé de plusieurs câbles d'alimentation. Suivez les procédures de coupure de l'alimentation à chaque fois que cela vous est demandé.

Informations sur la sécurité des rayons laser (si applicable)

Le lecteur optique présent dans l'unité centrale est classé en tant que produit laser de classe 1. Il porte une étiquette indiquant la classe des produits laser à laquelle il appartient.

Le lecteur optique est conforme au code américain "Department of Health and Human Services 21 Code of Federal Regulations (DHHS 21 CFR) Subchapter J" des produits laser de la classe 1. Par ailleurs, le lecteur est certifié conforme aux normes de l'IEC (International Electrotechnical Commission) 60825-1 : 2001 et CENELEC EN 60825-1 : 1994 pour les produits laser de Classe 1.



ATTENTION

Rayons laser invisibles en position ouverte. Evitez de fixer du regard le rayon laser ou de le regarder directement avec des instruments optiques.

Les produits laser de la classe 1 sont des appareils considérés comme non dangereux. Le lecteur optique contient un laser à l'arséniure de gallium de classe 3B d'une valeur nominale de 30 milliwatts à 830 nanomètres. Le lecteur contient des boîtiers, des composants électroniques et des dispositifs de verrouillage qui évitent toute exposition au rayon laser supérieure au niveau de rayonnement laser de classe 1 durant son fonctionnement et sa maintenance par l'utilisateur ou par le personnel spécialisé.

Intégrité et vérification des données



AVERTISSEMENT

Les produits sont conçus de manière à réduire le risque d'altérations ou de pertes de données non détectées. Cependant, en cas de coupure de courant non prévue ou de panne système, les utilisateurs sont vivement invités à vérifier la validité des opérations effectuées et des données enregistrées ou transmises par le système au moment de la coupure de courant ou de la panne.

Maitrise des déchets

Ce produit est conforme à la directive européenne LUSD (RoHS) 2002/95/CE concernant la limitation de certaines substances toxiques dans les Equipements Electriques et Electroniques.

Ce produit est conforme à la directive européenne (DEEE (WEEE) 2002/96/EC concernant la gestion des Equipements Electriques et Electroniques et de leurs déchets.

Recommandations de sécurité

Mentions Danger et Avertissement



DANGER

Seuls les composants enfichables à chaud peuvent être maintenus (ajoutés, retirés, remplacés) sans arrêter l'équipement.

Si le composant n'est pas remplaçable à chaud, l'équipement doit être arrêté **AVANT** d'effectuer l'opération de maintenance et les câbles d'alimentation doivent être déconnectés de la prise électrique.



DANGER

La non-déconnexion des câbles d'alimentation des prises électriques avant une intervention peut entraîner des blessures et endommager l'équipement.

Il est impératif de débrancher les câbles des prises électriques avant tout déplacement des armoires et des systèmes.



DANGER

Des conditions électriques dangereuses sont présents dans le bloc d'alimentation. Des conditions électriques dangereuses peuvent être présentes sur l'alimentation, le téléphone, et les câbles de communication.

Energie dangereuse :

Retirez tous vos bijoux avant d'intervenir.



DANGER

Le supercondensateur peut conserver une charge après le retrait de l'alimentation. Cette charge peut provoquer des blessures et endommager l'équipement.

Il est impératif de ne toucher aucune partie tant que le supercondensateur n'a pas été complètement déchargé.

Du fluide électrolyte peut s'échapper d'un supercondensateur en panne.

Il est impératif de porter des gants et des lunettes de protection pour éviter des contacts avec la peau et les yeux quand vous manipulez le supercondensateur.



DANGER

La pile interne devrait être remplacée régulièrement. Elle doit être remplacée par un modèle identique ou un modèle équivalent recommandé par le constructeur. Il y a danger d'explosion si un autre modèle est utilisé. Disposez des piles usagées selon les instructions du constructeur.



DANGER

Des précautions élémentaires de sécurité électrique doivent être suivies pour vous protéger du danger et protéger le tiroir des dommages.

Si un accident électrique se produit, coupez le courant en débranchant le cordon d'alimentation du serveur.



AVERTISSEMENT

Le refroidissement et la circulation d'air sont optimaux lorsque les armoires et les systèmes sont fermés.

Une fois l'opération de maintenance terminée, les armoires et les systèmes devront être refermés rapidement.

Avis importants



Important

ETIQUETAGE

Utilisez des étiquettes pour noter l'orientation et la position des câbles, des composants, des protections ou des connecteurs retirés.



Important

MANIPULATION DE COMPOSANTS SENSIBLES A L'ELECTRICITE STATIQUE

Les précautions suivantes doivent être prises lors de la manipulation de composants sensibles à l'électricité statique :

- Portez systématiquement un bracelet antistatique lorsque vous manipulez des composants.
 - Touchez la structure de l'armoire pour décharger l'électricité statique avant de manipuler les cartes.
 - Tenez les cartes et les périphériques par les extrémités.
 - Ne retirez le composant de son emballage anti-statique que lorsque vous êtes prêt à l'installer.
 - Si vous devez poser le composant lorsqu'il est hors de son emballage anti-statique, posez-le sur la mousse conductrice.
-

Préface

Ce guide explique comment utiliser la console matérielle destinée à gérer le serveur.

Note Le site Web du Support Bull peut être consulté pour des informations concernant les produits et les offres de service, ainsi que pour télécharger la documentation et les mises à jour :

<http://support.bull.com>

Public visé

Ce guide est destiné aux administrateurs et aux opérateurs de Système Bull.

Conventions typographiques

Les conventions typographiques suivantes sont utilisées dans ce guide :

Gras	Identifie : <ul style="list-style-type: none">• Les objets de l'interface tels que les noms de menus, les étiquettes, les boutons et les icônes.• Les noms de fichiers, de répertoires et les chemins.• Les mots clés qui nécessitent une attention particulière.
<i>Italique</i>	Identifie les références telles que les manuels ou les URL.
monospace	Identifie les parties de code des programmes, des lignes de commande, ou des messages affichés dans les fenêtres de commandes.
< >	Identifie les paramètres à saisir par l'utilisateur.
	Identifie la partie AVANT d'un composant.
	Identifie la partie ARRIERE d'un composant.

Bibliographie

Cette liste n'est pas exhaustive. Des documents utiles sont disponibles sur les CDs de ressources et de documentation livrés avec votre système. Il vous est fortement recommandé de vous référer à cette documentation avant de configurer, utiliser, maintenir ou mettre à jour votre système.

- *Site Preparation Guide*, 86A1 40FA
explique comment préparer une salle informatique pour les systèmes Bull, en conformité avec les standards en vigueur. Ce guide est destiné au personnel et aux professionnels impliqués dans la procédure de préparation du site..
- *bullx S6030 Guide d'installation*, 86 F1 26FE
explique comment installer et démarrer le serveur pour la première fois. Ce guide est destiné au personnel de maintenance qualifié.
- *bullx S6030 Service Guide*, 86 A7 85FB
explique comment maintenir le serveur. Ce guide est destiné au personnel de maintenance qualifié.
- *bullx S6010 Guide d'installation*, 86 F1 86FB
explique comment installer et démarrer le serveur pour la première fois. Ce guide est destiné au personnel de maintenance qualifié.
- *bullx S6010 Service Guide*, 86 A7 85FB
explique comment maintenir le serveur. Ce guide est destiné au personnel de maintenance qualifié.
- *bullx Cabling Guide*, 86 A1 94FE
explique comment câbler une configuration bullx multi-modules Ce guide est destiné aux administrateurs de serveurs, aux opérateurs et au personnel de maintenance.
- *iCare Console User's Guide*, 86 A1 71FA
explique comment utiliser la console destinée à gérer et maintenir les systèmes Bull. Ce guide est destiné aux administrateurs de systèmes Bull, aux opérateurs et au personnel de maintenance qualifié.
- *CD-ROM Resource and Documentation*
contient les outils et la documentation nécessaires à la configuration, à l'utilisation et à la maintenance de l'équipement.

Chapitre 1. Présentation du serveur

Ce chapitre présente les fonctionnalités et les composants du serveur. Il comprend les rubriques suivantes :

- Vue d'ensemble, page 1-2
- Composants, contrôles, voyants et ports , page 1-4

1.1. Vue d'ensemble

Les serveurs Bull destinés aux applications d'affaires et scientifiques sont fondés sur l'architecture MESCA (Multiple Environments on a SCalable Architecture), tirant parti de la dernière génération de processeurs Intel Xeon, du protocole QPI d'Intel, de la technologie Bull BCS et l'interconnexion Infiniband QDR. Les serveurs sont conçus pour atteindre une performance à l'échelle du petaflop tout en optimisant la consommation en énergie et la dissipation de chaleur. Deux types de systèmes sont disponibles suivant vos besoins :

serveur bullx S6010

Le serveur bullx S6010, noeud de calcul à haute densité, offre jusqu'à 4 processeurs, 32 mémoires DIMMs et 1 lecteur de disques internes par tiroir de 1,5U. Sa conception unique en "L" permet l'assemblage de 2 modules pour offrir jusqu'à 8 processeurs, 64 mémoires DIMMs et 2 disques internes par emplacement de 3U.

Jusqu'à 4 serveurs bullx S6010 peuvent être interconnectés via le BCS (Bull Coherence Switch) pour obtenir un serveur SMP de 6U offrant jusqu'à 16 processeurs et 128 mémoires DIMMs dans un assemblage 6U.

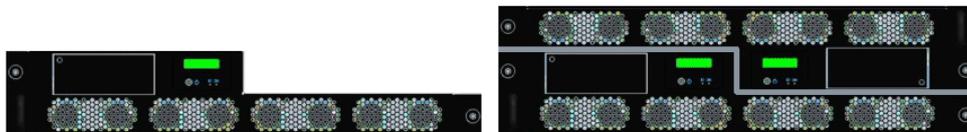


Figure 1-1. serveur bullx S6010

serveur bullx S6030

Le noeud de calcul/de service serveur bullx S6030 offre jusqu'à 4 processeurs, 32 mémoires DIMMs, 6 emplacements PCI-e et 8 lecteurs de disques par tiroir 3U. En option, un lecteur de DVD peut être installé dans un emplacement disque.

Jusqu'à 4 serveurs bullx S6030 peuvent être interconnectés via le BCS (Bull Coherence Switch) pour obtenir un serveur SMP de 12U offrant jusqu'à 16 processeurs, 128 mémoires DIMMs et 24 emplacements PCI-e. L'addition de cartes LSI fournit de 8 à 32 disques internes.



Figure 1-2. serveur bullx S6030

Les serveurs sont montés dans des armoires Bull pour un temps de déploiement et une fiabilité optimaux.



Figure 1-3. Série bullx S6000

Pour référence, il vous est conseillé d'enregistrer les données suivantes, indiquées sur les étiquettes apposées sur le serveur :

Système	Données
Nom du produit	
Code du produit	
Numéro du produit	
Numéro de série du système	

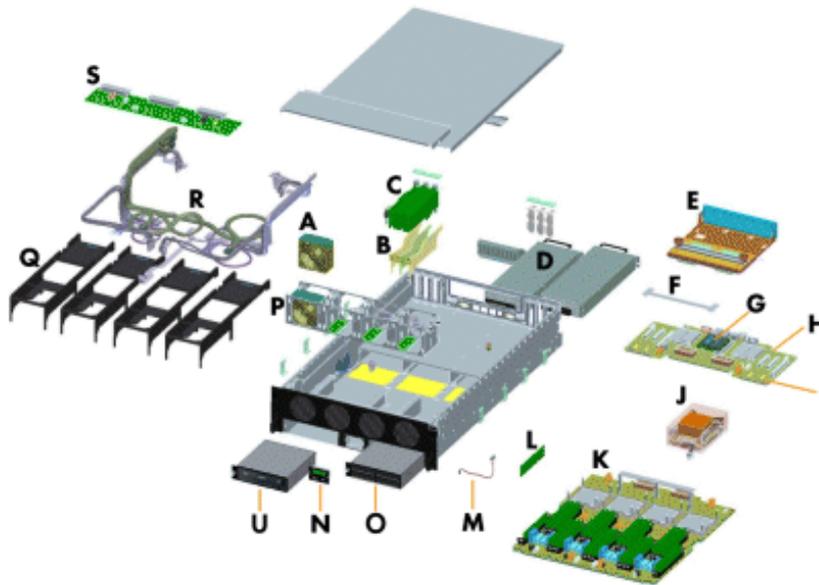
Table 1-1. Données produit du serveur

1.2. Composants, contrôles, voyants et ports

1.2.1. serveur bullx S6030

Composants (Vue éclatée)

Le diagramme suivant montre une vue éclatée des composants du serveur :



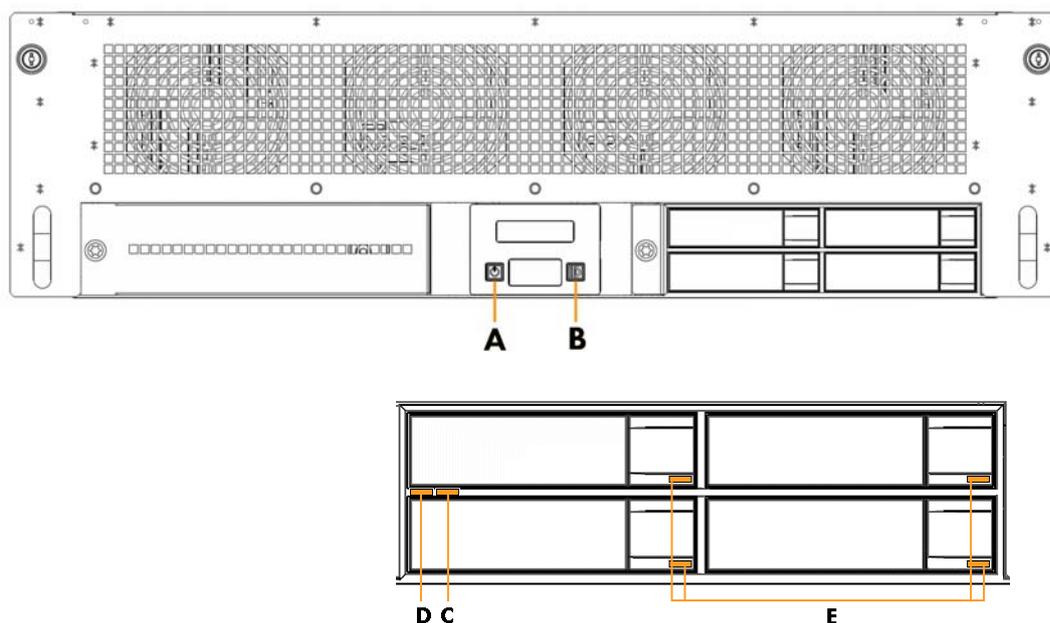
Repère	Description	Quantité
A	Ventilateur	8
B	Séparateur PCIe	2 à 4
C	Carte PCIe	Jusqu'à 6
D	Bloc d'alimentation	1 ou 2
E	Carte DSIB ou Carte SIB	1
F	Prépositionneur	1
G	Contrôleur de gestion intégré	1
H	Carte ILB	1
I	Pile ICH	1
J	Ensemble Processeur Nehalem	Jusqu'à 4
K	Carte MXB	1
L	Barrette mémoire	Jusqu'à 32
M	Switch Anti-Intrusion	1
N	Panneau de contrôle local (LCP)	1
O	Lecteur de disque dur (HDX)	1 ou 2
P	Bloc ventilateur	1
Q	Conduit d'air	4
R	Kit de câbles internes	1
S	Carte PDBU	1

Repère	Description	Quantité
Non illustré	Ultra Capacitor	1
U	Lecteur DVD (Optionnel)	1

Figure 1-4. Composants du serveur - Vue éclatée

Contrôles et voyants (vue avant)

Le serveur est équipé de voyants et de boutons à l'avant et à l'arrière. Le diagramme suivant montre les voyants et les boutons situés à l'avant du serveur.

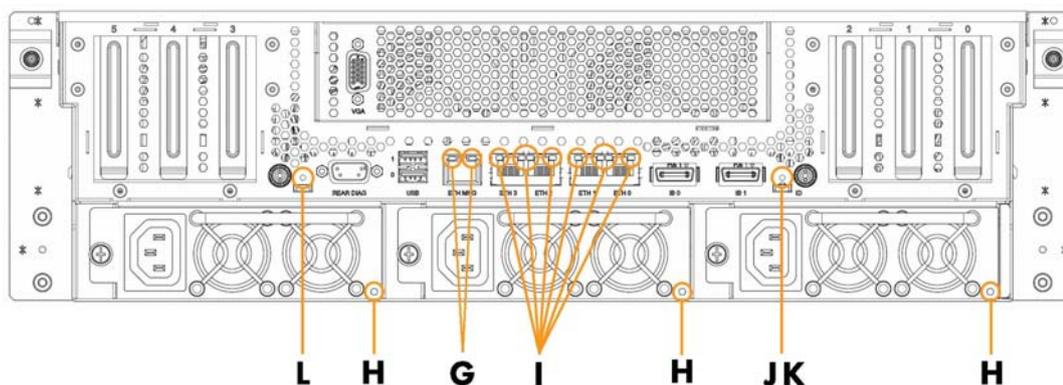


Repère	Voyant/Bouton	Couleur	Description
A	Voyant/Bouton de mise sous tension	Vert clignotant Vert fixe	Serveur en veille. Serveur démarré.
B	Voyant/Bouton d'identification	Bleu clignotant	Le bouton d'identification a été activé localement ou à distance depuis la console matérielle du serveur ; allume simultanément le voyant d'identification Bleu (G) à l'arrière du serveur.
C	Voyant de panne de ventilateur de disque	Orange clignotant	Panne de ventilateur de disque.
D	Voyant de surchauffe de disque	Orange clignotant	Panne de surchauffe de disque.
E	Voyant d'activité du disque	Vert clignotant	Disque actif.

Figure 1-5. Boutons et voyants du serveur - Vue avant

Contrôles et voyants (vue arrière)

Le serveur est équipé de voyants et de boutons à l'avant et à l'arrière. Le diagramme suivant montre les voyants et les boutons situés à l'arrière du serveur.

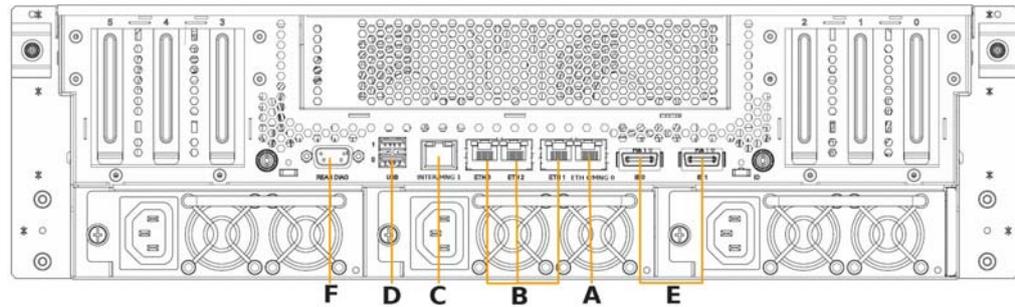


Repère	Voyant/Bouton	Couleur	Description
G	Voyant gauche du port de gestion	Vert fixe Vert clignotant	Lien actif. Lien inactif.
G	Voyant droit du port de gestion	Orange fixe Off (arrêté)	100 MBit/s. 10 MBit/s.
H	Voyant du bloc d'alimentation	Vert fixe Vert clignotant Orange clignotant	Bloc d'alimentation sous tension. Bloc d'alimentation en veille. Bloc d'alimentation en erreur.
I	Voyant gauche du port Gbit	Vert Orange Off (arrêté)	1 GBit/s. 100 MBit/s. 10 MBit/s.
I	Voyant droit du port Gbit	Vert fixe Vert clignotant	Lien établi. Lien actif.
J	Bouton de réinitialisation	N/A	Réinitialise le contrôleur de gestion intégré.
K	Voyant d'identification	Bleu clignotant	Le bouton d'identification (B) situé à l'avant du serveur a été activé localement ou à distance depuis la console matérielle.
L	Bouton de retour aux valeurs par défaut	N/A	Restaure les valeurs par défaut du contrôleur de gestion intégré.

Figure 1-6. Boutons et voyants du serveur - Vue arrière

Ports de connexion (Vue arrière)

Le diagramme suivant montre les ports de connexion situés à l'arrière du serveur.



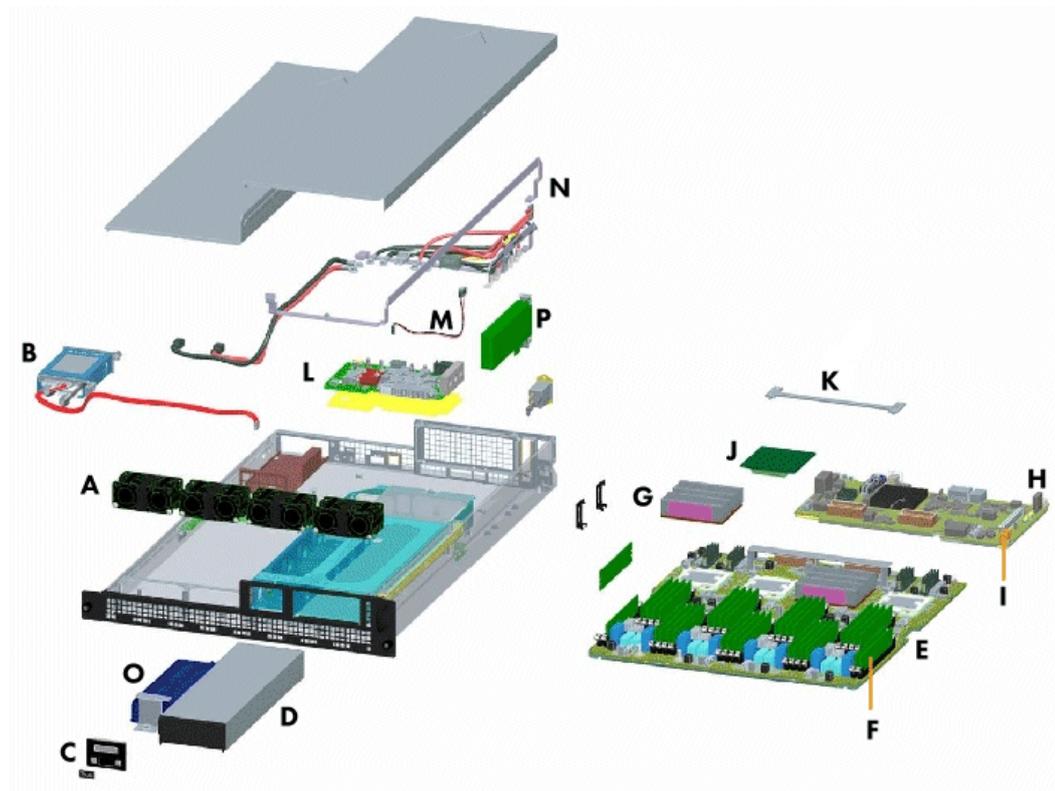
Repère	Description
A	Port ETH0/MNG0 (RJ45) : Shared Management / Host network port (Gestion partagée / port réseau hôte), ou uniquement port réseau hôte si INTER/MNG1 (C) est utilisé pour le réseau de gestion
B	Ports ETH1, ETH2, ETH3 (RJ45) : Port réseau d'entreprise
C	INTER/MNG1 (RJ45) : Port réseau dédié à la gestion ou à l'interconnexion des modules
D	Ports pour clé USB
E	Ports INFINIBAND : Port réseau infiniband (Optionnel)
F	Port VGA

Figure 1-7. Ports de connexion du serveur - Vue arrière

1.2.2. serveur bullx S6010

Composants (Vue éclatée)

Le diagramme suivant montre une vue éclatée des composants du serveur :

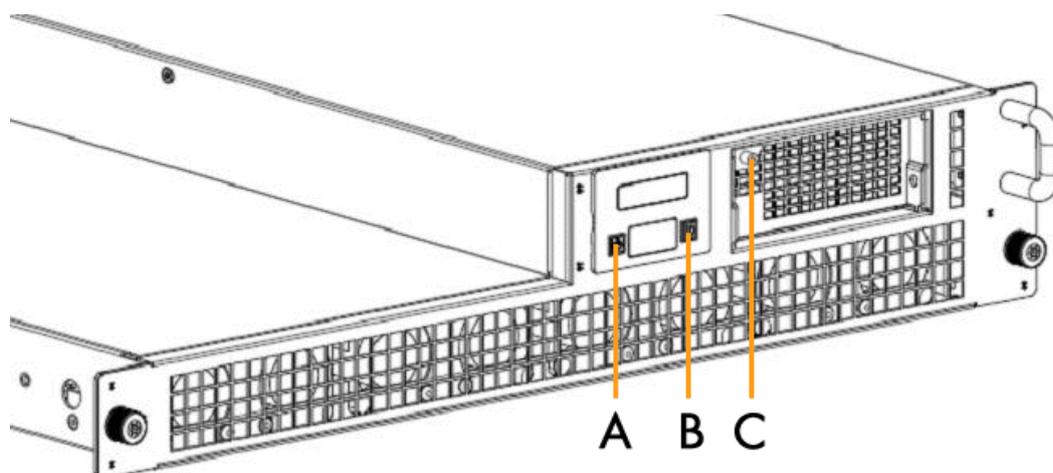


Repère	Description	Quantité
A	Unité de refroidissement	4
B	Lecteur de disque dur (HDD)	1
C	Panneau de contrôle local (LCP)	1
D	Bloc d'alimentation	1
E	Carte MXB	1
F	Barrette mémoire	Jusqu'à 32
G	Processeur Nehalem	Jusqu'à 4
H	I/O Legacy Board (ILBL)	1
I	Pile ICH	1
J	Dummy CSI Interconnect Legacy Board (DSIBL)	1
K	Prépositionneur	1
L	Carte PDBU	1
M	Switch Anti-Intrusion	1
N	Kit de câbles internes	1
O	Ultra Capacitor	1
P	Carte PCIe	1

Figure 1-8. Composants du serveur - Vue éclatée

Contrôles et voyants (vue avant)

Le serveur est équipé de voyants et de boutons à l'avant et à l'arrière. Le diagramme suivant montre les voyants et les boutons situés à l'avant du serveur.

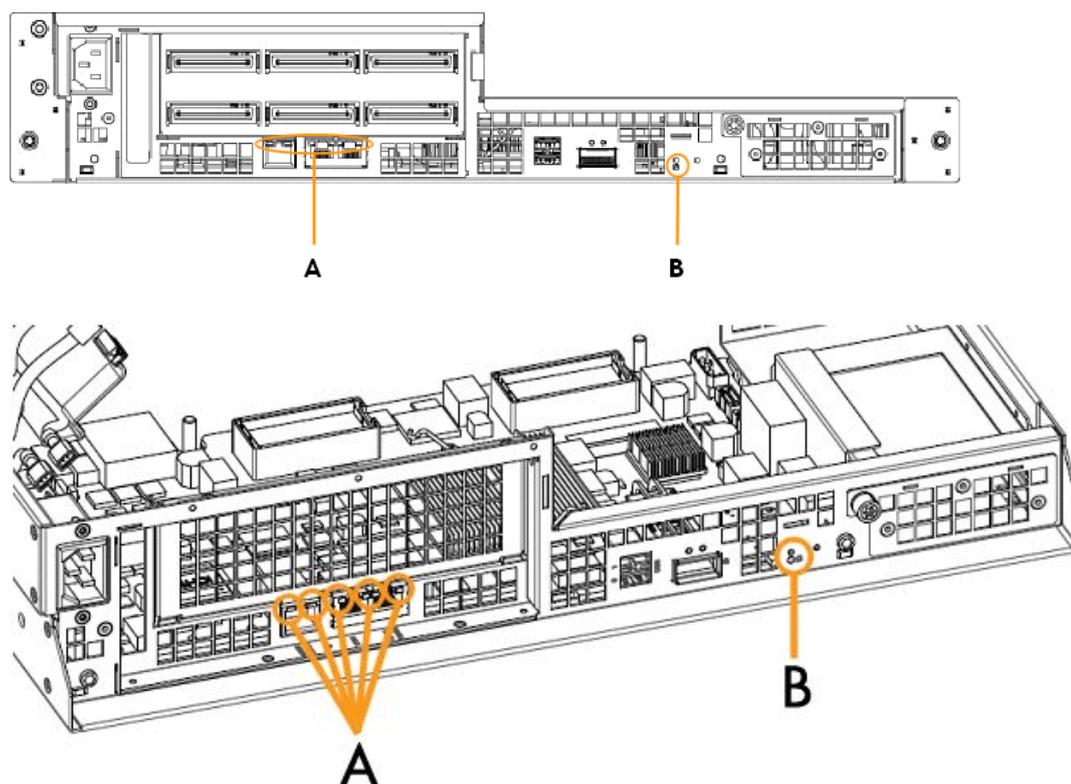


	Repère	Nom	Description
A		Voyant/Bouton de mise sous tension	Vert clignotant : serveur en veille. Vert fixe : serveur démarré.
B		Voyant/Bouton d'identification	Bleu clignotant : Le bouton d'identification appuyé ou activé depuis la console matérielle du serveur. Allume simultanément le voyant d'identification bleu situé à l'arrière du serveur.
C		Voyants du bloc d'alimentation	Vert fixe : bloc d'alimentation mis sous tension. Vert clignotant : bloc d'alimentation en veille. Ambre clignotant : bloc d'alimentation en erreur.

Figure 1-9. Boutons et voyants du serveur - Vue avant

Contrôles et voyants (vue arrière)

Le serveur est équipé de voyants et de boutons à l'avant et à l'arrière. Le diagramme suivant montre les voyants et les boutons situés à l'arrière du serveur.



Repère	Nom	Description
A	Voyants d'activité Ethernet	Indique l'activité réseau. Il y a 1 port de gestion et 2 ports Gbit. Pour le port de gestion : Voyant de gauche : Vert fixe : lien actif. Vert clignotant : lien inactif. Voyant de droite : Orange fixe : vitesse 100Mo/s Éteint : taux 10 Mo/s Pour les ports Gbit : (à la droite de chaque port) Voyant de gauche : Vert : vitesse 1Go/s Orange : 100 Mo/s Éteint : 10 Mo/s Voyant de droite : Vert fixe : lien établi. Vert clignotant : lien actif.
B	Voyant d'identification	Bleu clignotant

Figure 1-10. Boutons et voyants du serveur - Vue arrière

Ports de connexion (vue arrière)

Le diagramme suivant montre les ports de connexion situés à l'arrière du serveur.

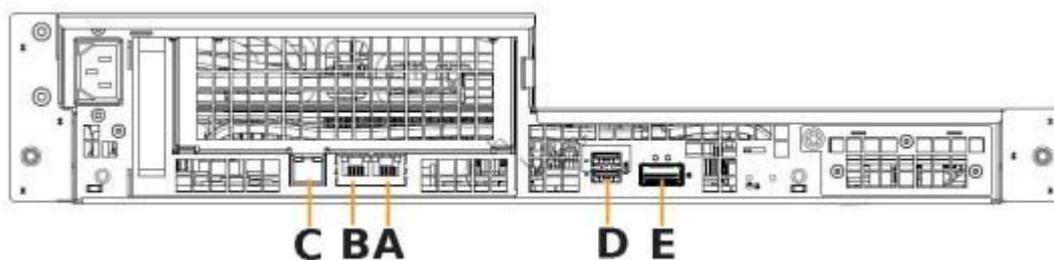


Figure 1-11. Ports de connexion du serveur mono-module - Vue arrière

Repère	Description
A	Port ETH0/MNG0 (RJ45) : Port réseau partagé pour le réseau de gestion et le réseau hôte ou uniquement port réseau hôte si INTER/MNG1 (C) est utilisé pour le réseau de gestion
B	Port ETH1 (RJ45) : Port réseau d'entreprise
C	INTER/MNG1 (RJ45) : Port dédié de gestion du réseau, ou port d'interconnexion de serveur (modèles multi-modules)
D	Ports USB :
E	Port INFINIBAND : Port réseau infiniband

Chapitre 2. Mise en route

Ce chapitre décrit les fonctionnalités de la console matérielle et explique comment démarrer et arrêter la console depuis un navigateur Web. Il comprend les rubriques suivantes :

- Démarrage de la console matérielle, page 2-2
- Présentation de la console matérielle, page 2-4
- Arrêt de la console matérielle, page 2-8
- Configuration initiale, page 2-8
- Installation de l'utilitaire KiraTool, page 2-9

2.1. Démarrage de la console matérielle

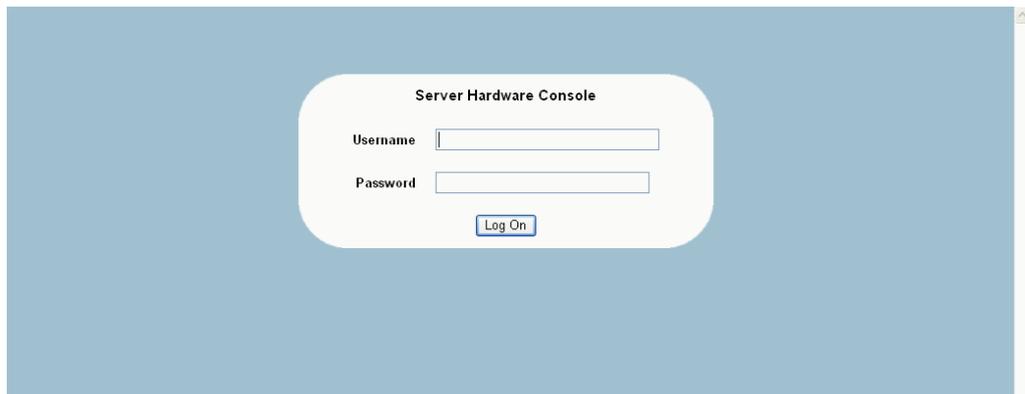
La console matérielle est lancée depuis un navigateur Web en utilisant une adresse IP standard ou sécurisée ou un nom d'hôte, suivant la configuration..

Prérequis

Le serveur est connecté à l'alimentation électrique du site et au réseau local d'entreprise.

Procédure

1. Lancez votre navigateur web et entrez l'adresse IP standard ou sécurisée ou le nom d'hôte, suivant la configuration. La page d'authentification s'ouvre.



console matérielle	
Username (Nom d'utilisateur)	Nom d'usine : super
Password (Mot de passe)	Mot de passe d'usine : pass

Figure 2-1. Logon (Connexion)

2. Complétez les champs Username (Nom d'utilisateur) et Password (Mot de passe) puis cliquez sur Log On (Connexion). Une fois authentifié, l'onglet System Control (Contrôle système) s'ouvre.



Important Il est fortement recommandé de changer le mot de passe d'usine du super utilisateur, une fois la configuration initiale terminée, en prenant soin d'enregistrer les détails de votre nouveau compte pour des connexions futures.
Si vous perdez les détails de votre compte et si vous êtes incapables de vous connecter à la console, contactez votre Ingénieur Support Technique.



Important Plusieurs utilisateurs peuvent accéder à la console simultanément. Si des modifications de configuration sont effectuées, elles peuvent ne pas être visibles aux autres utilisateurs tant qu'ils n'ont pas rafraîchi l'affichage de leur console. Vous pouvez afficher la liste des utilisateurs connectés depuis l'onglet Maintenance en sélectionnant Maintenance Operations > Connected Users (Opérations de maintenance - Utilisateurs connectés).

Que faire en cas d'incident ?

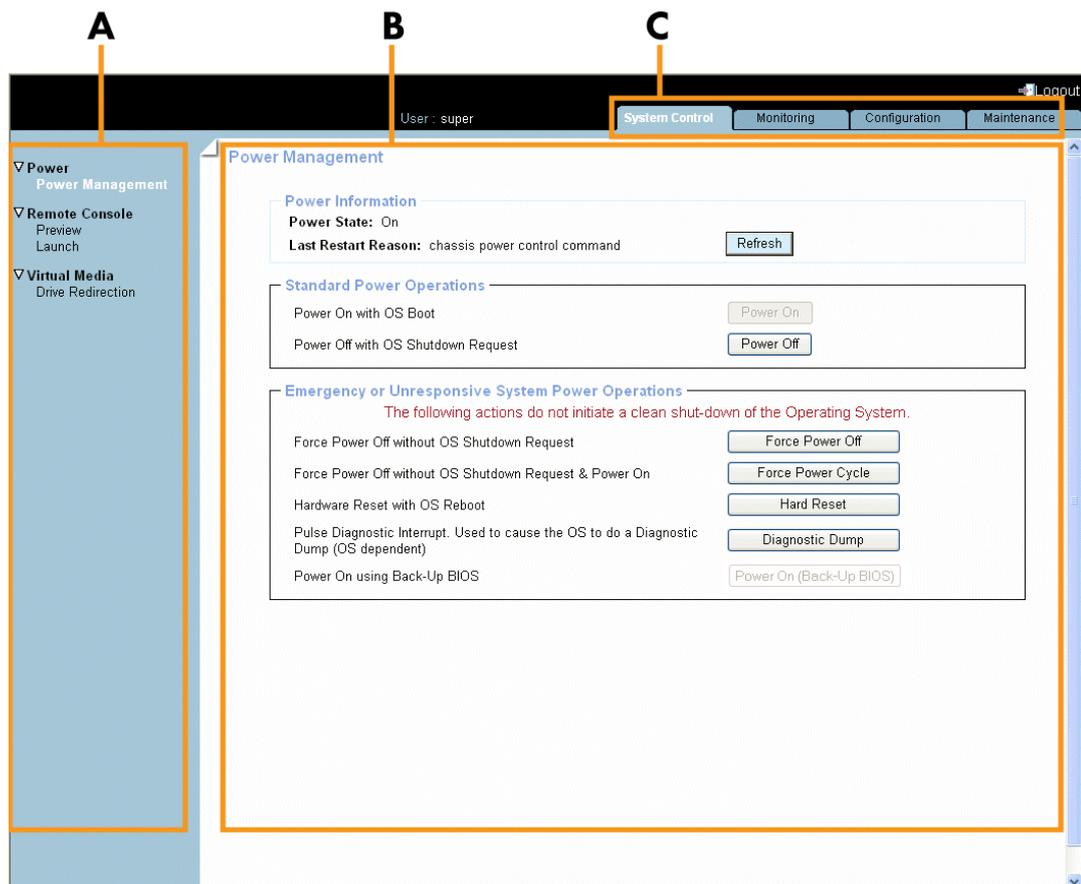
Si vous ne pouvez pas vous connecter à la console ou si les pages web ne s'affichent pas correctement, un des problèmes suivants peut en être la cause :

- Panne de réseau
- Configuration incorrecte du réseau
- Paramètres du navigateur incorrects (configuration proxy)

2.2. Présentation de la console matérielle

La console matérielle est une application d'administration web intégrée au contrôleur de gestion. Vous pouvez utiliser la console matérielle pour piloter, superviser et maintenir le matériel et pour configurer le contrôleur de gestion intégré, à distance. La console matérielle est accessible par le réseau local d'entreprise en utilisant le navigateur Microsoft Internet Explorer ou Mozilla Firefox.

Important Plusieurs utilisateurs peuvent accéder à la console simultanément. Si des modifications de configuration sont effectuées, elles peuvent ne pas être visibles aux autres utilisateurs tant qu'ils n'ont pas rafraîchi l'affichage de leur console. Vous pouvez afficher la liste des utilisateurs connectés depuis l'onglet Maintenance en sélectionnant Maintenance Operations > Connected Users (Opérations de maintenance - Utilisateurs connectés).



Présentation de la console	
A : Arbre de navigation	Fournit l'accès aux fonctions de la console. Notez que les fonctions affichées diffèrent suivant l'onglet sélectionné.
B : Volet de travail	Le volet de travail affiche les commandes et les informations associées aux éléments sélectionnés dans l'arbre de navigation.
C: Onglets	Quatre onglets permettent d'accéder à quatre familles de fonctions accessibles depuis les arbres de navigation associés : System Control (Contrôle système), Monitoring (Supervision), Configuration et Maintenance.

Figure 2-2. Présentation de la console matérielle

Caractéristiques de l'interface de la console

Le tableau suivant liste les fonctionnalités disponibles depuis l'interface et les permissions associées.

Onglet	Noeud de l'arborescence		Caractéristique	Permission
System Control (Contrôle système)	Power Management (Gestion de l'alimentation)	Power (Démarrage)	Power Information (Information sur l'alimentation)	<i>None (Aucune)</i>
		Power (Démarrage)	Standard Power Operations (Opérations standard d'alimentation)	Power Control (Gestion de l'alimentation)
		Power (Démarrage)	Emergency Power Operations (Gestion de l'alimentation en cas d'urgence)	Power Control (Gestion de l'alimentation)
	Remote Console (Console distante)	Preview (Aperçu)	Preview (Aperçu)	Remote Control Access (Accès à distance)
		Launch (Lancement)	-	Remote Control Access (Accès à distance)
	Virtual Media (Media virtuel)	Drive Redirection (Redirection du lecteur)	Drive Redirection (Redirection du lecteur)	Virtual Media Upload (Téléchargement d'un média virtuel)
Monitoring (Surveillance)	System Health (Santé du système)	Sensor Status (État des capteurs)	Viewing and Refreshing (Visualisation et rafraîchissement)	<i>None (Aucune)</i>
		System Event Log (Journal SEL)	Viewing and Refreshing (Visualisation et rafraîchissement)	
			Clearing (Effacement)	Alert Settings & Clear SEL (Configuration d'alertes & effacement du SEL)
		Messages	Viewing and Clearing (Visualisation et effacement)	Log View (Affichage des journaux)
Configuration	Global Settings (Paramètres globaux)	Platform (Plateforme)	Platform Settings (Paramètres plateforme)	Network Settings (Paramètres réseau)
		Managed Server (Serveur géré)	Managed Server Settings (Paramètres du serveur géré)	Network Settings (Paramètres réseau)
		Functional Profiles (Profils fonctionnels)	Functional Profile Settings (Paramètres du profil fonctionnel)	Network Settings (Paramètres réseau)
	BMC Settings (Paramètres BMC)	Network (Réseau)	Network Settings (Paramètres réseau)	Network Settings (Paramètres réseau) SSH/Telnet Access (Accès SSH/Telnet) (nécessaire pour utiliser les options disponibles dans la page Network Settings (Paramètres réseau))
		Date-Time (Date-heure)	Date/Time Settings (Paramètres Date/Heure)	Date/Time Settings (Paramètres Date/Heure)
		Messages	Event Management Settings (Paramètres de gestion des événements)	Log Settings (Paramètres des journaux) Network Settings (Paramètres réseau)

Onglet	Noeud de l'arborescence		Caractéristique	Permission
Configuration	BMC User Management (Gestion des utilisateurs BMC)	Users (Utilisateurs)	User Management (Gestion des utilisateurs)	User/Group Management (Gestion des utilisateurs/groupes)
		Groups (Groupes)	Group Management (Gestion des groupes)	
		Password (Mot de passe)	Password Management (Gestion des mots de passe)	Change Password (Changement du mot de passe)
	Security (Sécurité)	Encryption (Chiffrement)	Encryption Management (Gestion du chiffrement)	Security Settings (Paramètres de sécurité)
		SSL Certificate (Certificat SSL)	SSL Certificate Management (Gestion du certificat SSL)	SSL Certificate Management (Gestion du certificat SSL)
		User Logon Policy (Politique de connexion utilisateur)	User Logon Policy Management (Gestion de la politique de connexion utilisateur)	Security Settings (Paramètres de sécurité)
		Authentication (Authentification)	Authentication Management (Gestion de l'authentification)	Authentication Settings (Paramètres d'authentification)
		Power Button Lockout (Verrouillage du bouton de mise sous tension)	Power Button Lockout Management (Gestion du verrouillage du bouton de mise sous tension)	Security Settings (Paramètres de sécurité)
		User Lockout (Verrouillage utilisateur)	User Lockout Management (Gestion du verrouillage utilisateur)	
		Remote Console Settings (Paramètres de la console distante)	User Specific (Spécifique utilisateur)	User Specific RC Settings (Paramètres RC spécifiques utilisateur) Reset Keyboard/Mouse (USB) (Réinitialisation de clavier/souris (USB)) Reset USB (Réinitialisation de l'USB) Reset Video Engine (Réinitialisation du moteur vidéo)
	Transmission Encoding (Encodage de la transmission)			RC Settings (Encoding) (Paramètres console distante (Encodage))
	Miscellaneous RC Settings (Paramètres RC divers)			RC Settings (Monitor Mode) (Paramètres console distante (Mode moniteur)) RC Settings (Exclusive Access) (Paramètres console distante (Accès exclusif))

Onglet	Noeud de l'arborescence		Caractéristique	Permission	
Configuration	Remote Console Settings (Paramètres de la console distante)	User Specific (Spécifique utilisateur)	Mouse Hotkey (Touche rapide de la souris) Remote Console Button Key (Touche de la console distante)	RC Settings (Hotkeys) (Paramètres RC (Touches rapides))	
		Keyboard/Mouse (Clavier/souris)	Keyboard/Mouse Settings (Paramètres clavier/souris)		RC Keyboard/Mouse Settings (Paramètres clavier/souris de la console distante)
	Alert Settings (Paramètres d'alerte)	Filters (Filtres)	Filter Settings (Paramètres filtres)	Alert Settings & Clear SEL (Configuration d'alertes & effacement du SEL)	
		Policies (Politiques)	Policy Settings (Paramètres Politiques)		
		LAN Destinations (Destinations LAN)	LAN Destination Settings (Paramètres de destination LAN)		
General	General Settings (Paramètres généraux)				
Maintenance	Hardware Information (Information sur le matériel)	Management Controller (Contrôleur de gestion)	Management Controller Information (Information sur le contrôleur de gestion)	None	
		FRU	FRU Information (Informations sur les FRU)		
		Firmware Version (Version du firmware)	Firmware Information (Information sur les firmwares)		
	Firmware Update (Mise à jour du firmware)	Listed firmware (Firmwares listés)	Firmware Update (Mise à jour du firmware)	Firmware Update (Mise à jour du firmware)	
	Maintenance Operations (Opérations de maintenance)	Unit Reset (Réinitialisation de l'unité)		Reset Management Controller (Réinitialisation du contrôleur de gestion)	Maintenance/Board Reset (Réinitialisation Maintenance/Carte)
				Reset Keyboard/Mouse (USB) (Réinitialisation de clavier/souris (USB)) Reset USB (Réinitialisation de l'USB) Reset Video Engine (Réinitialisation du moteur vidéo)	Remote Console Access (Accès console distante)
		Identification LED (Voyant d'identification)	ID LED Management (Gestion des voyants d'identification)	Alert Settings & Clear SEL (Configuration d'alertes & effacement du SEL)	

Onglet	Noeud de l'arborescence		Caractéristique	Permission
Maintenance	Maintenance Operations (Opérations de maintenance)	Hardware Exclusion (Exclusion matérielle)	Hardware Exclusions (Exclusions matérielles)	Maintenance/Board Reset (Réinitialisation Maintenance/Carte)
		Connected Users (Utilisateurs connectés)	Connected Users Information (Informations sur les utilisateurs connectés)	None (Aucune)

Table 2-1. Interface features and permissions (Fonctionnalités de l'interface et permissions)

2.3. Arrêt de la console matérielle

Vous pouvez arrêter la console à tout moment en cliquant sur le lien Logout (Déconnecter) () dans l'angle supérieur droit.

Vous pouvez arrêter la console à n'importe quel moment en cliquant sur le bouton Logout (Déconnecter)

2.4. Configuration initiale

A la livraison du serveur, vous aurez à effectuer certaines tâches de configuration de base pour vérifier son fonctionnement et vous assurer qu'il est bien identifié par le logiciel de gestion. Ces tâches de configuration sont détaillées dans le chapitre 6. Configuration du contrôleur de gestion intégré du serveur et sont listées ci-dessous par ordre de priorité :

- Configuration des paramètres réseau pour l'accès à distance, page 6-6
- Configuration du nom du serveur géré, page 6-3
- Configuration des paramètres d'identification de la plateforme, page 6-2
- Modification des paramètres de l'horloge interne, page 6-10
- Configuration de la console système distante, page 4-2

Note Les autres tâches de configuration peuvent être effectuées, si nécessaire.



Important Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation.

2.5. Installation de l'utilitaire KiraTool

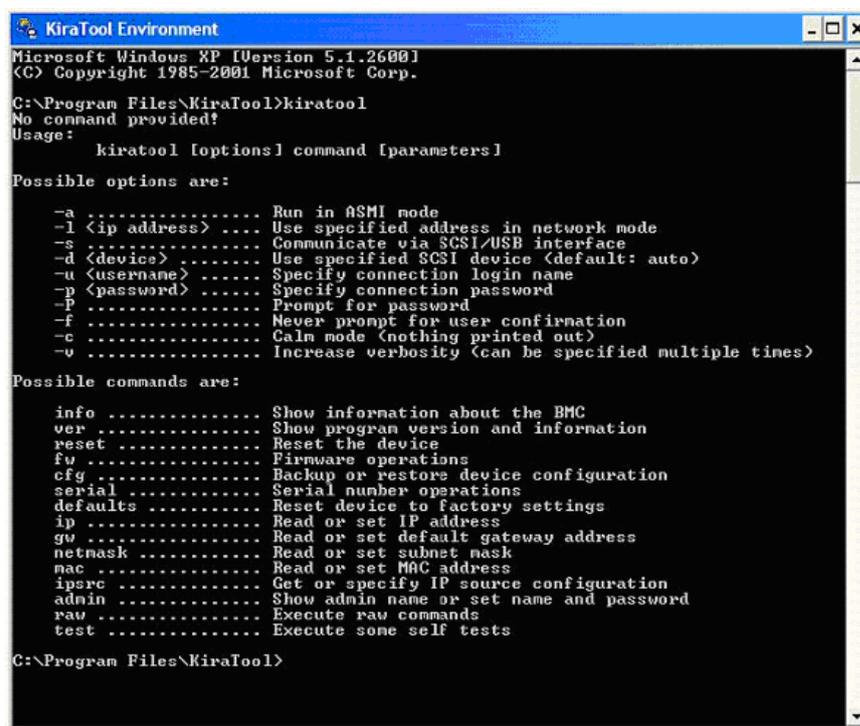
KiraTool, permettant de sauvegarder et de restaurer vos données de configuration, est disponible sur le *CD-ROM Resource and Documentation*.

Il vous est conseillé d'installer cet utilitaire pour que vous puissiez enregistrer et restaurer vos données de configuration.

Note Pour les dernières informations relatives à l'utilitaire *KiraTool*, consultez la documentation associée disponible sur le *CD-ROM Resource and Documentation*.

Version de Windows

1. Recherchez le fichier exécutable auto-extractible *KiraTool* (par exemple, *KiraTool.exe*) sur le *CD-ROM Resource and Documentation*.
2. Double-cliquez sur le fichier avec le bouton gauche de la souris et suivez les instructions à l'écran.
3. A la fin de la procédure, sélectionnez FINISH (Terminer) et une icône *KiraTool* apparaîtra automatiquement sur le bureau.
4. Pour utiliser l'utilitaire *KiraTool*, cliquez sur l'icône pour ouvrir une boîte de ligne de commande Windows standard dans le bon répertoire.
Les commandes et les options suivantes sont disponibles :



```
KiraTool Environment
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\KiraTool>kiratool
No command provided!
Usage:
    kiratool [options] command [parameters]

Possible options are:
-a ..... Run in ASMI mode
-l <ip address> ... Use specified address in network mode
-s ..... Communicate via SCSI/USB interface
-d <device> ..... Use specified SCSI device (default: auto)
-u <username> ..... Specify connection login name
-p <password> ..... Specify connection password
-P ..... Prompt for password
-f ..... Never prompt for user confirmation
-c ..... Calm mode (nothing printed out)
-v ..... Increase verbosity (can be specified multiple times)

Possible commands are:
info ..... Show information about the BMC
ver ..... Show program version and information
reset ..... Reset the device
fw ..... Firmware operations
cfg ..... Backup or restore device configuration
serial ..... Serial number operations
defaults ..... Reset device to factory settings
ip ..... Read or set IP address
gw ..... Read or set default gateway address
netmask ..... Read or set subnet mask
mac ..... Read or set MAC address
ipsrc ..... Get or specify IP source configuration
admin ..... Show admin name or set name and password
raw ..... Execute raw commands
test ..... Execute some self tests

C:\Program Files\KiraTool>
```

Figure 2-3. Commandes et options de l'utilitaire KiraTool - Windows

Version Linux

1. Recherchez le fichier exécutable KiraTool (par exemple, KiraTool) sur le *CD-ROM Resource and Documentation*
2. Copiez le fichier exécutable dans un répertoire de votre environnement \$PATH, par exemple `usr/local/bin`. Comme les répertoires système \$PATH sont protégés, vous devrez vous connecter en tant que `root` :

```
linux # cp kiratool /usr/local/bin
linux # chmod 755 /usr/bin/local/kiratool
```

3. Chargez le module kernel `sg` (requis pour lancer l'utilitaire KiraTool)

```
modprobe sg
```

4. Démarrez l'utilitaire KiraTool en appelant le fichier exécutable. Les commandes et les options suivantes sont disponibles :



```
root@valfed2:/usr/local/bin
File Edit View Terminal Help

[root@valfed2 bin]# KiraTool
No command provided!
Usage:
    KiraTool [options] command [parameters]

Possible options are:
  -l <ip address> ... Use specified address in network mode
  -s ..... Communicate via SCSI/USB interface
  -d <device> ..... Use specified SCSI device (default: auto)
  -u <username> ..... Specify connection login name
  -p <password> ..... Specify connection password
  -P ..... Prompt for password
  -f ..... Never prompt for user confirmation
  -c ..... Calm mode (nothing printed out)
  -v ..... Increase verbosity (can be specified multiple times)

Possible commands are:
  info ..... Show information about the BMC
  ver ..... Show program version and information
  reset ..... Reset the device
  fw ..... Firmware operations
  cfg ..... Backup or restore device configuration
  serial ..... Serial number operations
  defaults ..... Reset device to factory settings
  ip ..... Read or set IP address
  gw ..... Read or set default gateway address
  netmask ..... Read or set subnet mask
  mac ..... Read or set MAC address
  ipsrc ..... Get or specify IP source configuration
  admin ..... Show admin name or set name and password
  raw ..... Execute raw commands
  test ..... Execute some self tests
[root@valfed2 bin]#
```

Figure 2-4. Commandes et options de KiraTool - Linux

Chapitre 3. Gestion de l'alimentation

Ce chapitre explique comment utiliser les contrôles d'alimentation du serveur. Il comprend les rubriques suivantes :

- Présentation des fonctionnalités de gestion de l'alimentation, page 3-2
- Vérification de l'état d'alimentation, page 3-4
- Démarrage du serveur depuis la console, page 3-6
- Arrêt du serveur depuis la console, page 3-8
- Arrêt forcé / Réinitialisation du serveur, page 3-10

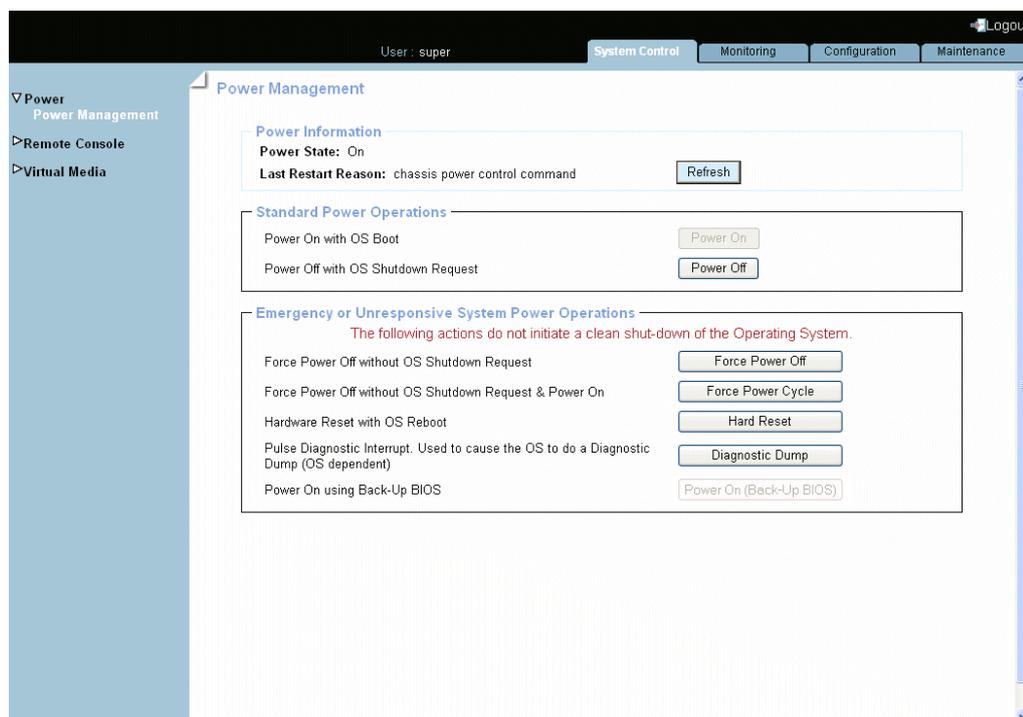
3.1. Présentation des fonctionnalités de gestion de l'alimentation

La page Power Management (Gestion de l'alimentation) permet de vérifier l'état d'alimentation du système, d'effectuer le démarrage du système, de forcer un arrêt et/ou de récupérer le système après une panne ou en cas d'urgence.

Les options de gestion de l'alimentation sont décrites dans la Figure 3-1 ci-dessous.

Procédure

- Depuis l'onglet System Control (Contrôle système), cliquez sur Power > Power Management (Alimentation - Gestion de l'alimentation) pour ouvrir la page Power Management (Gestion de l'alimentation).



La page Power Management (Gestion de l'alimentation) est divisée en trois zones :

- Power Information (Informations sur l'alimentation)
utilisée pour vérifier l'état d'alimentation du système.
- Standard Power Operations (Opérations standard d'alimentation)
utilisée pour effectuer les séquences de démarrage/arrêt.
- Emergency or Unresponsive System Power Operations (Gestion de l'alimentation en cas d'urgence ou de non-réponse)
utilisée pour effectuer des séquences de démarrage après une panne système ou en cas d'urgence.

Power Information (Information sur l'alimentation)	
Power State (État de l'alimentation)	2 valeurs possibles : <ul style="list-style-type: none"> • On (démarré) • Off (arrêté)
Last Restart Reason (Cause du dernier redémarrage)	Plusieurs valeurs possibles expliquant la dernière action ayant provoqué un redémarrage, comme détaillé dans le Tableau 3-1 ci-dessous
Bouton Refresh (Rafraîchir)	Permet de mettre à jour les données affichées.
Standard Power Operations (Opérations standard d'alimentation)	
Bouton Power On (Démarrage)	Accessible uniquement quand le système est arrêté. Lance la séquence de démarrage. Pendant cette séquence, le matériel est démarré et le système d'exploitation est chargé. Note : Si une erreur apparaît pendant cette séquence, le système passe automatiquement en mode veille.
Bouton Power Off (Arrêt)	Accessible uniquement quand le système est démarré. Demande au système d'exploitation d'effectuer un arrêt normal. Pendant cette séquence, le système d'exploitation enregistre les données, ferme toutes les applications et s'arrête. Note : Le système d'exploitation doit être configuré pour accepter la demande d'arrêt.
Emergency or Unresponsive System Power Operations (Gestion de l'alimentation en cas d'urgence ou de non-réponse)	
Important : Ces boutons ne doivent être utilisés que si le système d'exploitation ne répond pas à une demande d'arrêt normale. Ces séquences peuvent provoquer des pertes de données et des corruptions de fichiers.	
Bouton Force Power Off (Forcer l'arrêt)	Effectue une séquence d'arrêt indépendamment du système d'exploitation.
Bouton Force Power Cycle (Forcer le cycle de démarrage/arrêt)	Effectue une séquence d'arrêt indépendamment du système d'exploitation et relance automatiquement une séquence de démarrage.
Bouton Hard Reset (Redémarrer à froid)	Effectue une séquence de démarrage/arrêt indépendamment du système d'exploitation et est utilisé en dernier recours pour récupérer de force le système lorsqu'il est bloqué. Toutes les informations mises en cache sont effacées.
Bouton Diagnostic Dump (Vidage des diagnostics)	Déclenche une interruption pour les diagnostics de l'erreur. Le système d'exploitation vide le contenu de la mémoire sur le disque et le système est remis à l'état initial.
Bouton Power On (Back-Up BIOS) (Démarrage (Sauvegarde BIOS))	Effectue une séquence de démarrage qui utilise une version de sauvegarde du BIOS. Cette fonctionnalité est utilisée pour redémarrer le serveur quand l'intégrité du BIOS n'est plus assurée.

Figure 3-1. Présentation des fonctionnalités de gestion de l'alimentation

3.2. Vérification de l'état d'alimentation

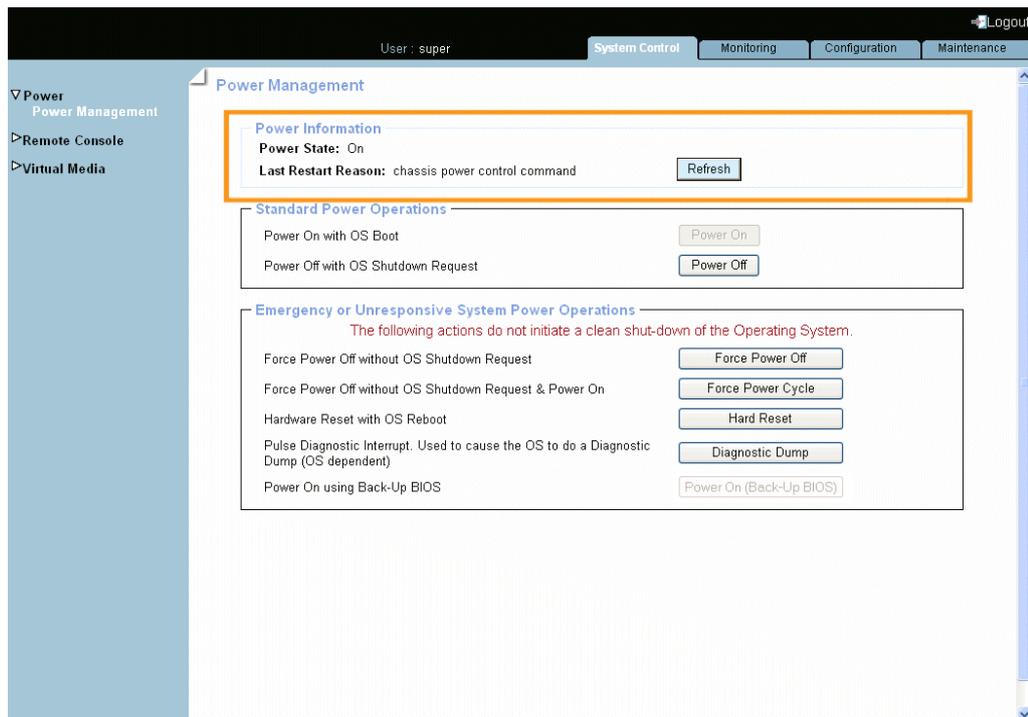
L'état d'alimentation du système peut être vérifié à tout moment depuis la page Power Management (Gestion de l'alimentation) boîte Power Information (Informations sur l'alimentation).



Important L'état de l'alimentation n'est pas mis à jour automatiquement. Par conséquent l'affichage peut ne pas refléter l'état réel. Vous pouvez mettre à jour l'état de l'alimentation avec le bouton Refresh (Rafraîchir).

Procédure

- Depuis l'onglet System Control (Contrôle système), cliquez sur Power > Power Management (Alimentation - Gestion de l'alimentation) pour ouvrir la page Power Management (Gestion de l'alimentation).



Power Information (Information sur l'alimentation)	
Note : Pour des détails sur les autres fonctions de gestion de l'alimentation, voir Figure 3-1, page 3-3.	
Power State (État de l'alimentation)	2 valeurs possibles : <ul style="list-style-type: none"> • On (démarré) • Off (arrêté)
Last Restart Reason (Cause du dernier redémarrage)	Plusieurs valeurs possibles expliquant la dernière action ayant provoqué un redémarrage, comme détaillé dans le Tableau 3-1 ci-dessous
Bouton Refresh (Rafraîchir)	Permet de mettre à jour les données affichées.

Figure 3-2. Vérification de l'état d'alimentation

Le tableau suivant détaille les valeurs pouvant apparaître dans le champ Last Restart Reasons (Causes du dernier redémarrage) de la boîte Power Information (Informations sur l'alimentation).

Last Restart Reason (Cause du dernier redémarrage)	Explication
Chassis power control command (Commande de contrôle de l'alimentation du châssis)	Le serveur a été redémarré depuis la console matérielle ou avec IPMITOOL via le réseau local.
Reset via push button (Réinitialisation avec le bouton poussoir)	Le serveur a été réinitialisé avec le bouton poussoir du serveur.
Power-up via push button (Démarrage avec le bouton poussoir)	Le serveur a été redémarré avec le bouton poussoir du serveur.
Watchdog expired (Temps de surveillance dépassé)	Le serveur a été redémarré automatiquement à l'expiration du temps de surveillance IPMI.
Reset via PEF (Platform Event Filtering) (Réinitialisation via PEF (Filtrage d'événements de plateforme))	Le serveur a été réinitialisé après la transmission d'un événement configuré pour effectuer automatiquement la réinitialisation.
Power-cycle via PEF (Démarrage via PEF)	Le serveur a été arrêté/redémarré après la transmission d'un événement configuré pour effectuer automatiquement le cycle arrêt/redémarrage.
Power-up due to always-restore power policy (Démarrage automatique)	Le serveur a été redémarré automatiquement lorsque le courant a été appliqué ou rétabli après une coupure secteur, en conformité avec les paramètres du système de gestion d'alimentation.
Power-up due to restore-previous power policy (Démarrage automatique)	Le serveur a été redémarré automatiquement lorsque le courant a été appliqué ou rétabli après une coupure secteur, en conformité avec les paramètres du système de gestion d'alimentation.
OEM	Le serveur a été redémarré automatiquement après la réception d'un signal de réveil par le réseau (WOL).

Table 3-1. Informations sur l'alimentation - Causes potentielles du dernier redémarrage

3.3. Démarrage du serveur depuis la console

Le système peut être démarré depuis la page Power Management Standard Power Operations (Gestion de l'alimentation - Opérations standard d'alimentation).



Important L'affichage de l'état de l'alimentation n'est pas mis à jour automatiquement. Par conséquent l'état affiché peut ne pas refléter l'état réel et le bouton Power On (Démarrage) peut ne pas être actif bien que le système soit arrêté. Vous pouvez mettre à jour l'état de l'alimentation avec le bouton Refresh (Rafraîchir).

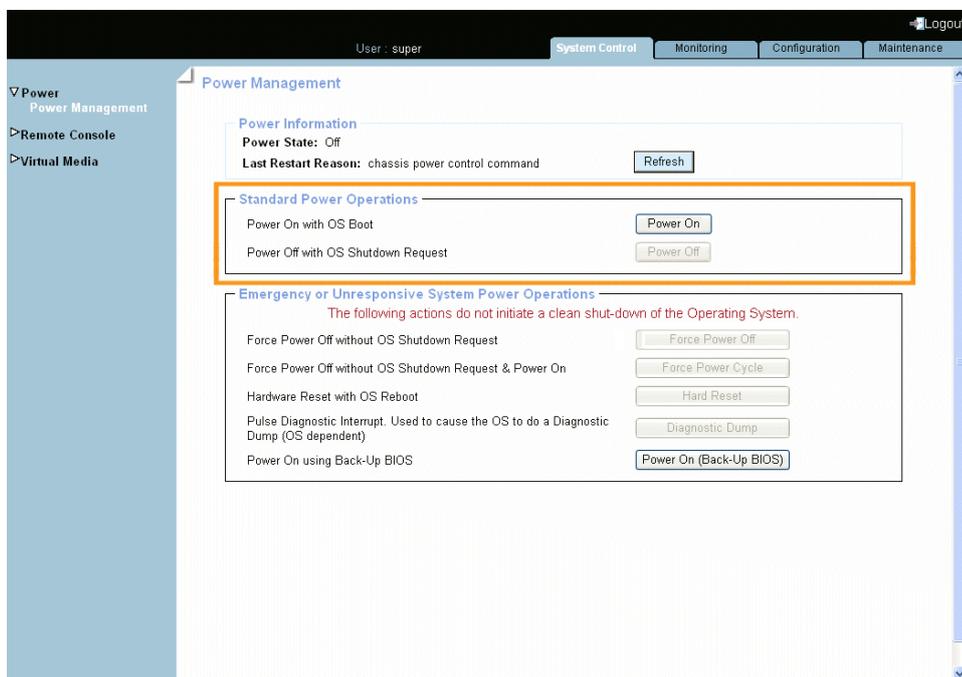
Prérequis

Vous avez la permission Power Control (Gestion de l'alimentation)

Le bouton Power On (Démarrage) est actif

Procédure

1. Depuis l'onglet System Control (Contrôle système), cliquez sur Power > Power Management (Alimentation - Gestion de l'alimentation) pour ouvrir la page Power Management (Gestion de l'alimentation).



Standard Power Operations (Opérations standard d'alimentation)	
<p>Note :</p> <p>Pour des détails sur les autres fonctions de gestion de l'alimentation, voir Figure 3-1, page 3-3.</p>	
Bouton Power On (Démarrage)	<p>Lance la séquence de démarrage. Pendant cette séquence, le matériel est démarré et le système d'exploitation est chargé.</p> <p>Note :</p> <p>Si une erreur apparaît pendant cette séquence, le système passe automatiquement en mode veille.</p>
Bouton Power Off (Arrêt)	Accessible uniquement quand le système est démarré.

Figure 3-3. Démarrage du serveur depuis la console

2. Depuis la boîte **Standard Power Operations** (Opérations standard d'alimentation), cliquez sur **Power On** (Démarrage) pour lancer la séquence de démarrage qui peut prendre quelques minutes.
3. Dans la boîte **Power Information** (Informations d'alimentation), cliquez sur le bouton **Refresh** (Rafraîchir) pour mettre à jour l'état de l'alimentation. Quand la séquence de démarrage est terminée, la valeur **Power State** (État d'alimentation) passe de **Off** à **On** et le bouton **Power Off** (Arrêt) est actif.
4. Connectez la Console système distante pour suivre la séquence de démarrage, comme expliqué dans Lancement de la console système distante, page 4-10.



Important Le bouton physique d'alimentation situé sur le panneau de contrôle local ne doit être utilisé que pour des opérations de maintenance et/ou en cas d'urgence ou de panne réseau.

Que faire en cas d'incident ?

- Le câble d'alimentation peut être débranché.
- La séquence de démarrage n'est pas terminée.
- L'alimentation peut être endommagée.

3.4. Arrêt du serveur depuis la console

Le système peut être arrêté depuis la page Power Management , boîte Standard Power Operations (Gestion de l'alimentation - Opérations standard d'alimentation).



Important L'affichage de l'état de l'alimentation n'est pas mis à jour dynamiquement. Par conséquent l'état affiché peut ne pas refléter l'état réel et le bouton Power Off (Arrêt) peut ne pas être activé bien que le système soit démarré. Vous pouvez mettre à jour l'état de l'alimentation avec le bouton Refresh (Rafraîchir).

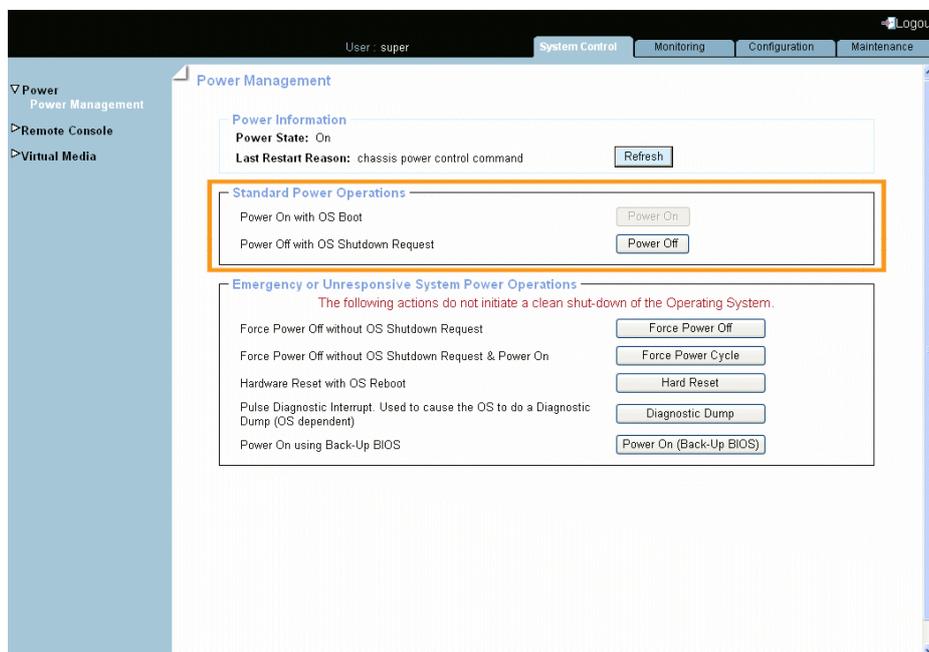
Prérequis

Vous avez la permission Power Control (Gestion de l'alimentation)

Le bouton Power Off (Arrêt) est actif

Procédure

1. Depuis l'onglet System Control (Contrôle système), cliquez sur Power > Power Management (Alimentation - Gestion de l'alimentation) pour ouvrir la page Power Management (Gestion de l'alimentation).



Standard Power Operations (Opérations standard d'alimentation)	
Note : Pour des détails sur les autres fonctions de gestion de l'alimentation, voir Figure 3-1, page 3-3.	
Bouton Power On (Démarrage)	Accessible uniquement quand le système est arrêté.
Bouton Power Off (Arrêt)	<p>Demande au système d'exploitation d'effectuer un arrêt normal.</p> <p>Pendant cette séquence, le système d'exploitation enregistre les données, ferme toutes les applications et s'arrête.</p> <p>Note : Le système d'exploitation doit être configuré pour accepter la demande d'arrêt.</p>

Figure 3-4. Arrêt du serveur depuis la console

2. Depuis la boîte **Standard Power Operations** (Opérations standard d'alimentation), cliquez sur **Power Off (Arrêt)** pour lancer la séquence d'arrêt qui peut prendre quelques minutes.
3. Dans la boîte **Power Information** (Informations d'alimentation), cliquez sur le bouton **Refresh** (Rafraîchir) pour mettre à jour l'état de l'alimentation. Quand la séquence d'arrêt est terminée, la valeur **Power State** (État de l'alimentation) passe de **On** à **Off** et le bouton **Power On** (Démarrage) est actif.
4. Connectez la Console système distante pour suivre la séquence d'arrêt, comme expliqué dans **Lancement de la console système distante**, page 4-10.



Important Le bouton physique d'alimentation situé sur le panneau de contrôle local ne doit être utilisé que pour des opérations de maintenance et/ou en cas d'urgence ou de panne réseau.

Que faire en cas d'incident ?

Si le système reste dans l'état **Power On** (Démarré) après une opération de **Power Off** (Arrêt), un des problèmes suivants peut en être la cause :

- La séquence d'arrêt n'est pas terminée.
- Le système est gelé.
- Le système n'est pas configuré pour accepter la séquence d'arrêt.

Vous pouvez avoir besoin de forcer l'arrêt du système à l'aide d'un des boutons d'arrêt accessibles depuis la boîte **Emergency or Unresponsive System Power Operations** (Gestion de l'alimentation en cas d'urgence ou de non-réponse).

3.5. Arrêt forcé / Réinitialisation du serveur

Dans le cas d'une panne système ou d'un blocage, l'arrêt forcé ou la réinitialisation du système peuvent être effectués depuis la page Power Management (Gestion de l'alimentation) boîte Emergency or Unresponsive System Power Operations (Gestion de l'alimentation en cas d'urgence ou de non-réponse).



Important L'affichage de l'état de l'alimentation n'est pas mis à jour automatiquement. Par conséquent l'état affiché peut ne pas refléter l'état réel et les boutons Arrêt/Réinitialisation d'urgence peuvent ne pas être actifs. Vous pouvez mettre à jour l'état de l'alimentation avec le bouton Refresh (Rafraîchir).

Prérequis

Vous avez la permission Power Control (Gestion de l'alimentation)

Le système reste dans l'état Power On (Démarrage) après une opération Power Off (Arrêt)

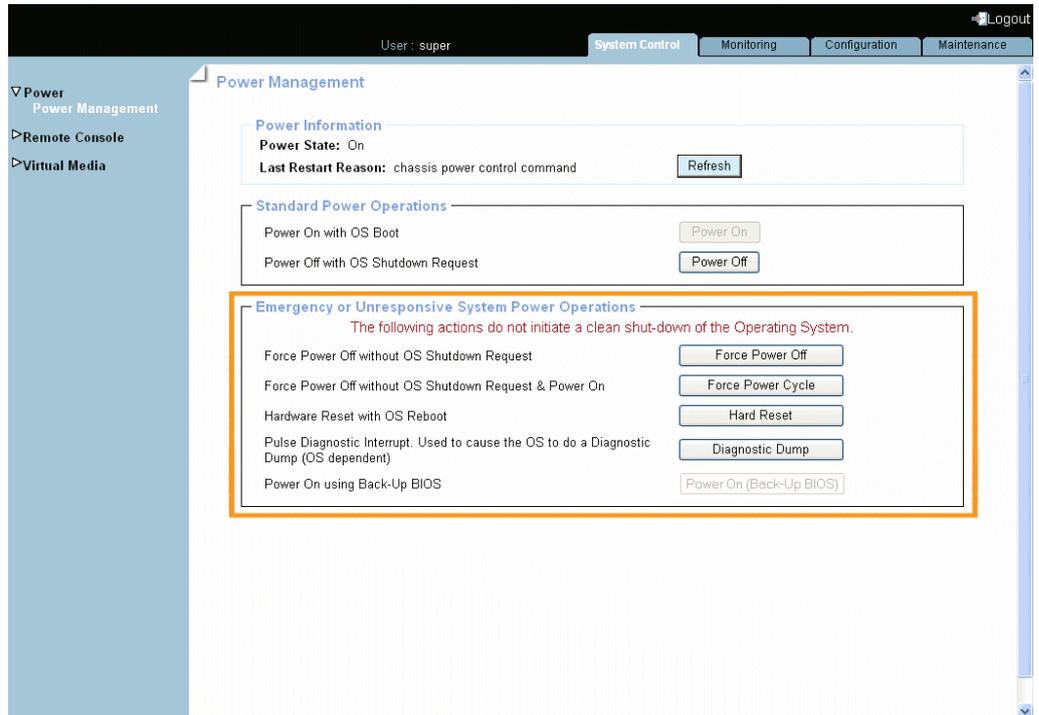
Procédure



AVERTISSEMENT

Les boutons Emergency or Unresponsive System Power Operations (Gestion de l'alimentation en cas d'urgence ou de non-réponse) ne doivent être utilisés que si le système d'exploitation ne répond pas à une demande d'arrêt normale. Ces séquences peuvent provoquer des pertes de données et des corruptions de fichiers.

1. Depuis l'onglet System Control (Contrôle système), cliquez sur Power > Power Management (Alimentation - Gestion de l'alimentation) pour ouvrir la page Power Management (Gestion de l'alimentation) et accéder à la boîte Emergency or Unresponsive System Power Operations (Gestion de l'alimentation en cas d'urgence ou de non-réponse).



Emergency or Unresponsive System Power Operations (Gestion de l'alimentation en cas d'urgence ou de non-réponse)	
<p>Important : Ces boutons ne doivent être utilisés que si le système d'exploitation ne répond pas à une demande d'arrêt normale. Ces séquences peuvent provoquer des pertes de données et des corruptions de fichiers.</p>	
<p>Note : Pour des détails sur les autres fonctions de gestion de l'alimentation, voir Figure 3-1, page 3-3.</p>	
Bouton Force Power Off (Forcer l'arrêt)	Effectue une séquence d'arrêt indépendamment du système d'exploitation.
Bouton Force Power Cycle (Forcer le cycle de démarrage/arrêt)	Effectue une séquence d'arrêt indépendamment du système d'exploitation et relance automatiquement une séquence de démarrage.
Bouton Hard Reset (Redémarrer à froid)	Redémarre le système d'exploitation sans effectuer d'arrêt du système. Toutes les informations mises en cache sont effacées. Utilisez-le en dernier recours pour forcer la récupération du système d'exploitation quand il est bloqué.
Bouton Diagnostic Dump (Vidage des diagnostics)	Déclenche une interruption pour les diagnostics de l'erreur. Le système d'exploitation vide le contenu de la mémoire sur le disque et le système est remis à l'état initial.
Bouton Power On (Back-Up BIOS) (Démarrage (Sauvegarde BIOS))	Effectue une séquence de démarrage qui utilise une version de sauvegarde du BIOS. Cette fonctionnalité est utilisée pour redémarrer le serveur quand l'intégrité du BIOS n'est plus assurée.

Figure 3-5. Arrêt d'urgence

2. Depuis la boîte **Emergency or Unresponsive System Power Operations (Gestion de l'alimentation en cas d'urgence ou de non-réponse)**, sélectionnez avec soin l'opération requise puis cliquez sur le bouton correspondant pour lancer la séquence sélectionnée qui peut prendre quelques minutes.
3. Dans la boîte **Power Information (Informations d'alimentation)**, cliquez sur le bouton **Refresh (Rafraîchir)** pour mettre à jour l'état de l'alimentation.

Chapitre 4. Utilisation de la console système distante

Ce chapitre explique comment configurer et utiliser la console système distante. Il comprend les rubriques suivantes :

- Configuration de la console système distante, page 4-2
- Lancement de la console système distante, page 4-10
- Arrêt de la console système distante, page 4-20

4.1. Configuration de la console système distante

La fonctionnalité Console système distante est utilisée pour se connecter directement au serveur depuis la console matérielle, permettant l'affichage, l'utilisation et le contrôle du serveur à distance en utilisant le clavier, l'écran et la souris de votre ordinateur local.

Cette fonctionnalité peut être utilisée avec la fonctionnalité Virtual Media (Média virtuel) pour exécuter des installations de logiciels et de firmwares à distance.

Notes Pour une utilisation régulière, les utilisateurs finaux se connecteront à distance au serveur en utilisant le bureau client distant compatible avec leur système d'exploitation (par ex. Terminal Server pour Microsoft Windows ou Xming pour Linux).

La Console système distante peut être configurée pour convenir à vos besoins depuis la console matérielle, comme expliqué dans les sections suivantes.

Note L'écriture des données sur un support CD/DVD virtuel n'est pas supporté.

Prérequis

La Console système distante est un applet Java qui établit une connexion TCP avec le contrôleur de gestion intégré (BMC) en utilisant le protocole RFB et requiert l'installation de Java Runtime Environment (JRE) version 1.4 ou supérieure sur votre ordinateur.

Pour pouvoir utiliser la fonctionnalité Console système distante, le réseau doit être configuré pour prendre en charge le protocole RFB.

4.1.1. Configuration des paramètres spécifiques utilisateur

La page **Remote Console Settings** (Paramètres de la console distante) permet de configurer certains paramètres pour :

- Améliorer les performances d'affichage de la Console système distante
- Configurer les options de démarrage par défaut.
- Spécifier des touches de raccourci pour lancer le processus de synchronisation de la souris.
- Configurer le bouton des combinaisons de touches affiché dans la barre de commande de la Console système distante

Prérequis

User Specific Remote Console Settings (Paramètres de la console distante spécifiques utilisateur) : vous utilisez le compte utilisateur **super**

Transmission Encoding (Encodage de la transmission) : vous avez la permission **RC Settings (Encoding)** (Paramètres console distante (Encodage))

Exclusive Access (Accès exclusif) : vous avez la permission **RC Settings (Exclusive Access)** (Paramètres console distante (Accès exclusif))

Monitor Mode (Mode moniteur) : vous avez la permission **RC Settings (Monitor Mode)** (Paramètres console distante (Mode moniteur))

Touches Mouse Hotkey et Remote Console Button (Touches rapides de la souris et de la console distante) : vous avez la permission **RC Settings (Hotkeys)** (Paramètres console distante (Touches rapides))

Procédure

1. Depuis l'onglet Configuration, cliquez sur Remote Console Settings > User Specific (Paramètres de la console distante - Spécifiques utilisateur). La page Remote Console Settings (Paramètres de la console distante) apparaît.

Connected on Module: 0 (Master) Logout

User : super System Control Monitoring Configuration Maintenance

Remote Console Settings

User Specific Remote Console Settings

The settings on this page are user specific. Modifications will affect the selected user only.

super Update

Transmission Encoding

Automatic Detection *

Pre-configured

Network Speed LAN (high color) *

Manually

Compression 0 - none *

Color Depth 16 bit - high col *

Miscellaneous Remote Console Settings

Start in Monitor Mode *

Start in Exclusive Access Mode *

Mouse Hotkey

Hotkey (Help) Alt+F12 *

Used for fast mouse synchronization (in Double Mouse mode) and to free the grabbed mouse (in Single Mouse mode).

Remote Console Button Keys

	Key Definition (Help)	Name
Button Key 1	confirm Ctrl+*Alt+*Delete *	
Button Key 2	ALT+F1 *	
Button Key 3	ALT+F2 *	
Button Key 4	F2 *	
Button Key 5	F12 *	
Button Key 6	ALT+F11 *	

More entries

Apply View Defaults

* Stored value is equal to the default.

User Specific Remote Console Settings (Paramètres de la console distante - Spécifiques utilisateur)	
<p>Cette boîte permet de configurer les paramètres de la Console système distante disponibles dans cette page pour votre propre compte utilisateur ou pour un autre utilisateur. Sélectionnez dans la liste déroulante un utilisateur puis cliquez sur le bouton Update (Mise à jour) pour afficher/modifier les paramètres de la Console système distante configurés pour cet utilisateur</p>	
Transmission Encoding (Encodage de la transmission)	
<p>Cela vous permet de changer l'algorithme d'encodage de l'affichage utilisé pour transmettre les données vidéo à la Console système distante dans le but d'améliorer ou d'optimiser la vitesse d'affichage sur l'écran distant.</p>	
Automatic Detection (Détection automatique)	L'encodage vidéo et le niveau de compression sont calculés automatiquement selon la bande passante disponible et les données courantes de la vidéo.
Pre-configured (Préconfiguré)	Sélectionnez dans la liste déroulante Network Speed (Vitesse du réseau) le paramètre préconfiguré correspondant aux spécifications de votre réseau.
Manually (Manuellement)	<p>Utilisez cette option pour ajuster manuellement la vitesse de compression et la profondeur des couleurs. Notez que les valeurs affichées dans la liste déroulante Color Depth (Profondeur des couleurs) diffèrent en fonction de la valeur sélectionnée dans la liste déroulante Compression.</p> <p>La profondeur des couleurs est de 16 Bit (65536 couleurs). Les autres profondeurs des couleurs sont destinées à des réseaux plus lents afin de permettre une transmission plus rapide des données. Par conséquent, la compression au niveau 0 (pas de compression) n'utilise que 16 Bit ou 8 Bit (256 couleurs) de profondeur des couleurs. Pour des bandes passantes inférieures, des profondeurs de couleurs de 4 Bit (16 couleurs) et de 2 Bit (4 nuances de gris) sont recommandées pour des interfaces de bureau typiques. Des images photos donnent les meilleurs résultats avec 4 Bit (16 nuances de gris). Une profondeur des couleurs de 1 Bit (noir et blanc) devra être utilisée pour des connexions réseau extrêmement lentes.</p>
Miscellaneous Remote Console Settings (Paramètres divers de la console distante)	
Start in Monitor Mode (Démarrer en mode d'accès moniteur)	Sélectionnez cette option pour démarrer la Console système distante avec l'option Monitor only (Moniteur uniquement) activée.
Start in Exclusive Access Mode (Démarrer en mode d'accès exclusif)	Sélectionnez cette option pour démarrer la Console système distante avec l'option Exclusive Access (Accès exclusif) activée.
Mouse Hotkey (Touche rapide de la souris)	
Hotkey (Touche rapide)	Ce champ permet d'indiquer une combinaison de touches rapides qui démarre le processus de synchronisation de la souris quand elle est sélectionnée dans la Console système distante. Cette touche rapide ne fonctionne que si vous avez sélectionné Linux Mouse Type (Type de souris Linux), comme décrit dans Configuration du clavier et de la souris, page 4-6

Remote Console Button Keys (Touches de la console distante)	
<p>Cette boîte permet de définir jusqu'à 32 combinaisons de touches qui peuvent être envoyées au serveur distant.</p> <p>Par défaut, la combinaison confirm Control+Alt+Delete est définie pour la Touche 1, où confirm signifie qu'une boîte de dialogue de confirmation demandera à l'utilisateur de confirmer cette action avant que cette combinaison ne soit envoyée au serveur distant.</p>	
More Entries (Entrées supplémentaires)	Pour ajouter des entrées supplémentaires, sélectionnez ce bouton et complétez la Key Definition (Définition de la touche) comme expliqué dans la rubrique d'aide associée.
Key Definition (Définition des touches)	La combinaison de touches devant être envoyée au serveur distant.
Name (Nom)	Nom facultatif pour une identification facile de l'action associée à la combinaison de touches.
Help (Aide)	Explique comment définir les combinaisons de touches.
Bouton View Defaults (Afficher les valeurs par défaut)	Permet d'afficher les valeurs d'usine. Cliquez sur Apply (Appliquer) pour restaurer la configuration d'usine.

Figure 4-1. Console système distante - Paramètres spécifiques utilisateur

2. Complétez les champs requis puis cliquez sur **Apply** (Appliquer).
3. Utilisez l'utilitaire **KiraTool**, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin.

4.1.2. Configuration du clavier et de la souris

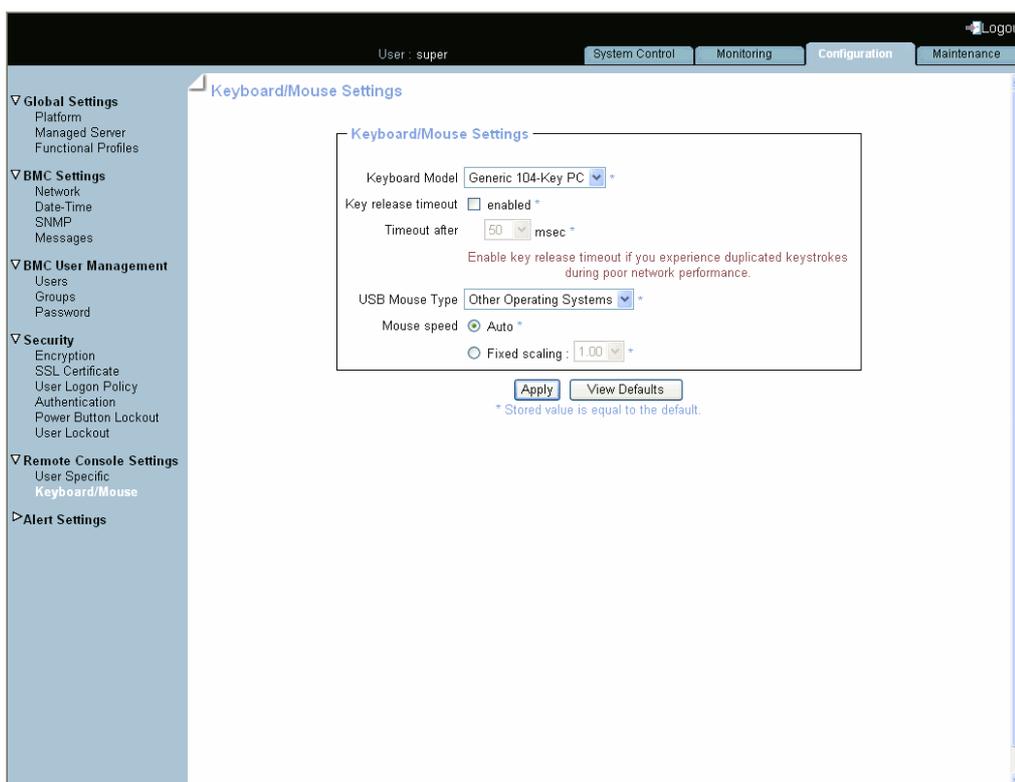
Cette page permet de configurer les paramètres du clavier et de la souris pour utiliser votre souris et clavier locaux afin de contrôler le serveur distant à travers la Console système distante.

Prérequis

Vous avez la permission RC Keyboard/Mouse Settings (Paramètres clavier/souris de la console distante)

Procédure

1. Depuis l'onglet Configuration, cliquez sur Remote Console Settings > Keyboard/Mouse (Paramètres de la console distante – Clavier/Souris). La page Keyboard/Mouse Settings (Paramètres clavier/souris) apparaît.



Keyboard/Mouse Settings (Paramètres clavier/souris)	
Keyboard Model (Modèle de clavier)	Utilisez la liste déroulante pour sélectionner le type de clavier.
Key Release Timeout (Délai de relâchement d'une touche)	Cochez cette option si vous rencontrez des frappes répétées indésirables lorsque vous utilisez votre clavier local pour contrôler le système à distance. Ce problème se produit généralement dans un contexte de basse performance du réseau local. Notez que quand cette option est cochée, la touche est automatiquement considérée comme relâchée même si elle est maintenue appuyée.
Timeout After (Expiration du délai après)	La valeur du délai de relâchement d'une touche est en millisecondes.
USB Mouse Type (Type de souris USB)	Les souris transmettent leurs mouvements en utilisant des valeurs absolues ou relatives, suivant le système d'exploitation distant.
Mouse Speed (Vitesse de la souris)	Par défaut, Auto est coché : Ce mode détecte automatiquement les paramètres de vitesse et d'accélération de votre souris pour déterminer la position du pointeur de la souris sur l'écran distant. Sélectionnez Fixed Scaling (Mise à l'échelle fixe) si vous rencontrez des problèmes de synchronisation entre le pointeur de la souris distante et votre souris locale. Ce mode traduit les mouvements de la souris de la manière suivante : un déplacement d'un pixel sur votre station de travail local correspond à "n" pixels sur le système distant. Procédez par tâtonnement pour sélectionner la meilleur valeur "n" dans la liste déroulante. Cette option fonctionne uniquement si l'accélération de la souris est arrêtée sur le système distant.
Bouton View Defaults (Afficher les valeurs par défaut)	Permet d'afficher les valeurs d'usine. Cliquez sur Apply (Appliquer) pour restaurer la configuration d'usine.

Figure 4-2. Console système distante - Paramètres clavier et souris

2. Changez les paramètres du clavier et de la souris si nécessaire puis cliquez sur **Apply** (Appliquer).
3. Utilisez l'utilitaire KiraTool , fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin.

4.1.3. Partage des lecteurs locaux

La fonction de redirection d'un lecteur de médias virtuel permet de monter des fichiers images disquettes ou CD-ROM et de partager vos lecteurs locaux (lecteurs de disquettes, CD-ROM, clés USB, disques durs...) avec le système distant à travers une connexion réseau TCP. Vous pouvez connecter des fichiers images en utilisant la console matérielle ou à travers la Console système distante. La fonction de partage des lecteurs locaux est disponible uniquement en utilisant la Console système distante.

Cette section décrit comment activer/désactiver la fonctionnalité de redirection du lecteur de la Console système distante. Vous pouvez également activer l'accès en écriture pour que le système distant puisse écrire des données sur les lecteurs partagés.

Note L'écriture des données sur un support CD/DVD virtuel n'est pas supporté.

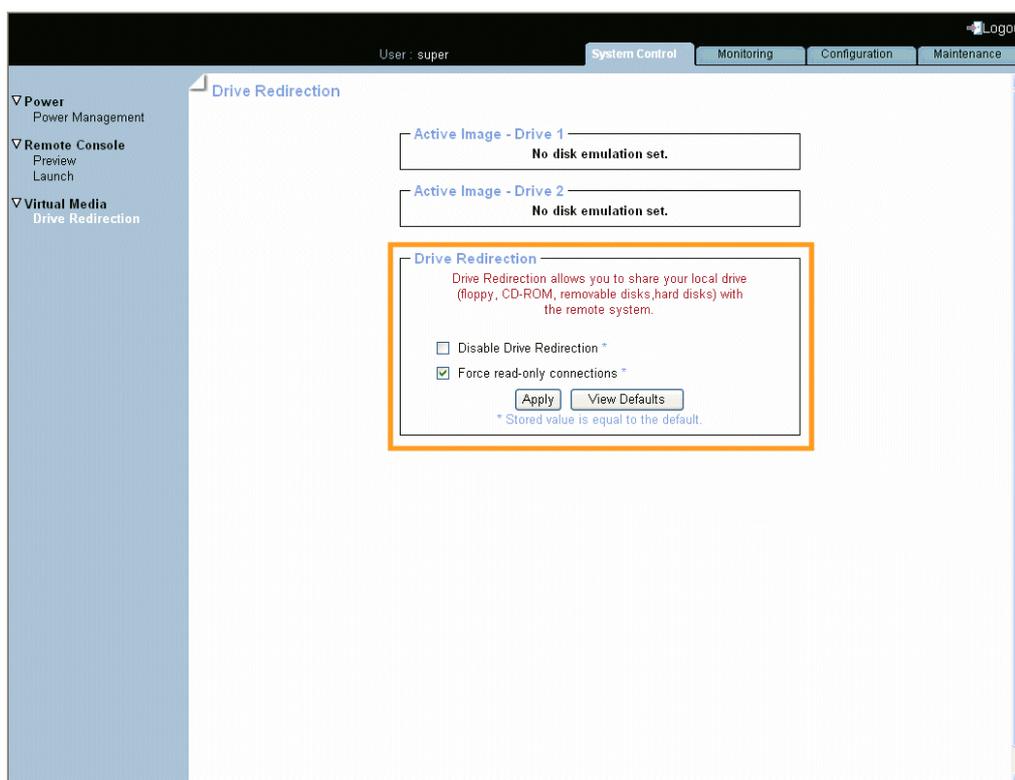
Prérequis

Vous avez la permission **Virtual Media Upload** (Téléchargement de médias virtuels)

Note Pour activer/désactiver la fonction de redirection de lecteur de la console matérielle, attribuez/retirez la permission **Virtual Media Upload** (Téléchargement d'un média virtuel).

Procédure

1. Depuis l'onglet **System Control** (Contrôle système), cliquez sur **Virtual Media > Drive Redirection** (Média virtuel - Redirection du lecteur) pour ouvrir la page **Drive Redirection** (Redirection du lecteur).



Active Image - Drive # Boxes (Boîtes Image active et N° de lecteur)	
Active Image - Drive # (Image active - Numéro du lecteur)	<p>Affiche les détails sur l'image ou sur le lecteur actuellement connecté et fournit des boutons de commande, qui peuvent varier suivant le composant connecté.</p> <p>Quand aucune image ou aucun lecteur n'est connecté, le message No disk emulation is set (Aucune émulation de disque n'est définie) est affiché.</p>
Boîte Drive Redirection (Redirection du lecteur)	
Disable Drive Redirection (Désactiver la redirection du lecteur)	<p>Décochez cette case pour activer la fonction de redirection du lecteur de média virtuel de la Console système distante.</p> <p>Cochez cette case pour désactiver la fonction de redirection du lecteur de média virtuel de la Console système distante.</p>
Force read-only connections (Forcer les connexions en lecture seule)	<p>Cochez cette case pour désactiver l'accès en écriture, les lecteurs partagés sont en lecture seule. Les données peuvent être lues par le système distant, mais pas écrasées pour une intégrité des données améliorée et pour la sécurité du système - Recommandé.</p> <p>Décochez cette case pour activer l'accès en écriture.</p> <p>AVERTISSEMENT : activez l'accès en écriture avec précaution car vous risquez d'endommager les données et les systèmes de fichiers.</p>
Bouton View Defaults (Afficher les valeurs par défaut)	Permet d'afficher les valeurs d'usine.

Figure 4-3. Drive Redirection (Redirection du lecteur)

2. Cochez ou décochez les cases suivant vos besoins puis cliquez sur Apply (Appliquer).

4.2. Lancement de la console système distante

La Console système distante peut être prévisualisée et/ou lancée, à tout moment, directement depuis la console matérielle.

Note Si un message d'avertissement de sécurité, vous demande d'installer et de lancer un plug-in Java, vérifiez l'authenticité de ce plug-in puis cliquez sur **Yes (Oui)** pour installer et lancer ce plug-in.

Procédure

Cette procédure décrit comment lancer et/ou prévisualiser la Console système distante.

1. Depuis l'onglet **System Control (Contrôle système)**, développez le menu **Remote Console (console distante)**.
 - Si vous voulez prévisualiser la Console système distante, passez à l'étape 2
 - Si vous voulez prévisualiser puis lancer la Console système distante, passez à l'étape 3,
 - Si vous voulez lancer la Console système distante directement, passez à l'étape 4, .
2. Pour prévisualiser la Console système distante depuis la console matérielle, cliquez sur **Preview (Prévisualiser)** pour ouvrir la page **Remote Console Preview (Prévisualisation de la console distante)**.

L'affichage n'est pas rafraîchi dynamiquement. Si besoin, cliquez sur le bouton **Refresh (Rafraîchir)** pour mettre à jour l'affichage.



Boîte Preview (Prévisualisation)	
Lien Click to launch (Cliquez pour lancer)	Cliquez sur ce lien pour lancer la Console système distante.
Bouton Refresh (Rafraîchir)	L'affichage n'est pas rafraîchi dynamiquement. Cliquez sur ce bouton pour rafraîchir l'affichage de la Console système distante.
Desktop size information (Informations sur la taille du bureau)	Taille actuelle du bureau de la Console système distante.

Figure 4-4. Prévisualisation de la console système distante

3. Pour prévisualiser puis lancer la Console système distante, cliquez sur **Preview (Prévisualiser)** pour ouvrir la page **Remote Console Preview (Prévisualisation de la console distante)** puis cliquez sur le lien **Click to launch (Cliquez pour lancer)**. La Console système distante s'ouvre dans une nouvelle fenêtre.
4. Pour lancer directement la Console système distante, cliquez sur **Launch (Lancer)**. La Console système distante s'ouvre dans une nouvelle fenêtre.

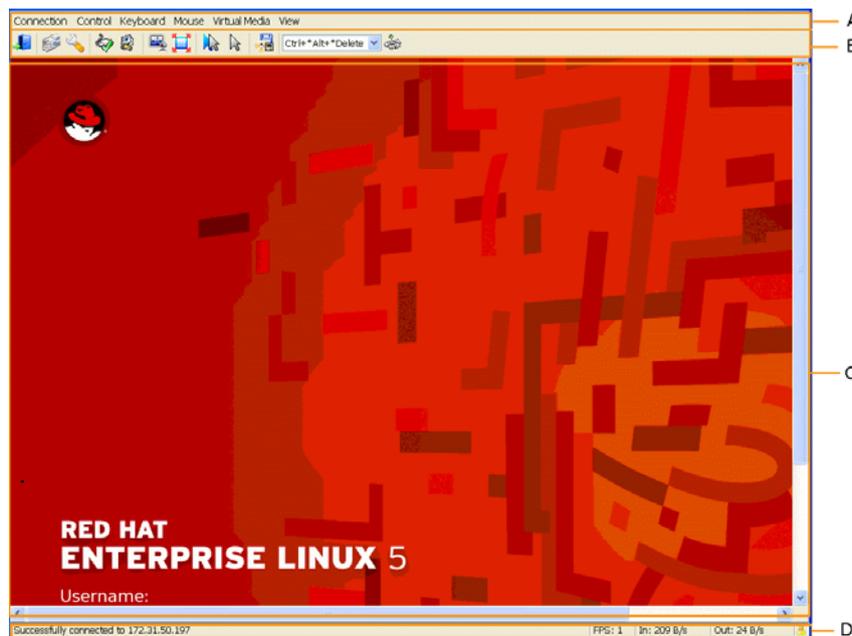
Que faire en cas d'incident ?

- La configuration du réseau n'est pas correcte.
- La version Java Runtime Environment (JRE) 1.4 ou supérieure n'est pas installée sur votre ordinateur.
- Votre réseau n'est pas configuré pour prendre en charge le protocole RFB.

Contactez votre administrateur réseau.

4.2.1. Présentation de la console système distante

Après vous être connecté à la Console système distante, elle se comporte comme si vous étiez assis en face du système distant, tout en utilisant le clavier et la souris locales.



Élément	Description
A : Barre de menu	<p>La barre de menu donne accès aux menus suivants :</p> <ul style="list-style-type: none">• Connection (Connexion)• Control (Commandes)• Clavier• Souris• Virtual Media (Média virtuel)• View (Affichage) <p>Pour plus de détails, consultez Menus de la console système distante, page 4-12.</p>

Élément	Description
B : Barre d'outils	<p>La barre d'outils donne accès aux commandes suivantes :</p> <ul style="list-style-type: none"> • Exit (Sortie) • Screenshot (Capture d'écran) • Properties (Propriétés) • Enter/Leave Monitor Only Mode (Entrer/Quitter le mode Moniteur seul) • Enter/Leave Exclusive Access Mode (Entrer / Quitter le mode Accès exclusif) • Scaling (Mise à l'échelle) • Full Screen Mode (Mode plein écran) • Virtual Media (Média virtuel) • Select Keyboard Macro (Sélectionner macro clavier) • Send Keyboard Macro (Envoyer macro clavier) • Sync Mouse (Reserved) (Synchroniser la souris (Réservé)) • Single Cursor Mode (Mode curseur seul) <p>Pour plus de détails, consultez Barre d'outils de la console système distante, page 4-14.</p>
C: Bureau distant	Cette zone affiche l'écran du bureau du système distant.
D: Barre d'état	La barre d'état donne des informations relatives à la connexion.

Figure 4-5. Présentation de la Console système distante

4.2.2. Menus de la console système distante

Cette section décrit les fonctionnalités disponibles pour configurer et utiliser la barre de menu de la Console système distante.

Connection Control Keyboard Mouse VirtualMedia View

Nom du menu	Éléments du menu	Description
Connection (Connexion)	Properties (Propriétés)	Sélectionnez pour afficher et définir les options de l'écran distant.
	Connection Info (Informations de connexion)	Sélectionnez pour afficher les informations de connexion à distance, telles que Device Address (adresse du dispositif), Connection Port (port de connexion), Incoming/Outgoing Speed (vitesse en entrée/sortie)... .
	Save Screenshot (Sauvegarder Copie d'écran)	Sélectionnez pour enregistrer l'écran distant.
	Screenshot to clipboard (Copie d'écran vers le presse-papier)	Sélectionnez pour copier l'écran distant dans le presse-papier.
	Exit (Sortie)	Sélectionnez pour fermer la connexion distante.

Nom du menu	Éléments du menu	Description
Control (Commandes)	Enter Monitor Only Mode (Entrer dans le mode Moniteur seul)	Sélectionnez pour désactiver l'interaction clavier et souris distante.
	Enter Exclusive Access Mode (Entrer dans le mode Accès exclusif)	Sélectionnez pour forcer la fermeture des sessions distantes de tous les autres utilisateurs jusqu'à ce que l'utilisateur exclusif désactive cette option ou se déconnecte.
	Chat Window (Fenêtre de discussion)	Sélectionnez pour afficher une fenêtre de discussion qui vous permet d'interagir avec d'autres utilisateurs connectés à la console système distante.
Clavier	Keyboard Macros (Macros clavier)	Sélectionnez la macro du clavier requise depuis la liste affichée.
	Local Keyboard Mapping (Mappage du clavier local)	Sélectionnez la langue du clavier depuis la liste affichée.
Souris	Sync Mouse (Synchronisation souris)	Réservé.
	Single Cursor Mode (Mode curseur seul)	Sélectionnez pour désactiver / activer la souris locale. Appuyez sur Alt+F12 pour quitter ce mode.
Virtual Media (Média virtuel)	Virtual Media (Média virtuel)	Sélectionnez pour afficher et connecter un média virtuel. Pour plus de détails, voir Virtualisation de médias, page 4-15.
View (Affichage)	Scaling (Mise à l'échelle)	Sélectionnez pour afficher et définir le type de cadrage et les options de qualité de la fenêtre distante.
	Full Screen Mode (Mode plein écran)	Sélectionnez pour afficher la console distante en mode Plein écran. Appuyez sur Ctrl+Alt+F pour quitter ce mode.
	Show Toolbar (Montrer la barre d'outils)	Sélectionnez pour afficher la barre d'outils de la console distante. Désélectionnez pour cacher la barre d'outils de la console distante.
	Show Statusbar (Montrer la barre d'état)	Sélectionnez pour afficher la barre d'état de la console distante. Désélectionnez pour cacher la barre d'état de la console distante.

Figure 4-6. Console système distante menus



Important Si vous avez un problème avec le clavier, cliquez sur **Keyboard > Local Keyboard Mapping (Clavier - Mappage du clavier local)**. Sélectionnez une autre langue clavier puis resélectionnez la langue clavier requise. Le problème devrait être résolu.

4.2.3. Barre d'outils de la console système distante

Cette section décrit les fonctionnalités disponibles depuis la barre d'outils de la Console système distante.



Icône du bouton	Nom du bouton	Description
	Exit (Sortie)	Sélectionnez pour fermer la connexion distante.
	Screenshot to clipboard (Copie d'écran vers le presse-papier)	Sélectionnez pour copier l'écran distant dans le presse-papier.
	Propriétés (Propriétés)	Sélectionnez pour afficher et définir les options de l'écran distant.
	Enter Monitor Only Mode (Entrer dans le mode Moniteur seul)	Sélectionnez pour désactiver l'interaction clavier et souris distante. Une croix rouge apparaît. Sélectionnez à nouveau pour annuler.
	Enter Exclusive Access Mode (Entrer dans le mode Accès exclusif)	Sélectionnez pour forcer la fermeture des sessions distantes de tous les autres utilisateurs jusqu'à ce que l'utilisateur exclusif désactive cette option ou se déconnecte. Une croix rouge apparaît. Sélectionnez à nouveau pour annuler.
	Scaling (Mise à l'échelle)	Sélectionnez pour afficher et définir le type de cadrage et les options de qualité de la fenêtre distante.
	Full Screen Mode (Mode plein écran)	Sélectionnez pour afficher la console distante en mode Plein écran. Appuyez sur Ctrl+Alt+F pour quitter ce mode.
	Virtual Media (Média virtuel)	Sélectionnez pour afficher et connecter un média virtuel. Pour plus de détails, voir Virtualisation de médias, page 4-15.
	Keyboard Macros (Macros clavier)	Sélectionnez la macro du clavier requise depuis la liste affichée.
	Send Keyboard Macro (Envoyer macro clavier)	Envoyez la macro clavier sélectionnée.
	Sync Mouse (Synchronisation souris)	Réservé.
	Single Cursor Mode (Mode curseur seul)	Sélectionnez pour désactiver / activer la souris locale. Appuyez sur Alt+F12 pour quitter ce mode.

Figure 4-7. Console système distante Barre d'outils

4.3. Virtualisation de médias

En utilisant la fonctionnalité Virtual Media (Media virtuel), vous pouvez virtualiser jusqu'à deux images ou disques, autorisant l'utilisation depuis la Console système distante de n'importe quelle image disquette ou CD, lecteur de disquettes, disque optique et/ou dispositif de stockage de masse USB disponible sur votre ordinateur local ou n'importe où sur le réseau.

Le système distant a ensuite accès au média virtuel sur votre ordinateur local et peut lire et écrire sur ce média comme s'il était physiquement présent sur le système distant. Ces lecteurs virtuels peuvent ensuite être utilisés pour des opérations telles que l'installation d'un logiciel et d'un firmware, la mise à jour de pilotes ou l'installation de nouveaux systèmes d'exploitation.

Cette section vous guide à travers les procédures suivantes :

- Virtualisation d'un lecteur local, page 4-15
- Virtualisation d'un fichier image, page 4-17
- Virtualisation d'un dossier local, page 4-19

4.3.1. Virtualisation d'un lecteur local

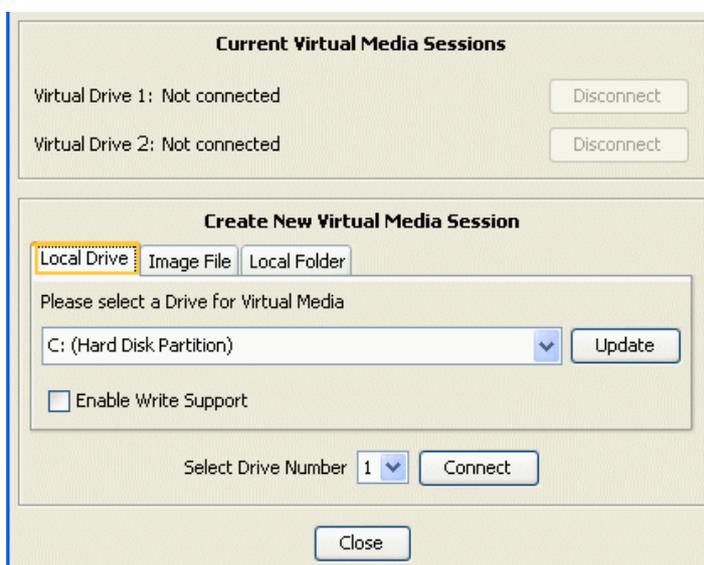
Vous pouvez sélectionner n'importe quel lecteur local et le rendre accessible au serveur distant.

Prérequis

La redirection des lecteurs est activée depuis la console matérielle

Procédure

1. Depuis la barre de menus de la Console système distante, sélectionnez **Virtual Media** (Média virtuel), ou sélectionnez le bouton **Virtual Media** (Média virtuel) () depuis la barre d'outils. La boîte de dialogue **Virtual Media** (Média virtuel) s'ouvre, affichant les options d'état **Current Virtual Media Sessions** (Sessions média virtuel courantes) et l'onglet **Local Drive** (Lecteur local) dans le champ **Create New Virtual Media Session** (Créer une nouvelle session média virtuel).



Current Virtual Media Sessions (Sessions médias virtuels en cours)	
Virtual Drive (Lecteur virtuel) X	Deux valeurs possibles : Connecté / Non connecté
Bouton Disconnect (Déconnecter)	Appuyez sur ce bouton pour déconnecter un lecteur. Si aucun lecteur n'est connecté, ce bouton est grisé.
Onglet Create New Virtual Media Session - Local Drive (Créer une nouvelle session média virtuel - Lecteur local)	
Liste Select a Drive for Virtual Media (Sélectionner un lecteur pour un média virtuel)	Appuyez sur la flèche de déroulement pour sélectionner le lecteur local requis.
Case à cocher Enable Write Support (Activer l'accès en écriture)	Sélectionnez cette case à cocher pour permettre la lecture de données sur le lecteur local.
Liste Select Drive Number (Sélectionner le numéro du lecteur)	Appuyez sur la flèche de déroulement pour sélectionner le numéro de montage du lecteur requis.
Bouton Update (Mettre à jour)	Appuyez sur ce bouton pour mettre à jour la liste des lecteurs locaux.
Bouton Connect (Connecter)	Appuyez sur le bouton Connect (Connecter) pour monter le lecteur. Virtual Drive (Lecteur virtuel) X : Connected (connecté) apparaît dans la zone Current Virtual Media Sessions (Sessions média virtuel courantes) et le bouton Disconnect (Déconnecter) correspondant est activé.

Figure 4-8. Media virtuel – Disque local

2. Configurez le lecteur local comme expliqué précédemment et cliquez sur **Connect (Connecter)**. Le lecteur local est maintenant monté et peut être utilisé par le serveur distant pour lire et/ou écrire (si activé) des données.

4.3.2. Virtualisation d'un fichier image

Vous pouvez émuler jusqu'à deux fichiers image comme des dispositifs USB et les rendre accessibles au serveur distant.

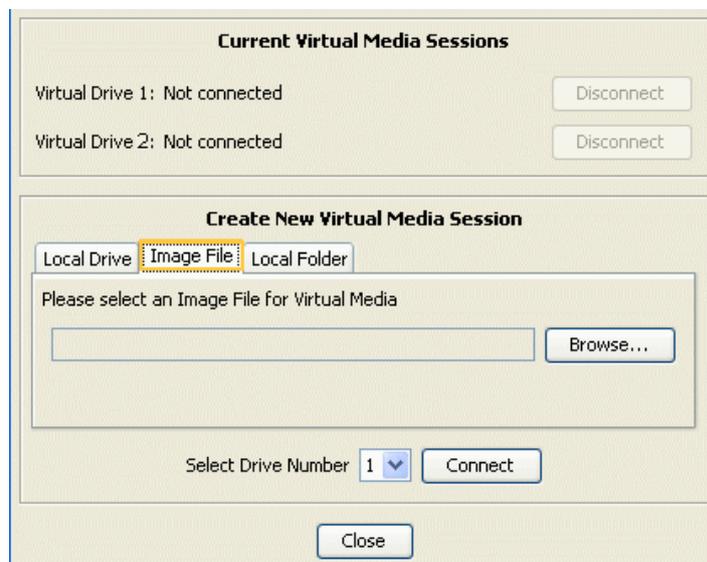
Prérequis

La redirection des lecteurs est activée depuis la console matérielle

Le fichier image a été créé

Procédure

1. Depuis la barre de menus de la Console système distante, sélectionnez **Virtual Media** (Média virtuel), ou sélectionnez le bouton **Virtual Media** (Média virtuel) () depuis la barre d'outils. La boîte de dialogue **Virtual Media** (Média virtuel) s'ouvre, affichant les options d'état **Current Virtual Media Sessions** (Sessions média virtuel courantes) et l'onglet **Local Drive** (Lecteur local) dans le champ **Create New Virtual Media Session** (Créer une nouvelle session média virtuel).
2. Sélectionnez l'onglet **Image File** (Fichier image).



Current Virtual Media Sessions (Sessions médias virtuels en cours)	
Virtual Drive (Lecteur virtuel) X	Deux valeurs possibles : Connecté / Non connecté
Bouton Disconnect (Déconnecter)	Appuyez sur ce bouton pour déconnecter un lecteur. Si aucun lecteur n'est connecté, ce bouton est grisé.
Onglet Create New Virtual Media Session - Image File (Créer une nouvelle session média virtuel - Fichier image)	
Liste Select an Image File for Virtual Media (Sélectionner un fichier image pour un média virtuel)	Appuyez sur la bouton Browse (Afficher) pour sélectionner le fichier image requis.
Liste Select Drive Number (Sélectionner le numéro du lecteur)	Appuyez sur la flèche de déroulement pour sélectionner le numéro de montage du lecteur requis.
Bouton Connect (Connecter)	Appuyez sur le bouton Connect (Connecter) pour monter le fichier image. Virtual Drive (Lecteur virtuel) X : Connected (connecté) apparaît dans la zone Current Virtual Media Sessions (Sessions média virtuel courantes) et le bouton Disconnect (Déconnecter) correspondant est activé.

Figure 4-9. Media virtuel – Fichier image

- Montez le fichier image comme expliqué précédemment et cliquez sur Connect (Connecter). Le fichier image est maintenant monté et peut être utilisé par le serveur distant.

4.3.3. Virtualisation d'un dossier local

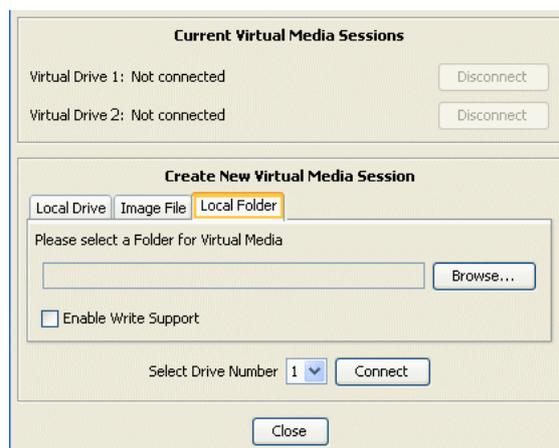
Vous pouvez sélectionner n'importe quel dossier local de votre ordinateur et le rendre accessible au serveur distant.

Prérequis

La redirection des lecteurs est activée depuis la console matérielle

Procédure

1. Depuis la barre de menus de la Console système distante, sélectionnez **Virtual Media** (Média virtuel), ou sélectionnez le bouton **Virtual Media** (Média virtuel) () depuis la barre d'outils. La boîte de dialogue **Virtual Media** (Média virtuel) s'ouvre, affichant les options d'état **Current Virtual Media Sessions** (Sessions média virtuel courantes) et l'onglet **Local Drive** (Lecteur local) dans le champ **Create New Virtual Media Session** (Créer une nouvelle session média virtuel).
2. Sélectionnez l'onglet **Local Folder** (Dossier local).



Current Virtual Media Sessions (Sessions médias virtuels en cours)	
Virtual Drive (Lecteur virtuel) X	Deux valeurs possibles : Connecté / Non connecté
Bouton Disconnect (Déconnecter)	Appuyez sur ce bouton pour déconnecter un lecteur. Si aucun lecteur n'est connecté, ce bouton est grisé.
Onglet Create New Virtual Media Session - Local Folder (Créer une nouvelle session média virtuel - Dossier local)	
Liste Select a Folder for Virtual Media (Sélectionner un dossier pour média virtuel)	Appuyez sur la bouton Browse (Afficher) pour sélectionner le fichier image requis.
Case à cocher Enable Write Support (Activer l'accès en écriture)	Sélectionnez cette case à cocher pour permettre aux données d'être écrites dans le dossier local.
Liste Select Drive Number (Sélectionner le numéro du lecteur)	Appuyez sur la flèche de déroulement pour sélectionner le numéro de montage du lecteur requis.
Bouton Connect (Connecter)	Appuyez sur le bouton Connect (Connecter) pour monter le lecteur. Virtual Drive (Lecteur virtuel) X : Connected (connecté) apparaît dans la zone Current Virtual Media Sessions (Sessions média virtuel courantes) et le bouton Disconnect (Déconnecter) correspondant est activé.

Figure 4-10. Media virtuel – Dossier local

- Configurez le lecteur local comme expliqué précédemment et cliquez sur **Connect** (Connecter) Le dossier local est maintenant monté et peut être utilisé par le serveur distant pour lire et/ou écrire (si activé) des données.

4.4. Arrêt de la console système distante

La Console système distante peut être arrêtée à tout moment en sélectionnant **Connection > Exit** (Connexion - Quitter) depuis la barre de menu ou en sélectionnant le bouton **Exit** (Quitter) () depuis la barre d'outils.

Chapitre 5. Surveillance du serveur

Ce chapitre explique comment surveiller l'activité du serveur et afficher et gérer les journaux d'événements et les messages. Il comprend les rubriques suivantes :

- Configuration initiale de la messagerie et des alertes, page 5-2
- Vérification des capteurs de surveillance, page 5-2
- Vérification et effacement du journal SEL, page 5-4
- Vérification du journal des messages Board & Security, page 5-6
- Téléchargement et suppression du journal BIOS, page 5-7



Important L'information vous aidant à dépanner le serveur en cas d'opération incorrecte est donnée dans **Dépannage du serveur**, page A-1..

5.1. Configuration initiale de la messagerie et des alertes

A la livraison du serveur, vous aurez à effectuer certaines tâches de configuration de base pour pouvoir bénéficier de toutes les fonctionnalités de messagerie et d'alertes disponibles. Ces tâches de configuration sont détaillées dans le chapitre 6, Configuration du contrôleur de gestion intégré du serveur et sont listées ci-dessous :

- Configuration du journal des messages Board & Security, page 6-12
- Configuration des paramètres d'alerte, page 6-50

5.2. Vérification des capteurs de surveillance

Le système est équipé de capteurs qui surveillent l'état de composants matériels, tels que :

- Etat de l'alimentation
- Présence, absence, redondance de composants
- Tension
- Température
- Vitesse des ventilateurs
- Intrusion physique
- etc.

Procédure

1. Depuis l'onglet Monitoring (Surveillance), cliquez sur System Health > Sensors (Santé du système - Capteurs) pour afficher la page Sensor Status (État des capteurs).
2. Cliquez sur Refresh (Rafraîchir) et vérifiez que toutes les icônes des composants sont vertes.

Si l'icône d'un composant n'est pas vert, voir l'annexe A Dépannage du serveur pour plus d'informations.

The screenshot shows the 'Sensor Status' page in a web interface. The top navigation bar includes 'System Control', 'Monitoring', 'Configuration', and 'Maintenance'. The left sidebar shows 'System Health' with sub-items 'Sensors', 'System Event Log', and 'Messages'. The main content area is titled 'Sensor Status' and contains two tables:

BMC Sensor Status

Sensor Type	Sensor Name	Sensor Status	Sensor Reading
System ACPI Power State	ACPI Pwr State	SD/G0: working	

SMC Sensor Status

Sensor Type	Sensor Name	Sensor Status	Sensor Reading
Physical Security	Mod. Intrusion	No intrusion	
Power Supply	PS_0	Presence detected	
Power Supply	PS_1	Presence detected	
Power Supply	PS_2	Device Absent	
Power Unit	Pwr Redundancy		
Power	Pwr Consumption		936 Watts
Processor	PROC_0	Presence detected	
Processor	PROC_1	Presence detected	
Processor	PROC_2	Presence detected	
Processor	PROC_3	Presence detected	

Legend:

- Temperature (Green circle)
- Voltage (Green circle)
- Cooling (Green circle)

Page Sensor Status (État des capteurs)	
Bouton Refresh (Rafraîchir)	La page Sensor Status (État des capteurs) n'est pas mise à jour automatiquement. Par conséquent, l'affichage peut ne pas refléter l'état réel du capteur. Utilisez ce bouton, situé en haut et en bas de la page, pour mettre à jour l'affichage.
Description des icônes d'état	
<p>Les icônes d'état situées à gauche de certains capteurs indiquent l'état du composant surveillé par rapport aux valeurs seuils nominales.</p> <p>NOTE :</p> <p>L'état des capteurs de température, tension et refroidissement est surveillé de façon individuelle et globale. Par défaut, l'état global des capteurs de température ou de tension ou de refroidissement est représenté par l'icône situé à leur gauche. Pour visualiser l'état des capteurs individuels, sélectionnez le bouton Expand (Développer) correspondant.</p> <p>Si l'état d'un capteur individuel devient critique (ROUGE), l'icône d'état global correspondant deviendra ROUGE.</p>	
VERT	NORMAL Fonctionnement correct. Aucun problème détecté.
ROUGE	CRITIQUE Un problème a été détecté. Une action préventive ou corrective immédiate est nécessaire. Si l'icône d'un composant n'est pas vert, voir l'annexe A Dépannage du serveur pour plus d'informations.
GRIS	Capteur non disponible.

Figure 5-1. Sensor Status (État des capteurs)

 **Important** Les valeurs et les relevés sont détaillés dans Description des filtres d'alertes prédéfinis, page A-2.

5.3. Vérification et effacement du journal SEL

Les événements enregistrés dans le journal SEL sont conformes au standard IPMI, en particulier ceux concernant :

- Les unités d'alimentation
- Les ventilateurs
- Les capteurs de température

-
- Notes**
- Les événements enregistrés dans ce journal peuvent être transmis via le système d'alerte d'événements à un gestionnaire SNMP ou par courriel au personnel.
 - Vous pouvez accéder à un autre journal, appelé le journal Board and Security Messages (Messages Board & Security). Ce journal enregistre les événements non IPMI.
-



AVERTISSEMENT

Le journal SEL ne peut enregistrer que 512 entrées à la fois.

Une fois cette limite atteinte, le JOURNAL N'EST PAS VIDÉ AUTOMATIQUEMENT pour permettre l'arrivée de nouveaux événements. Au-delà de la limite de 512 entrées, les NOUVEAUX ÉVÉNEMENTS NE SONT PAS ENREGISTRÉS.

Il est fortement recommandé de vider ce journal régulièrement, avec le bouton Clear (Vider) pour que les derniers événements puisse être enregistrés.

Notez que les entrées vidées sont supprimées et ne peuvent plus être récupérées.

-
- Note** La console iCare collecte automatiquement les journaux d'événements système et peut être configurée pour vider automatiquement le journal SEL. Consultez le manuel *iCare Console User's Guide* pour plus de détails.
-

Prérequis

Affichage : aucun

Effacement : vous avez la permission Alert Settings & Clear SEL (Configuration d'alertes & effacement du SEL)

Procédure

- Depuis l'onglet Monitoring (Surveillance), cliquez sur System Health > System Event Log (Santé du système - Journal SEL) pour ouvrir la page System Event Log (Journal SEL).

Date	Time	Sensor Name	Description	Direction
2009-10-23	18:10:44	ILB 1.2V IB	Limit Exceeded	Assertion Event
2009-10-23	18:10:42	PROC_3	Presence detected	Assertion Event
2009-10-23	18:10:42	PROC_2	Presence detected	Assertion Event
2009-10-23	18:10:42	PROC_1	Presence detected	Assertion Event
2009-10-23	18:10:42	PROC_0	Presence detected	Assertion Event
2009-10-23	18:10:41	FANPR_3 Redund.	Fully Redundant	Assertion Event
2009-10-23	18:10:41	FANPR_2 Redund.	Fully Redundant	Assertion Event
2009-10-23	18:10:41	FANPR_1 Redund.	Fully Redundant	Assertion Event
2009-10-23	18:10:41	FANPR_0 Redund.	Fully Redundant	Assertion Event
2009-10-23	18:10:38	FANPR_7 Presence	Device Present	Assertion Event
2009-10-22	16:00:36	FANPR_0 Redund.	Fully Redundant	Assertion Event
2009-10-22	16:00:32	FAN_7 Presence	Device Present	Assertion Event
2009-10-22	16:00:32	FAN_6 Presence	Device Present	Assertion Event
2009-10-22	16:00:32	FAN_5 Presence	Device Present	Assertion Event
2009-10-22	16:00:32	FAN_4 Presence	Device Present	Assertion Event
2009-10-22	16:00:32	FAN_3 Presence	Device Present	Assertion Event
2009-10-22	16:00:32	FAN_2 Presence	Device Present	Assertion Event
2009-10-22	16:00:32	FAN_1 Presence	Device Present	Assertion Event
2009-10-22	16:00:32	FAN_0 Presence	Device Present	Assertion Event
2009-10-22	16:00:31	ACPI Pwr State	S0/G0: working	Assertion Event
2009-10-22	16:00:31	PS_2	Presence detected	Assertion Event
2009-10-22	16:00:31	Pwr Redundancy	Fully Redundant	Assertion Event
2009-10-22	16:00:31	PS_1	Presence detected	Assertion Event
2009-10-22	16:00:31	PS_0	Presence detected	Assertion Event
2009-10-22	16:00:30	Mod. Intrusion	General Chassis intrusion	Assertion Event

Figure 5-2. Journal SEL

- Utilisez le bouton Refresh (Rafraîchir) pour mettre à jour l'affichage à tout moment.
- Utilisez le bouton Clear (Effacer) pour vider le journal. Les entrées sont supprimées et ne peuvent plus être récupérées.

Note Les messages SEL et les opérations de récupération associées sont expliqués dans l'annexe A - Dépannage du serveur.

5.4. Vérification du journal des messages Board & Security

Le journal des messages Board & Security enregistre les événements non IPMI, tels que les erreurs de démarrage, les authentifications utilisateurs, les connexions distantes, les violations de sécurité, les suppressions de journal ou les mises à niveau de firmware.

Note Les événements conformes au standard IPMI sont enregistrés dans le journal SEL.

Prérequis

Vous avez la permission Log View (Consultation des journaux)

Procédure

1. Depuis l'onglet Monitoring (Surveillance), cliquez sur System Health > Messages (Santé du système - Messages) pour afficher la page Board & Security Messages (Messages Board & Security).

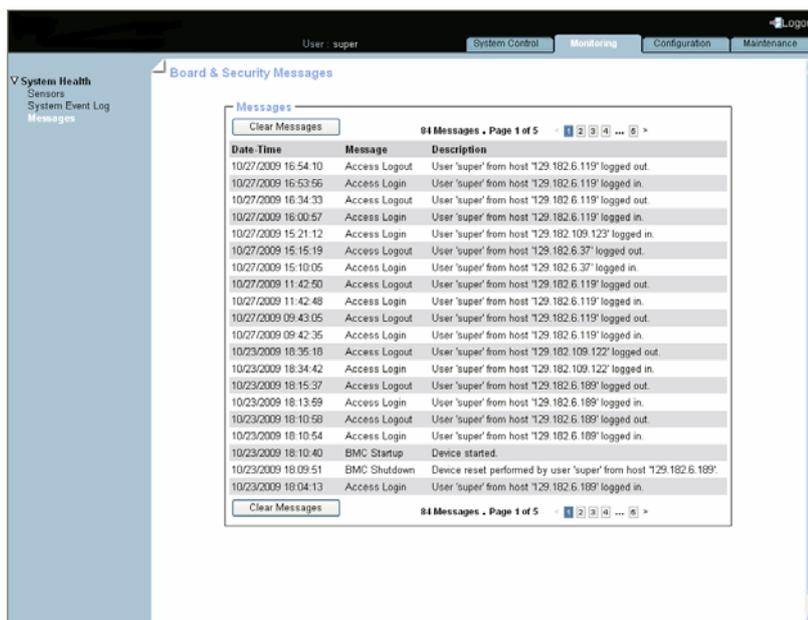


Figure 5-3. Messages Board & Security

2. Parcourez les messages avec les flèches de navigation ou les boutons de numéros de page.



Important Ce journal peut enregistrer jusqu'à 1 000 événements. Une fois cette limite atteinte, l'arrivée de nouveaux messages supprimera automatiquement les plus anciens messages du journal.

5.5. Téléchargement et suppression du journal BIOS

Les journaux du BIOS logs sont envoyés à l'EMM. Si votre serveur n'est pas contrôlé par la console iCare, vous pouvez récupérer et supprimer ces journaux du BIOS avec la console matérielle.

Note Il vous est conseillé de contrôler vos serveurs avec la console iCare. Les journaux du BIOS sont alors rassemblés dans la base de données de la console iCare. Vous pouvez lire, supprimer et restaurer la base de données avec l'interface de la console iCare. Les journaux du BIOS sont gérés par la console iCare et supprimés de l'EMM.



AVERTISSEMENT

N'utilisez pas cette fonction de la console matérielle pour gérer les journaux du BIOS si votre serveur est contrôlé par la console iCare.

Vous pouvez interroger les journaux du BIOS pour aider à l'analyse de pannes matérielles ou à une maintenance préventive.

dans le cas d'ERREURS NON CORRECTIBLES ou d'ERREURS FATALES détectées par le processeur de la ressource, le BIOS journalise tous les registres contenant CORRECTABLE ERROR (Erreur correctible), UNCORRECTABLE ERROR (Erreur incorrectible), or FATAL ERRORS (Erreurs fatales).

Note Pas plus de 15 UNCORRECTABLE ERRORS (Erreurs incorrectibles) et 6 FATAL ERRORS (Erreurs fatales) ne sont collectées par les journaux EMM. Les erreurs supplémentaires sont perdues.

Prérequis

Vous avez la permission Log View (Consultation des journaux)

Procédure

1. Depuis l'onglet Maintenance, cliquez sur Maintenance Operations > BIOS Logs (Opérations de maintenance – Journaux du BIOS) pour ouvrir la page BIOS Logs (Journaux du BIOS).

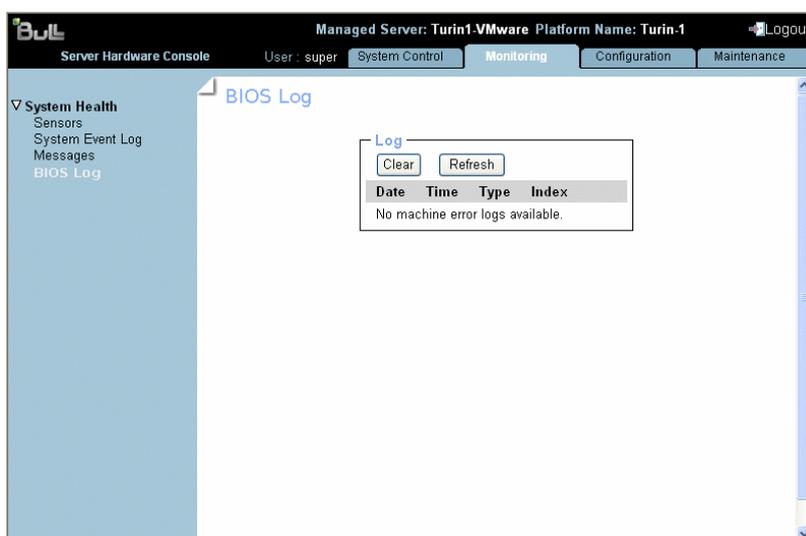


Figure 5-4. Journaux du BIOS

Chapitre 6. Configuration du contrôleur de gestion intégré du serveur

Ce chapitre explique comment configurer le contrôleur de gestion intégré du serveur en fonction de votre environnement de travail. Il comprend les rubriques suivantes :

- Configuration des paramètres d'identification de la plateforme, page 6-2
- Configuration du nom du serveur géré, page 6-3
- Modification des paramètres du profil fonctionnel, page 6-4
- Configuration des paramètres réseau pour l'accès à distance, page 6-6
- Modification des paramètres de l'horloge interne, page 6-10
- Configuration du journal des messages Board & Security, page 6-12
- Gestion des groupes, des utilisateurs et des permissions, page 6-14
- Configuration des paramètres de sécurité, page 6-37
- Configuration de la transmission d'alertes, page 6-50



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

6.1. Configuration des paramètres d'identification de la plateforme



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Chaque tiroir doit avoir une identification et un nom de plateforme unique pour une identification facile et fiable par les logiciels de gestion et de maintenance tels que Bull System Manager (BSM) et iCare.

Prérequis

Vous avez la permission Network Settings (Paramètres réseau)

Procédure

1. Depuis l'onglet Configuration, cliquez sur Global Settings > Platform (Paramètres globaux - Plateforme) pour ouvrir la page Platform Settings (Paramètres plateforme).

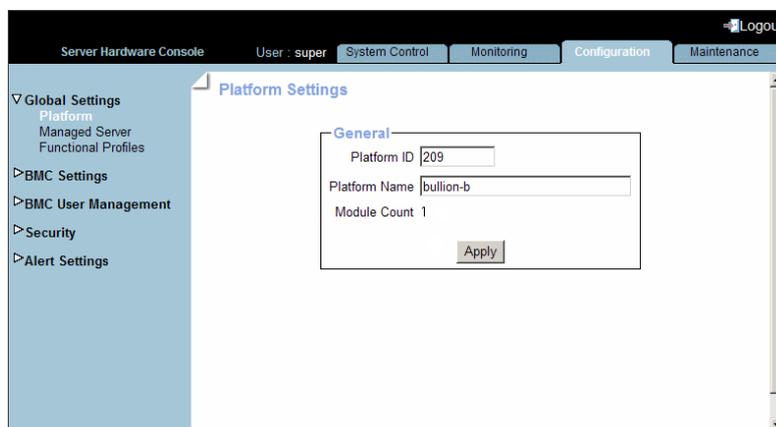


Figure 6-1. Platform Settings (Paramètres plateforme)

2. Complétez les champs puis cliquez sur Apply (Appliquer).

Note Le champ Module Count est en lecture seule.

6.2. Configuration du nom du serveur géré



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Prérequis

Vous avez la permission Network Settings (Paramètres réseau)

Procédure

1. Depuis l'onglet Configuration, cliquez sur Global Settings > Platform (Paramètres globaux - Plateforme) pour ouvrir la page Platform Settings (Paramètres plateforme).

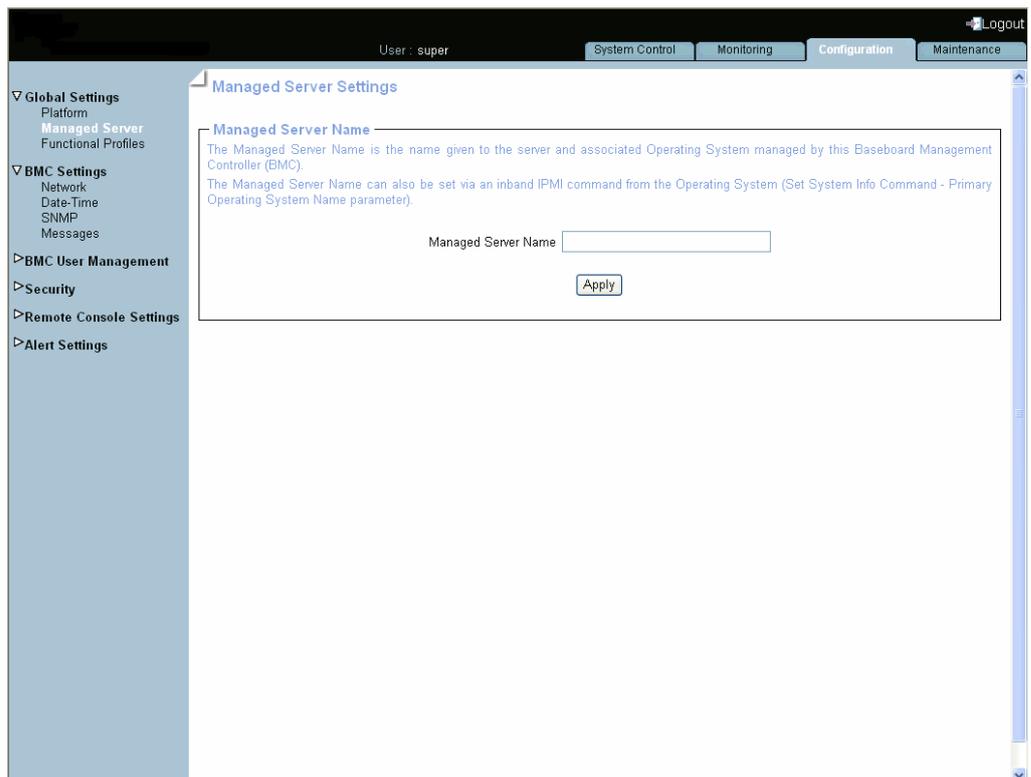


Figure 6-2. Managed Server Settings (Paramètres du serveur géré)

2. Complétez les champs puis cliquez sur Apply (Appliquer).

6.3. Modification des paramètres du profil fonctionnel



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Un profil fonctionnel est un ensemble de paramètres définissant la stratégie de restauration de l'alimentation et l'usage de la vitesse maximum des ventilateurs au démarrage du système. Vous pouvez définir jusqu'à deux profils fonctionnels (0 ou 1) pour votre système et sélectionner l'un ou l'autre au démarrage.

Note Quand l'état d'alimentation du système est ON, le profil fonctionnel actuel est affiché mais ne peut pas être modifié.

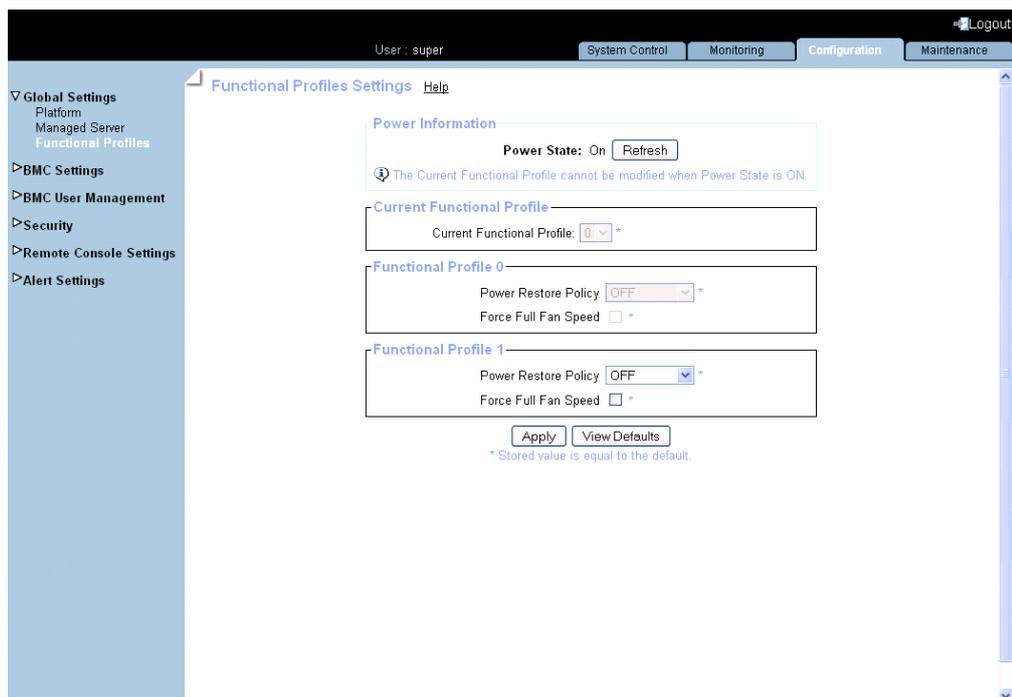
Prérequis

Le système est arrêté

Vous avez la permission Network Settings (Paramètres réseau)

Procédure

1. Depuis l'onglet Configuration, cliquez sur Global Settings > Functional Profiles (Paramètres globaux - Profils fonctionnels) pour ouvrir la page Functional Profiles Settings (Paramètres profils fonctionnels).



Boîte Power Information (Informations sur l'alimentation)	
Power State (État de l'alimentation)	2 valeurs possibles : <ul style="list-style-type: none"> • On (démarré) • Off (arrêté)
Bouton Refresh (Rafraîchir)	Permet de mettre à jour les données affichées.
Boîte Current Functional Profile (Profil fonctionnel actuel)	
Liste déroulante Current Functional Profile (Profil fonctionnel actuel)	Utilisez la liste déroulante pour définir un profil fonctionnel ou pour sélectionner le profil fonctionnel que vous souhaitez appliquer au prochain démarrage. Note : Quand l'état d'alimentation du système est ON (démarré), le profil fonctionnel actuel est affiché mais ne peut pas être modifié.
Boîte Functional Profile <x> (Profil fonctionnel)	
Liste déroulante Power Restore Policy (Stratégie de restauration de l'alimentation)	Utilisez la liste déroulante pour sélectionner la stratégie de restauration de l'alimentation que vous voulez appliquer au retour du secteur après une coupure : <ul style="list-style-type: none"> • Sélectionnez OFF si vous voulez que le système reste arrêté quand le secteur revient. • Sélectionnez RESTORE si vous voulez que le système revienne au même état que celui dans lequel il se trouvait avant la coupure secteur. • Sélectionnez ON si vous voulez que le système démarre quand le secteur revient.
Case à cocher Force Full Fan Speed (Forcer la vitesse maximum du ventilateur)	Cocher la case pour force la vitesse maximum du ventilateur. Au prochain démarrage, la vitesse du ventilateur sera toujours configurée à la vitesse maximum, sans aucune régulation de la part du firmware.
Bouton View Defaults (Afficher les valeurs par défaut)	Permet d'afficher les valeurs d'usine. Cliquez sur Apply (Appliquer) pour restaurer la configuration d'usine.

Figure 6-3. Paramètres des profils fonctionnels

2. Complétez cette page selon vos besoins puis cliquez sur **Apply** (Appliquer).

6.4. Configuration des paramètres réseau pour l'accès à distance



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

La page Network Settings (Paramètres réseau) permet de configurer ou de modifier les paramètres réseau du contrôleur de gestion intégré pour un accès à distance à la console depuis un ordinateur ou une station de travail avec un navigateur Web.

Prérequis

Vous avez la permission Network Settings (Paramètres réseau)



AVERTISSEMENT

Une bonne connaissance de l'administration des réseaux est nécessaire pour compléter cette page.

Si les nouveaux paramètres réseau sont incorrects, vous pouvez perdre la connexion à la console.

Il est conseillé de noter les paramètres actuels avant de saisir de nouvelles valeurs afin de pouvoir restaurer la connexion à la console en cas de problème.

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC Settings > Network (Paramètres BMC - Réseau) pour ouvrir la page Network Settings (Paramètres réseau).

Server Hardware Console User: super System Control Monitoring Configuration Maintenance Logout

Network Settings

⚠ Changing BMC network settings may result in a loss of the remote connection to the BMC. Please ensure that all the values are correct before applying changes so that you can reconnect remotely to the BMC.

General

IP Auto-Configuration: None

Preferred Host Name (DHCP only):

IP Address:

Subnet Mask: 255.255.255.0

Gateway IP Address:

Primary DNS Server IP Address:

Secondary DNS Server IP Address:

Advanced

Enable TELNET Access *

TELNET Port: 23

Enable SSH Access *

SSH Port: 22

Enable CLP-SSH Access *

CLP-SSH Port: 44

Remote Console & HTTPS Port: 443

HTTP Port: 80

Enable Serial Terminal Access *

Disable Setup Protocol *

Ethernet Interface for Management: MNGO

Network Adapter Configuration

MNGO Network Adapter Configuration

MNGO Ethernet Port for Management: ETH0

Inhibit the PHY Reset of the shared Ethernet Controller *

Apply View Defaults

* Stored value is equal to the default.

Boîte générale	
IP Auto-Configuration (Configuration automatique IP)	<p>Cette liste déroulante permet d'activer ou de désactiver la configuration automatique via un serveur DHCP ou BOOTP :</p> <ul style="list-style-type: none"> • None (Aucune) : La configuration automatique est désactivée. • DHCP : les paramètres réseau sont récupérés depuis un serveur DHCP (valeur d'usine). • BOOTP : les paramètres réseau sont récupérés depuis un serveur BOOTP.
Preferred host name (DHCP only) (Nom de l'hôte préféré (uniquement DHCP))	Accessible uniquement si DHCP est sélectionné. Le nom d'hôte que vous voulez communiquer au serveur DHCP.
IP Address (Adresse IP)	Accessible uniquement si None (Aucune) est sélectionnée. L'adresse IP statique que vous voulez utiliser (valeur d'usine : 192.x.x.x).
Subnet Mask (Masque de sous-réseau)	Accessible uniquement si None (Aucune) est sélectionnée. Le masque de sous-réseau que vous voulez utiliser (valeur d'usine : 255.255.255.0).
Gateway IP Address (Adresse IP de la passerelle)	Accessible uniquement si None (Aucune) est sélectionnée. Votre adresse IP de la passerelle par défaut, le cas échéant.
Primary DNS Server IP Address (Adresse IP du serveur DNS principal)	Accessible uniquement si None (Aucune) est sélectionnée. Votre adresse IP du serveur DNS principal, le cas échéant.
Secondary DNS Server IP Address (Adresse IP du serveur DNS secondaire)	Accessible uniquement si None (Aucune) est sélectionnée. Votre adresse IP du serveur DNS secondaire, le cas échéant.
Boîte Advanced (Avancé)	
Enable TELNET Access (Activer l'accès TELNET)	Sélectionnez cette option pour permettre une connexion en utilisant un client Telnet . Vous devez avoir la permission SSH/Telnet Access (Accès SSH/Telnet).
TELNET Port (Port TELNET)	Le numéro de port Telnet (valeur d'usine : 23).
Enable SSH Access (Activer l'accès SSH)	Sélectionnez cette option pour permettre une connexion en utilisant un client SSH . Vous devez avoir la permission SSH/Telnet Access (Accès SSH/Telnet).
SSH Port (Port SSH)	Le numéro du port Secure Shell (SSH) (valeur d'usine : 22).
Enable CLP-SSH Access (Activer l'accès CLP-SSH)	Sélectionnez cette option pour permettre une connexion à partir d'une invite de ligne de commande SSH (CPL). Vous devez avoir la permission SSH/Telnet Access (Accès SSH/Telnet).
CLP-SSH Port (Port CLP-SSH)	Le numéro de port CLP-SSH (valeur d'usine : 44).

Boîte Advanced (Avancé)	
Remote Console & HTTPS Port (console distante et port HTTPS)	Le numéro du port utilisé pour les connexions standard HTTPS, (valeur usine par défaut : 443).
HTTP Port (Port HTTP)	Le numéro du port utilisé pour les connexions standard HTTP (valeur d'usine : 80).
Enable Serial Terminal Access (Activer l'accès Terminal série)	Sélectionnez cette option pour ouvrir une connexion Telnet au port série du serveur pour connecter le serveur en mode terminal. Vous devez avoir la permission SSH/Telnet Access (Accès SSH/Telnet).
Disable Setup Protocol (Désactiver le protocole d'installation)	Sélectionnez cette option pour empêcher l' <i>outil psetup (Windows)</i> et/ou l' <i>outil mc-setup (Linux)</i> , utilisés pour découvrir le serveur sur le réseau pendant la première installation, de re-détecter ce serveur quand vous installez de nouveaux serveurs.
Ethernet Interface for Management (Interface Ethernet pour la gestion)	Le numéro de port Ethernet utilisé pour connecter le contrôleur de gestion intégré au réseau local d'entreprise (LAN). Par défaut, le port Ethernet ETH0/MNG0 est utilisé : Le réseau de gestion et le réseau hôte partagent cette connexion et le câble réseau est connecté au port Ethernet ETH0/MNG0. Autrement, vous pouvez séparer le réseau de gestion et le réseau hôte en utilisant le port Ethernet INTER/MNG1 pour le réseau de gestion et le port Ethernet MNG0 pour le réseau hôte. Dans ce cas, sélectionnez MNG1, puis connectez le câble du réseau de gestion au port Ethernet INTER/MNG1 et le câble du réseau hôte au port Ethernet MNG0.
Configuration de l'adaptateur réseau MNG0	
MNG0 Ethernet Port for Management (Port Ethernet MNG0 pour la gestion)	Sélectionnez le port Ethernet ETH0 ou ETH1
Inhibit the PHY Reset of the shared Ethernet Controller (Inhiber a réinitialisation PHY du contrôleur Ethernet partagé)	Sélectionnez cette option pour empêcher le contrôleur Ethernet d'être réinitialisé quand le serveur est réinitialisé.
Configuration de l'adaptateur réseau MNG1	
Current Parameters (Paramètres actuels)	Affiche les paramètres actuels du réseau.
Speed (Vitesse)	Vitesse de l'interface LAN <ul style="list-style-type: none"> • Autodetect (Détection automatique) : ajuste automatiquement la vitesse de l'interface (valeur d'usine). • 10Mbps : vitesse fixée en fonction du réseau. • 100Mbps : vitesse fixée en fonction du réseau. Autodetect (Détection automatique) est sélectionnée par défaut. Si vous rencontrez des problèmes de connexion, sélectionnez la valeur fixée correspondant à votre infrastructure réseau.

Configuration de l'adaptateur réseau MNG1	
Duplex Mode (Mode duplex)	<p>Interface LAN en mode duplex.</p> <ul style="list-style-type: none"> • Autodetect (Détection automatique) : configure automatiquement le mode duplex requis par votre infrastructure réseau (valeur d'usine). • Half Duplex : mode duplex fixé en fonction du réseau. • Full Duplex : mode duplex fixé en fonction du réseau. <p>Autodetect (Détection automatique) est sélectionnée par défaut. Si vous rencontrez des problèmes de connexion, sélectionnez la valeur duplex correspondant à votre infrastructure réseau.</p>
Bouton View Defaults (Afficher les valeurs par défaut)	Permet d'afficher les valeurs d'usine. Cliquez sur Apply (Appliquer) pour restaurer la configuration d'usine.

Note * Suivant le modèle de serveur et la configuration réseau, les deux boîtes **MNGx Network Adapter Configuration** (Configuration de l'adaptateur réseau MNGx) peuvent ne pas être visibles.

Figure 6-4. Paramètres réseau - valeurs d'usine

2. Complétez cette page selon vos besoins puis cliquez sur **Apply** (Appliquer).
3. Déconnectez la console.
4. Démarrez la console avec la nouvelle configuration réseau depuis un ordinateur distant ou une station de travail distante pour tester la connexion.
5. Utilisez l'utilitaire **KiraTool**, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

Que faire en cas d'incident ?

Si vous ne pouvez pas vous connecter à la console depuis un ordinateur distant ou une station de travail distante, un des problèmes suivants peut en être la cause :

- Le câble réseau peut être débranché.
- La configuration du réseau n'est pas correcte.
- Le réseau peut être arrêté.

6.5. Modification des paramètres de l'horloge interne



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

La page Date/Time Settings (Paramètres Date/Heure) permet de configurer l'horloge interne du contrôleur de gestion intégré. Vous pouvez configurer l'horloge manuellement ou vous connecter à un serveur Network Time Protocol (NTP) (Protocole d'heure réseau).



AVERTISSEMENT

Si vous n'utilisez pas un serveur NTP, la date et l'heure ne seront pas persistantes. En cas de coupure secteur, vous devrez réinitialiser la date et l'heure.

Prérequis

Vous avez la permission Date/Time Settings (Paramètres Date/Heure)

Si vous voulez utiliser NTP, vous devez disposer des adresses IP des serveurs NTP que vous désirez utiliser

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC Settings > Date-Time (Paramètres BMC – Date-Heure) pour ouvrir la page Date/Time Settings (Paramètres date/heure).

The screenshot shows the BMC web interface. At the top, there's a navigation bar with 'User: super', 'System Control', 'Monitoring', 'Configuration', and 'Maintenance'. The 'Configuration' tab is active. On the left, a sidebar lists settings categories: Global Settings (Platform, Managed Server, Functional Profiles), BMC Settings (Network, Date-Time, SNMP, Messages), BMC User Management, Security, Remote Console Settings, and Alert Settings. The 'Date-Time' option under BMC Settings is selected. The main content area is titled 'Date/Time Settings' and contains a 'General' section with the following fields:

- Time Zone: (GMT +00:00) England, Ireland, Portugal (dropdown menu)
- Adjust for daylight savings time *
- User Specified Time *
- Date (Month, Day, Year): October 27, 2009
- Time: 17 : 32 : 32 (hh:mm:ss)
- Synchronize with NTP server
- Primary Time Server: [text input]
- Secondary Time Server: [text input]

At the bottom of the form, there are 'Apply' and 'View Defaults' buttons. Below the buttons, a note states: '* Stored value is equal to the default.'

Général	
Time Zone (Fuseau horaire)	Utilisez cette liste déroulante pour définir la différence entre l'heure locale et l'heure universelle.
Adjust for daylight savings time (Ajuster à l'heure d'été)	Sélectionnez cette option pour ajuster automatiquement l'heure locale (DST).
User Specified Time (Heure spécifiée par l'utilisateur)	Cette option vous permet de configurer manuellement l'horloge interne du serveur. Entrez manuellement la date et l'heure locales et vérifiez que la valeur de l'écart UTC soit correcte.
Synchronize with NTP Server (Synchroniser avec le serveur NTP)	Cette option vous permet d'entrer les adresses IP des serveurs NTP que vous voulez utiliser. Vous devez utiliser la liste déroulante Time Zone (Fuseau horaire).
Bouton View Defaults (Afficher les valeurs par défaut)	Permet d'afficher les valeurs d'usine.

Figure 6-5. Paramètres Date/Heure - valeurs d'usine

2. Si nécessaire, changez la valeur Time Zone (Fuseau horaire) et cochez ou décochez la case Adjust for daylight savings time (Régler l'heure d'été).
3. Cliquez, soit sur User Specified (Spécifié par l'utilisateur), soit sur Synchronize with NTP Server (Synchroniser avec le serveur NTP), complétez les champs appropriés puis cliquez sur Apply (Appliquer).
4. Utilisez l'utilitaire KiraTool, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

6.6. Configuration du journal des messages Board & Security



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Cette section décrit comment configurer le journal des messages Board & Security, qui enregistre les événements non IPMI, telles que les erreurs de démarrage, les authentifications des utilisateurs, les connexions, la violation de sécurité, la suppression de journal ou la mise à jour du firmware.

Note Les événements conformes au standard IPMI sont enregistrés dans le journal SEL. Vous pouvez configurer les règles de la messagerie SEL avec Alert Settings (Configuration des alertes).



Important La transmission des alertes et des messages à la console iCare doit être configurée directement depuis l'interface de la console iCare. Consultez le manuel *iCare Console User's Guide* pour plus de détails.

Prérequis

Vous avez la permission Log Settings (Paramètres journaux)

Vous avez configuré votre serveur SMTP / SNMP pour la messagerie

Vous avez configuré votre serveur SMTP / SNMP pour la messagerie

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC Settings > Messages (Paramètres BMC - Messages) pour ouvrir la page Event Management - Settings (Paramètres – Gestion des événements) :

The screenshot shows the 'Event Management - Settings' page in a web interface. The top navigation bar includes 'User: super', 'Power Control', 'Monitoring', 'Configuration', and 'Logout'. The left sidebar menu has 'General Settings' (BCE Blade, Network, Date-Time, SNMP, Messages, FPIF Image Selection), 'User Management', 'Security Management', and 'Alert Settings'. The main content area is titled 'Event Management - Settings' and contains two configuration sections:

- SNMP Configuration:** Includes a checkbox for 'SNMP Logging Enabled *'. Below it is a table with three columns: 'Destination IP', 'Port #', and 'Community'. The table contains five rows, each with '162' in the Port # column and 'public' in the Community column. A link below the table reads 'Click here to view the kira100 SNMP MIB'.
- SysLog Configuration:** Includes a checkbox for 'Enable Syslog Forwarding *' and a text input field for 'IP Address'.

At the bottom of the configuration area are 'Apply' and 'View Defaults' buttons, and a note: '* Stored value is equal to the default.'

Configuration SNMP	
SNMP Logging Enabled (Connexion SNMP validée)	Quand elle est sélectionnée, cette option permet d'envoyer des messages Board & Security par interruptions SNMP.
Destination IP (IP de destination)	Adresse IP et numéro de port du gestionnaire SNMP
Port # (Port N°)	
Community (Communauté)	Nom de la communauté SNMP pour le gestionnaire SNMP (exemple : public)
Click here to view ... link (Lien Cliquez ici pour afficher ...)	Ce lien permet d'afficher et d'enregistrer en tant que fichier .txt le fichier système MIB. Ce fichier est nécessaire au gestionnaire SNMP pour interpréter les messages d'interruption.
Configuration SysLog	
Enable Syslog Forwarding (Activer la transmission Syslog)	Quand cette option est sélectionnée, elle permet l'envoi des messages Board & Security par le protocole syslog, afin de permettre la centralisation des journaux Board & Security sur une plate-forme Linux.
IP Address (Adresse IP)	Adresse IP de la plate-forme Linux.

Figure 6-6. Paramètres de gestion d'événements - valeurs d'usine

2. Complétez les champs demandés.
3. Cliquez sur **Apply** (Appliquer).
4. Utilisez l'utilitaire **KiraTool**, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

6.7. Gestion des utilisateurs



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

L'accès aux fonctions et données de la console est basé sur les utilisateurs, les groupes et les permissions. Depuis l'onglet Configuration, utilisez le menu User Management (Gestion des utilisateurs) pour mettre en place une politique de gestion des utilisateurs basée sur des permissions, permettant à ces utilisateurs de n'accéder qu'aux fonctions et aux données dont ils ont besoin.

6.7.1. Création d'un compte utilisateur



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Le serveur est livré avec deux groupes prédéfinis et un utilisateur prédéfini :

- Le groupe Admin doté de toutes les permissions pour un accès complet au système et un super utilisateur par défaut.
- groupe users sans permissions et sans utilisateurs prédéfinis.

Vous pouvez créer et gérer des utilisateurs et des permissions associées selon vos besoins.

Note Les groupes et les utilisateurs prédéfinis ne peuvent pas être renommés ou supprimés, mais le mot de passe du super utilisateur par défaut peut être changé. Les permissions pour le groupe Admin par défaut ne sont pas modifiables. Les permissions pour le groupe users par défaut sont modifiables.



Important Le système est équipé d'un processeur indépendant de l'hôte et d'une unité mémoire qui sont limités en termes d'instructions de traitement et d'espace mémoire. Pour garantir un temps de réponse acceptable, il vous est demandé de :

- Ne pas dépasser 25 connexions utilisateurs simultanées.
 - Ne pas dépasser 150 comptes utilisateurs.
-

Prérequis

Vous avez la permission User/Group Management (Gestion utilisateurs/groupes)

Vous avez créé le groupe dont l'utilisateur doit être membre

Note Si vous n'avez pas créé le groupe dont l'utilisateur doit être membre, l'utilisateur nouvellement créé sera lié au groupe users prédéfini.

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC User Management > Users (BMC Gestion des utilisateurs - Utilisateurs) pour afficher la page User Management (Gestion des utilisateurs).
2. Cliquez sur Create (Créer) pour afficher la boîte de dialogue User Creation (Création d'utilisateur).

The screenshot shows the BMC User Management interface. On the left is a navigation tree with categories like Global Settings, BMC Settings, BMC User Management, Security, Remote Console Settings, and Alert Settings. The main area is titled 'User Management' and contains two panels. The top panel, 'General', shows a list of 'User Accounts' with 'super' listed and buttons for 'Create', 'Modify', and 'Delete'. The bottom panel, 'User Creation', contains the following fields and options:

- User Name * (text input)
- Full User Name (text input)
- Password * (text input, with note '(min length:4)')
- Confirm Password * (text input)
- Group Membership: users (default setting) (dropdown menu)
- Email Address (text input)
- Phone Number (text input)
- User must change password at next logon. (Note that the Change Password permission must be enabled for the group)
- Account is enabled
- Buttons: Create, Cancel
- * Mandatory

User Creation (Création d'un utilisateur)

User Name (Nom d'utilisateur)	<p>Nom que l'utilisateur utilisera pour se connecter (souvent un "nom court").</p> <ul style="list-style-type: none"> • Nom limité à 32 caractères. • Les caractères suivants ne sont pas admis : "'`&*&#37; ~?/ et l'espace.
Full User Name (Nom d'utilisateur complet)	<p>Le nom complet de l'utilisateur.</p> <ul style="list-style-type: none"> • Nom limité à 32 caractères. • Les caractères suivants ne sont pas admis : "'`&*&#37; ~?/ et l'espace.
Password (Mot de passe)	<p>Le mot de passe que l'utilisateur utilisera pour se connecter.</p>
Confirm Password (Confirmer le mot de passe)	<ul style="list-style-type: none"> • Longueur minimum du mot de passe : 4 caractères. • Longueur maximum du mot de passe : 32 caractères. • Le caractère suivant n'est pas admis : espace.

User Creation (Création d'un utilisateur)	
Group Membership (Appartenance au groupe)	Utilisez cette liste déroulante pour sélectionner le groupe dont cet utilisateur va être membre, selon les permissions que vous voulez donner à l'utilisateur. Note : Si vous ne sélectionnez pas un groupe, l'utilisateur nouvellement créé est lié automatiquement au groupe d'utilisateurs prédéfini. La permission Change Password (Changer le mot de passe) n'est pas activée pour le groupe d'utilisateurs prédéfini.
Email Address (Adresse mail)	Adresse mail de l'utilisateur. Exemple : john.smith@acme.com.
Phone Number (Numéro de téléphone)	Numéro de téléphone de l'utilisateur N'utilisez que des chiffres et optionnellement les caractères .+ sans espace. Exemples : 0625252525, +33.1.25.25.25
User must change password at next logon (L'utilisateur doit changer de mot de passe à la prochaine connexion)	Quand cette option est cochée, elle force l'utilisateur à changer son mot de passe à la prochaine connexion. Note : La permission Change Password (Changer de mot de passe) doit être activée pour le groupe sinon l'utilisateur ne pourra plus se connecter.
Account is enabled (Le compte est activé)	Quand cette option est décochée, elle rend le compte utilisateur indisponible : les informations sur le compte utilisateur sont conservées mais il n'est plus possible de se connecter avec ce compte.

Figure 6-7. Gestion des utilisateurs – Création d'un utilisateur

3. Complétez les champs demandés.
4. Cliquez sur **Apply** (Appliquer). L'utilisateur est créé et apparaît dans la boîte **User Accounts** (Comptes utilisateurs).
5. Utilisez l'utilitaire **KiraTool**, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

6.7.2. Affichage des détails des comptes utilisateurs



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Pour faciliter la gestion des utilisateurs, vous pouvez afficher les informations de base d'un compte utilisateur à tout moment. Vous pouvez vouloir utiliser cette fonctionnalité, par exemple, pour vérifier les informations d'un compte utilisateur après sa création ou sa modification ou pour vérifier si un utilisateur est ou n'est pas verrouillé.

Prérequis

Vous avez la permission User/Group Management (Gestion utilisateurs/groupes)

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC User Management > Users (BMC Gestion des utilisateurs - Utilisateurs) pour afficher la page User Management (Gestion des utilisateurs).
2. Dans la liste User Accounts (Comptes utilisateurs), sélectionnez un utilisateur pour afficher la boîte Account Details (Détails du compte).

The screenshot displays the BMC User Management web interface. The top navigation bar includes 'System Control', 'Monitoring', 'Configuration', and 'Maintenance'. The left sidebar shows a tree view with categories like 'Global Settings', 'BMC Settings', 'BMC User Management', 'Security', 'Remote Console Settings', and 'Alert Settings'. The main content area is titled 'User Management' and contains a 'General' section with a 'User Accounts' table. The table has one entry for the user 'super'. Below the table are 'Create', 'Modify', and 'Delete' buttons. The 'Account Details' section for the 'super' user shows the following information:

User name:	super
Full user name:	Supervisor
Group membership:	Admin
<input type="checkbox"/>	User must change password at next logon
<input checked="" type="checkbox"/>	Account is enabled

Below the details, a status message reads: 'This user is not locked out and may log on.'

Account Details (Détails du compte)	
User Name (Nom d'utilisateur)	Nom que l'utilisateur utilise pour se connecter (souvent un "nom court").
Full User Name (Nom d'utilisateur complet)	Le nom complet de l'utilisateur.
Group membership (Appartenance au groupe)	Groupe dont l'utilisateur est membre (et par conséquent les permissions que l'utilisateur possède).
Email Address (Adresse mail)	Adresse mail de l'utilisateur. Cette entrée n'apparaît pas si le champ n'est pas rempli quand l'utilisateur est créé.
Phone Number (Numéro de téléphone)	Numéro de téléphone de l'utilisateur Cette entrée n'apparaît pas si le champ n'est pas rempli quand l'utilisateur est créé.
User must change password at next logon (L'utilisateur doit changer de mot de passe à la prochaine connexion)	Quand cette option est cochée, elle force l'utilisateur à changer son mot de passe à la prochaine connexion. Note : La permission Change Password (Changer de mot de passe) doit être activée pour le groupe sinon l'utilisateur ne pourra plus se connecter.
Account is enabled (Le compte est activé)	Quand cette case est cochée, le compte utilisateur est actif et l'utilisateur peut se connecter.

Figure 6-8. Gestion des utilisateurs - Détails du compte

6.7.3. Modification d'un compte utilisateur



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Vous pouvez éditer les informations d'un compte utilisateur à tout moment.

6.7.3.1. Mise à jour des détails

Vous pouvez changer les détails d'un compte utilisateur (nom d'utilisateur, nom d'utilisateur complet, mot de passe, adresse mail et numéro de téléphone) à tout moment. Vous pouvez vouloir le faire, par exemple, si un nom de ressource est changé ou si une ressource change de rôle dans votre organisation.

Note Vous ne pouvez pas changer les détails du compte de l'utilisateur **super** prédéfini. Cependant, le mot de passe par défaut de l'utilisateur **super** peut être changé via la page **Password Management** (Gestion des mots de passe), comme expliqué dans **Modification du mot de passe**, page 6-26

Prérequis

Vous avez la permission **User/Group Management** (Gestion utilisateurs/groupes)

Procédure

1. Depuis l'onglet **Configuration**, cliquez sur **BMC User Management > Users** (BMC Gestion des utilisateurs - Utilisateurs) pour afficher la page **User Management** (Gestion des utilisateurs).
1. Depuis l'onglet **Configuration**, cliquez sur **> Users** (Utilisateurs) pour afficher la page **User Management** (Gestion des utilisateurs).
2. Sélectionnez le compte utilisateur que vous voulez modifier dans la liste **User Accounts** (Comptes utilisateurs) puis cliquez sur **Modify** (Modifier) pour ouvrir la boîte **User Account Modification** (Modification d'un compte utilisateur).
3. Modifiez un (ou plusieurs) des champs suivants selon vos besoins :
 - **User Name** (Nom d'utilisateur),
 - **Full User Name** (Nom d'utilisateur complet),
 - **Password** (Mot de passe) et **Confirm Password** (Confirmer le mot de passe),
 - **Email Address** (Adresse mail),
 - **Phone Number** (Numéro de téléphone).

Note Pour plus d'informations sur ces champs, voir Figure 6-7, page 6-16.

4. Cliquez sur **Modify** (Modifier). Les détails du compte utilisateur sont changés.
5. Utilisez l'utilitaire **KiraTool**, fourni sur le CD **Resource and Documentation**, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir **Sauvegarde des données de configuration**, page 7-13.

6.7.3.2. Changement de groupe

Un groupe est un ensemble d'utilisateurs qui ont les mêmes permissions. Les utilisateurs héritent automatiquement des permissions du groupe dont ils sont membres. Vous pouvez changer les permissions attribuées aux utilisateurs en changeant le groupe dont ils sont membres.

Prérequis

Le groupe doit être créé

Vous avez la permission User/Group Management (Gestion utilisateurs/groupes)

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC User Management > Users (BMC Gestion des utilisateurs - Utilisateurs) pour afficher la page User Management (Gestion des utilisateurs).
2. Sélectionnez le compte utilisateur que vous voulez modifier dans la liste User Accounts (Comptes utilisateurs) puis cliquez sur Modify (Modifier) pour ouvrir la boîte User Account Modification (Modification d'un compte utilisateur).
3. Sélectionnez dans la liste déroulante Group Membership (Membres du groupe) le groupe souhaité, en fonction des permissions que vous voulez donner à l'utilisateur.
4. Cliquez sur Modify (Modifier). Le groupe auquel l'utilisateur appartient est mis à jour.
5. Utilisez l'utilitaire KiraTool, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

6.7.4. Désactivation/Activation des comptes utilisateurs



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Parfois, vous pouvez vouloir rendre des comptes utilisateurs indisponibles. Vous pouvez vouloir utiliser cette fonctionnalité, par exemple, lorsqu'une intervention de maintenance est planifiée. Quand vous désactivez un compte utilisateur, les informations sur ce compte utilisateur sont conservées mais l'utilisateur ne peut plus se connecter. Le compte utilisateur reste inactif jusqu'à ce qu'il soit réactivé.

Prérequis

Vous avez la permission User/Group Management (Gestion utilisateurs/groupes)

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC User Management > Users (BMC Gestion des utilisateurs - Utilisateurs) pour afficher la page User Management (Gestion des utilisateurs).
2. Sélectionnez le compte utilisateur que vous voulez modifier dans la liste User Accounts (Comptes utilisateurs) puis cliquez sur Modify (Modifier) pour ouvrir la boîte User Account Modification (Modification d'un compte utilisateur).
3. Pour désactiver le compte, décochez la case Account is enabled (Le compte est activé) ; pour activer le compte, cochez la case.
4. Cliquez sur Modify (Modifier). Le compte est mis à jour.
5. Utilisez l'utilitaire KiraTool, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

6.7.5. Forçage du changement du mot de passe utilisateur



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

La procédure suivante décrit comment forcer un utilisateur à changer son mot de passe à la prochaine connexion.

Prérequis

Vous avez la permission User/Group Management (Gestion utilisateurs/groupes)

Le groupe a la permission Change Password (Changement de mot de passe)

Procédure

1. Vérifiez que la permission Change Password (Changement de mot de passe) est activée pour le groupe auquel appartient l'utilisateur.
 - a. Depuis l'onglet Configuration, cliquez sur User Management > Groups (Gestion des utilisateurs - Groupes) pour afficher la page Group Management (Gestion des groupes).
 - b. Sélectionnez le groupe auquel appartient l'utilisateur et cliquez sur Permissions pour afficher la page Group Permissions (Permissions du groupe).
 - c. Vérifiez que la permission Change Password (Changement de mot de passe) est activée pour le groupe. Si ce n'est pas le cas, activez la permission Change Password (Changement de mot de passe) pour le groupe.

2. Depuis l'onglet Configuration, cliquez sur User Management > Users (Gestion des utilisateurs - Utilisateurs) pour afficher la page User Management (Gestion des utilisateurs).
3. Sélectionnez le compte utilisateur que vous voulez modifier dans la liste User Accounts (Comptes utilisateurs) puis cliquez sur Modify (Modifier) pour ouvrir la boîte User Account Modification (Modification d'un compte utilisateur).
4. Cochez la case User must change password at next logon (L'utilisateur doit changer de mot de passe à la prochaine connexion).
5. Cliquez sur Modify (Modifier). Il sera demandé à l'utilisateur de changer son mot de passe la prochaine fois qu'il tentera de se connecter.

Note Une fois que l'utilisateur a changé son mot de passe, la case à cocher User must change password at next logon (L'utilisateur doit changer son mot de passe la prochaine connexion) de son compte est décochée automatiquement.

6.7.6. Suppression d'un compte utilisateur



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Vous pouvez supprimer un compte utilisateur lorsqu'il n'est plus utilisé. Le compte utilisateur supprimé sera retiré du groupe associé.

Prérequis

Vous avez la permission User/Group Management (Gestion utilisateurs/groupes)

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC User Management > Users (BMC Gestion des utilisateurs - Utilisateurs) pour afficher la page User Management (Gestion des utilisateurs).
2. Sélectionnez un utilisateur dans la liste User Accounts (Comptes utilisateurs) et cliquez sur Delete (Supprimer). La boîte User Account Deletion (Suppression d'un compte utilisateur) apparaît.

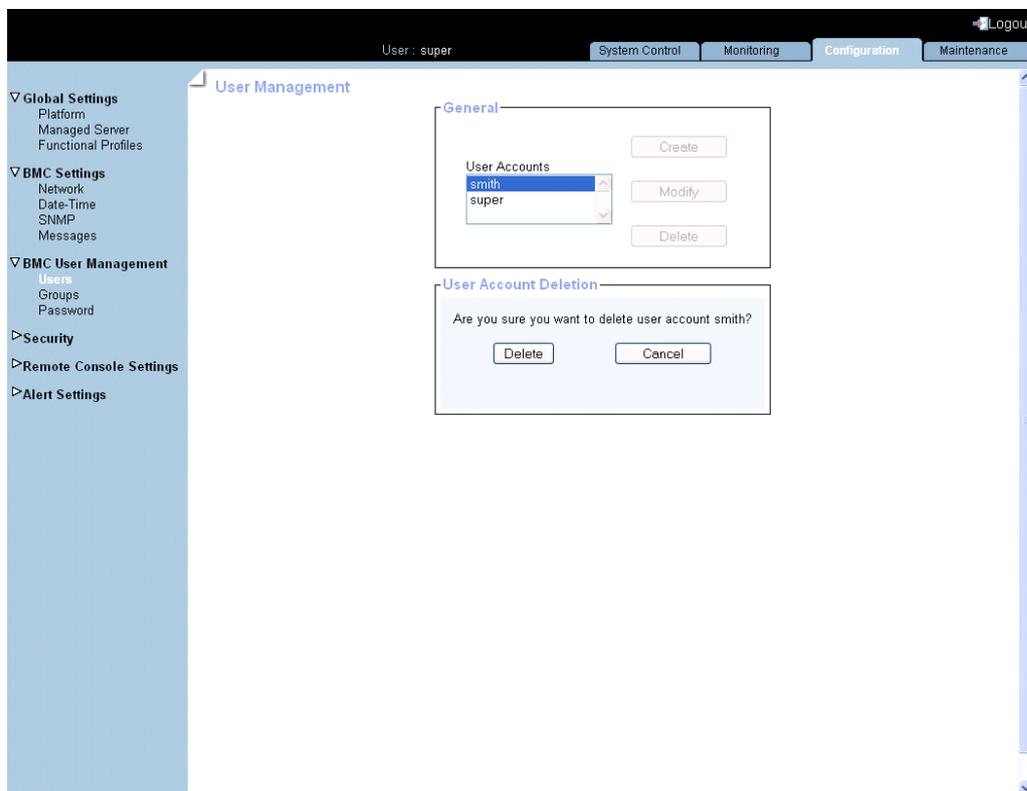


Figure 6-9. User Account Deletion (Suppression d'un compte utilisateur)

3. Cliquez sur Delete (Supprimer) pour confirmer. L'utilisateur est supprimé de la liste et du groupe associé.
4. Utilisez l'utilitaire KiraTool, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

6.7.7. Déverrouillage manuel d'un compte utilisateur



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

La fonction de verrouillage désactive un compte utilisateur si un certain nombre d'échecs de connexion se produit à cause de mots de passe erronés. Si la durée de verrouillage est indiquée, le compte utilisateur est automatiquement déverrouillé après le temps indiqué. Si la durée de verrouillage n'est pas indiquée, le compte utilisateur devra être déverrouillé manuellement.

Prérequis

Vous avez la permission User/Group Management (Gestion utilisateurs/groupes)

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC User Management > Users (BMC Gestion des utilisateurs - Utilisateurs) pour afficher la page User Management (Gestion des utilisateurs).
2. Sélectionnez l'utilisateur verrouillé dans la liste User Accounts (Comptes utilisateurs). Le message suivant est affiché dans la boîte Account Details (Détails du compte).

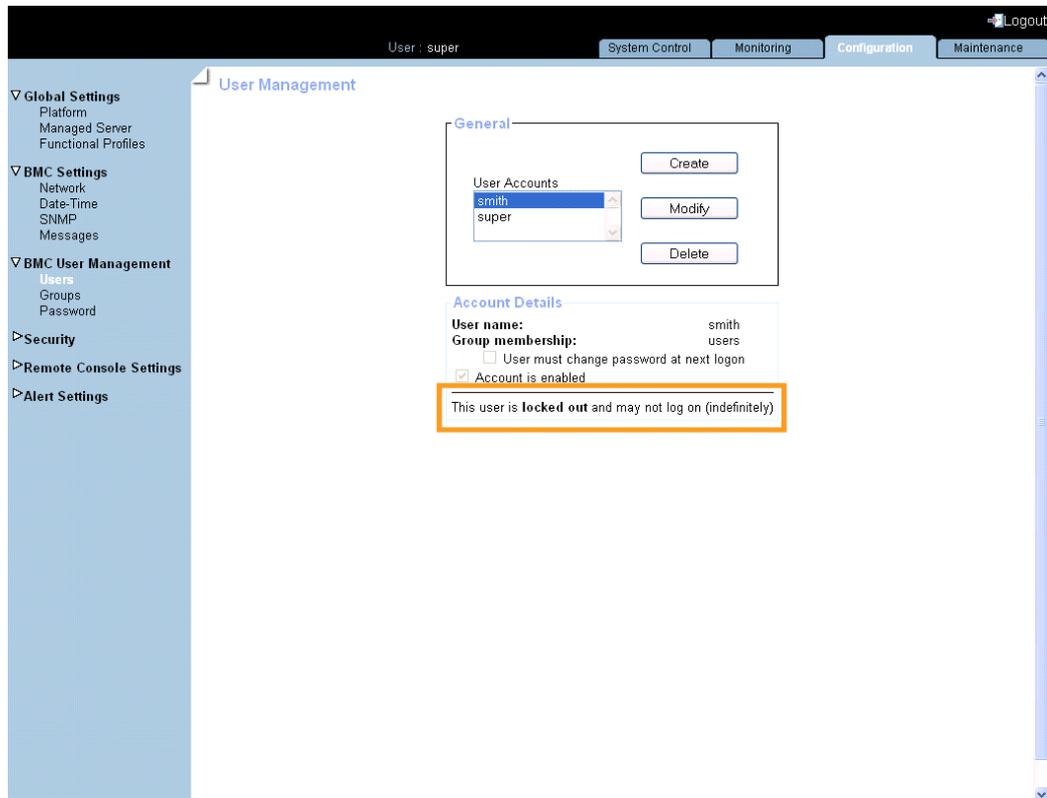
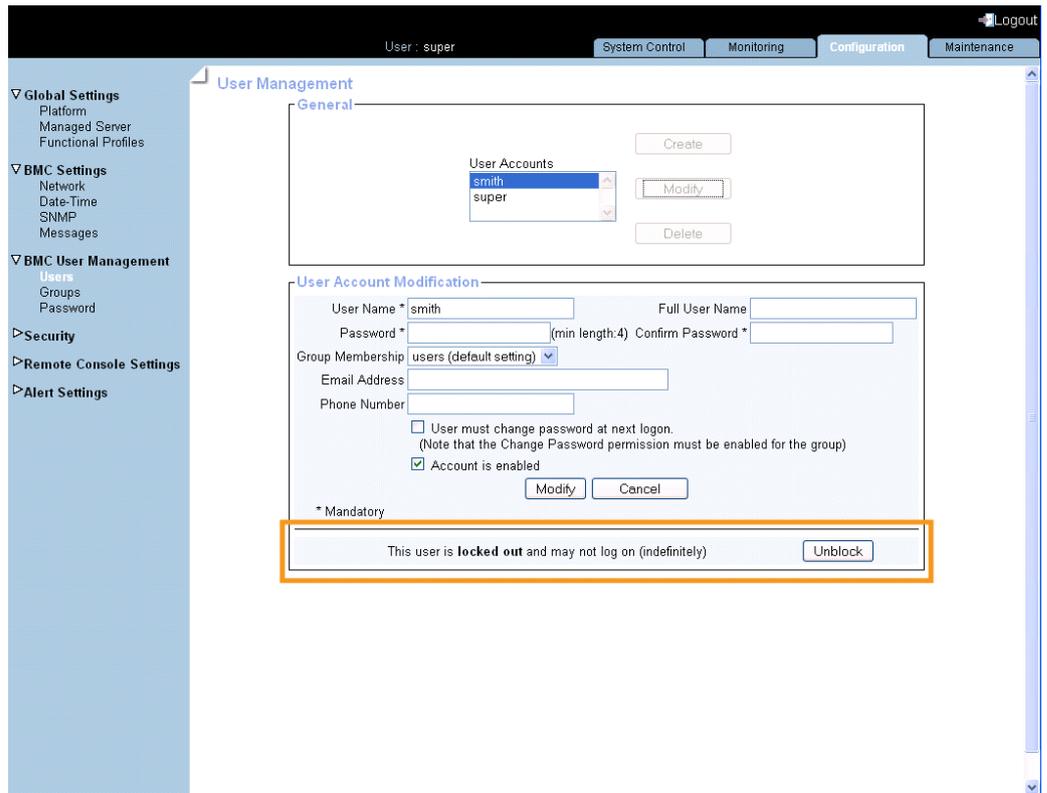


Figure 6-10. Gestion des utilisateurs - Utilisateur verrouillé

3. Cliquez sur **Modify** (Modifier) pour afficher la boîte de dialogue **User Account Modification** (Modification d'un compte utilisateur).



4. Cliquez sur **Unblock** (Débloquer). Le compte utilisateur est déverrouillé et l'utilisateur peut maintenant se reconnecter.

6.7.8. Modification du mot de passe



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

La procédure suivante explique comment changer le mot de passe du compte utilisateur courant.

Prérequis

Vous avez la permission Change Password (Changer le mot de passe)

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC User Management > Password (BMC Gestion des utilisateurs - Mots de passe) pour afficher la page Password Management (Gestion des mots de passe).

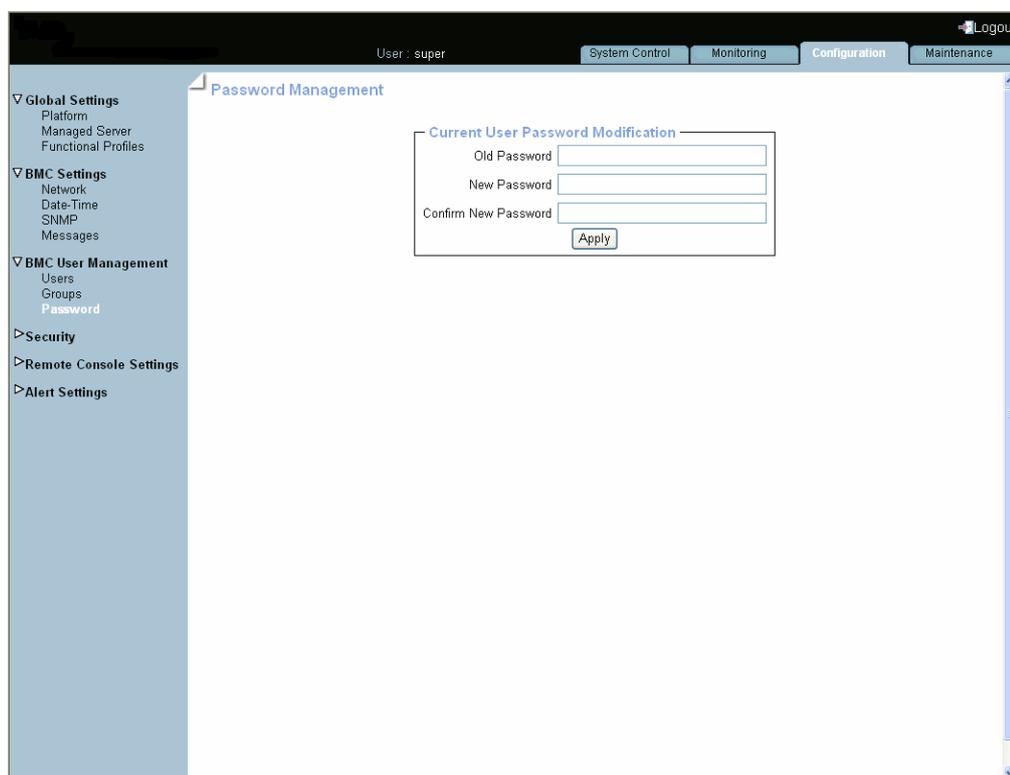


Figure 6-11. Password Management (Gestion des mots de passe)



- Longueur minimum du mot de passe : 4 caractères.
- Longueur maximum du mot de passe : 32 caractères.
- Le caractère 'Espace' est interdit.

2. Complétez les 3 champs.
3. Cliquez sur Apply (Appliquer). Votre nouveau mot de passe est maintenant valide et doit être utilisé pour votre prochaine connexion.

6.7.9. Création d'un groupe



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

La console matérielle est livrée avec deux groupes prédéfinis et un utilisateur prédéfini :

- Le groupe Admin doté de toutes les permissions pour un accès complet au système et un super utilisateur par défaut.
- Le groupe Users sans permission et sans utilisateur prédéfini.

Vous pouvez créer et gérer de nouveaux groupes et des permissions associées pour convenir à vos besoins.



important Les groupes et les utilisateurs prédéfinis ne peuvent pas être renommés ou supprimés, mais le mot de passe du super utilisateur par défaut peut être changé.

Les permissions pour le groupe Admin ne sont pas modifiables.

Les permissions pour le groupe Users sont modifiables.

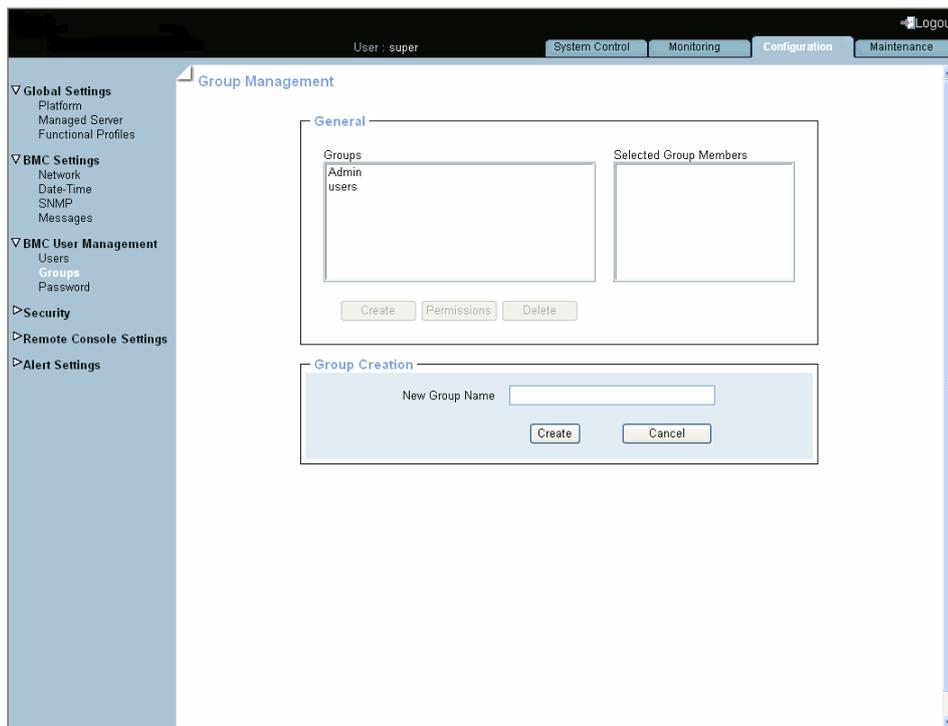
Prérequis

Vous avez la permission User/Group Management (Gestion utilisateurs/groupes)

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC User Management > Groups (BMC Gestion des utilisateurs - Groupes) pour afficher la page Group Management (Gestion des groupes).

2. Cliquez sur **Create** (Créer) pour ouvrir la boîte **Group Creation** (Création d'un groupe).



Group Creation (Création de groupe)	
New Group Name (Nouveau nom de groupe)	Nom donné au groupe. Restrictions : <ul style="list-style-type: none"> • Nom limité à 32 caractères. • Caractères interdits : "'`&*&#37; ~?/ et l'espace.

Figure 6-12. Gestion des groupes - Création d'un groupe

3. Entrez le nom du groupe dans le champ **New Group Name** (Nouveau nom de groupe) puis cliquez sur **Create** (Créer). Le groupe est créé et apparaît dans la boîte **Groups** (Groupes). Vous pouvez maintenant définir les permissions et configurer les utilisateurs pour ce groupe.
4. Utilisez l'utilitaire **KiraTool**, fourni sur le CD **Resource and Documentation**, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir **Sauvegarde des données de configuration**, page 7-13.

6.7.10. Configuration des permissions



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Les fonctionnalités accessibles à un utilisateur dépendent des permissions définies pour le groupe auquel appartient cet utilisateur. Cette section décrit comment spécifier et mettre à jour les permissions qui s'appliquent aux utilisateurs associés à un groupe.

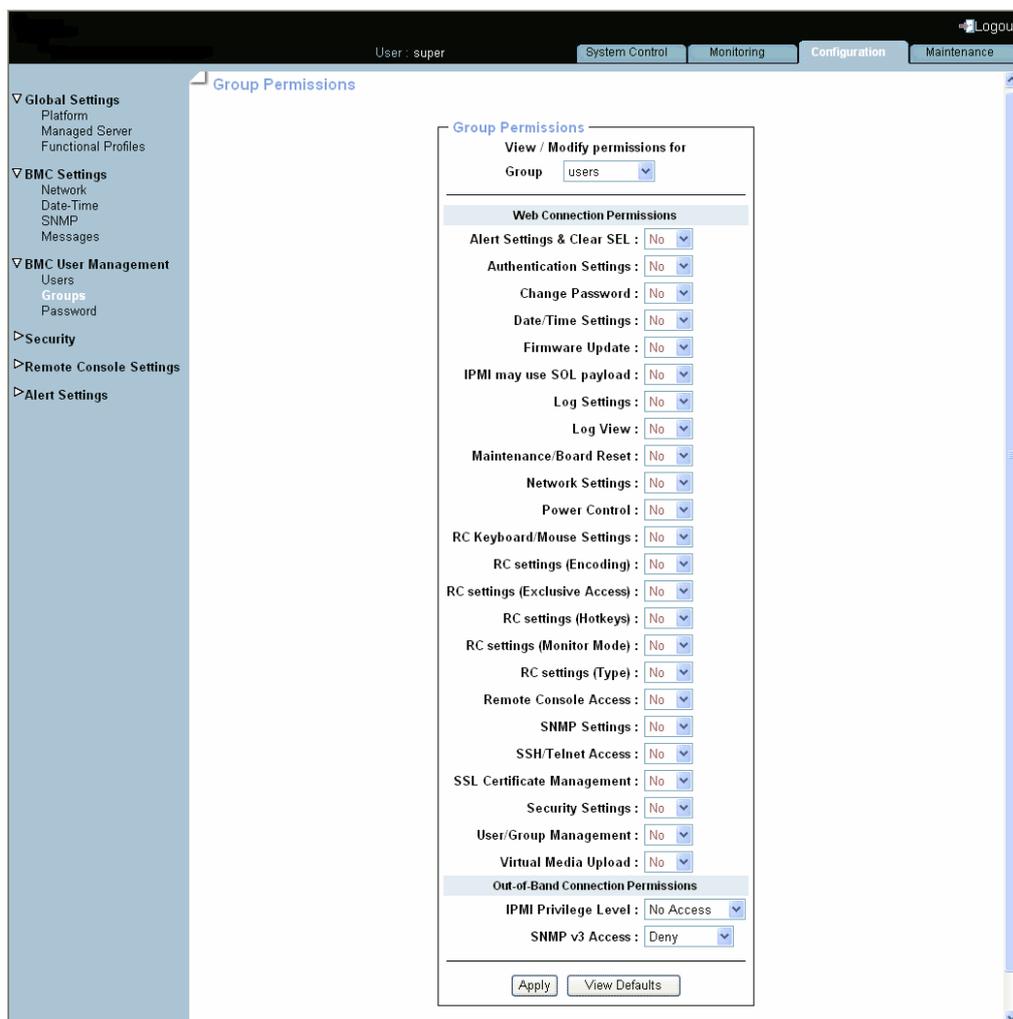
Prérequis

Vous avez la permission User/Group Management (Gestion utilisateurs/groupes)

Vous avez créé le groupe pour lequel vous voulez définir les permissions

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC User Management > Groups (BMC Gestion des utilisateurs - Groupes) pour afficher la page Group Management (Gestion des groupes).
2. Sélectionnez le groupe et cliquez sur Permissions pour afficher la page Group Permissions (Permissions du groupe).



Permissions du groupe	
View / Modify Permissions for Group (Voir / Modifier les permissions pour le groupe)	Cette liste déroulante permet de sélectionner un groupe pour afficher et/ou modifier les permissions définies pour le groupe sélectionné.
Web Connection Permissions (Permissions de connexion au Web)	Cette liste permet d'activer ou de désactiver les fonctionnalités de la console pour le groupe sélectionné. Sélectionnez Yes (Oui) ou No (Non) pour activer ou désactiver la fonction associée à chaque permission puis cliquez sur Apply (Appliquer). Utilisez les tableaux 6-1 et 6-2 pour vous aider à sélectionner les permissions. Note : Certaines caractéristiques sont accessibles à tous les utilisateurs et les permissions associées non configurables ne sont pas listées dans cette page.
IPMI Out-of-Band Connection Permissions (Permissions Connexions hors bande IPMI)	La liste déroulante IPMI Privilege Level (Niveau de privilège IPMI) permet de définir un rôle pour le groupe sélectionné. Voir le tableau 6-3 et les spécifications IPMI pour plus de détails.
SNMP v3 Access (Accès SNMP v3)	Les comptes utilisateurs ayant cette permission peuvent envoyer des commandes SNMP v3 sur le réseau local.

Figure 6-13. Permissions du groupe

3. Utilisez les tableaux 6-1 et 6-2 ci-dessous pour vous aider à sélectionner les permissions que vous voulez attribuer au groupe sélectionné.
4. Cliquez sur Apply (Appliquer) pour valider les permissions sélectionnées pour le groupe.
5. Utilisez l'utilitaire KiraTool, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

Les tableaux suivants listent les permissions et les fonctions associées.

Console : Permissions non configurables

Caractéristique	Onglet
Power Information (Informations sur l'alimentation) : Viewing & Refreshing (Affichage et rafraîchissement)	System Control (Contrôle système)
Sensor Status (État des capteurs)	Monitoring (Surveillance)
System Event Log (Journal SEL) : Viewing & Refreshing (Affichage et rafraîchissement)	Monitoring (Surveillance)
Management Controller (Contrôleur de gestion)	Maintenance
FRU	Maintenance
Firmware Version (Version de firmware)	Maintenance
Connected Users (Utilisateurs connectés)	Maintenance

Table 6-1. console matérielle : Permissions non configurables

Console : Permissions configurables

Permission configurable	Caractéristique	Onglet
Alert Settings & Clear SEL (Configuration d'alertes & effacement du SEL)	System Event Log (Journal SEL) : Clearing (Effacement)	Monitoring (Surveillance)
	Filters (Filtres)	Configuration
	Policies (Politiques)	Configuration
	LAN Destinations (Destinations LAN)	Configuration
	Général	Configuration
	Identification LED (Voyant d'identification)	Maintenance
Authentication Settings (Paramètres d'authentification)	Authentication (Authentification)	Configuration
Change Password (Changement du mot de passe)	Password (Mot de passe)	Configuration
Date/Time Settings (Paramètres Date/Heure)	Date-Time (Date-heure)	Configuration
Firmware Update (Mise à jour du firmware)	<i>Listed Firmware Upgrades (Mise à niveau des firmwares listés)</i>	Maintenance
IPMI may use SOL payload (IPMI peut utiliser la connexion SOL)	Serial-Over-Lan connection (Connexion Serial-Over-LAN (SOL)) (Les comptes utilisateurs ayant ces permissions peuvent lancer une session SOL)	-
Log Settings (Paramètres des journaux)	Messages	Configuration
Log View (Affichage des journaux)	Messages	Monitoring (Surveillance)
Maintenance/Board Reset (Maintenance/Réinitialisation Cartes)	Reset Management Controller (Réinitialisation du contrôleur de gestion)	Maintenance
	Hardware Exclusion (Exclusion matérielle)	Maintenance
Network Settings (Paramètres réseau)	Platform (Plateforme)	Configuration
	Managed Server (Serveur géré)	Configuration
	Functional Profile Settings (Paramètres du profil fonctionnel)	Configuration
	Network (Réseau)	Configuration
Power Control (Gestion de l'alimentation)	Power Management (Gestion de l'alimentation)	Power Control (Gestion de l'alimentation)
RC Keyboard/Mouse Settings (Paramètres clavier/souris de la console distante)	Keyboard & Mouse (Clavier et souris)	Configuration
RC Settings (Encoding) (Paramètres console distante (Encodage))	Transmission Encoding (Encodage de la transmission)	Configuration

Permission configurable	Caractéristique	Onglet
RC Settings (Exclusive Access) (Paramètres console distante (Accès exclusif))	Miscellaneous Remote Console Settings (Paramètres divers de la console distante) (Exclusive Access Mode (Mode Accès exclusif))	Configuration
RC Settings (Hotkeys) (Paramètres console distante (Touches rapides))	Mouse Hotkey Remote Console Button Key (Touche rapide de la souris Touche console distante)	Configuration
RC Settings (Monitor Mode) (Paramètres console distante (Mode moniteur))	Miscellaneous Remote Console Settings (Monitor Mode) (Paramètres divers de la console distante (Mode moniteur))	Configuration
RC Settings (Type) (Paramètres console distante (Type))	Réservé	-
Remote Console Access (Accès console distante)	Preview (Aperçu)	System Control (Contrôle système)
	Launch (Lancement)	System Control (Contrôle système)
Remote Console Access (Accès console distante)	Reset Keyboard/Mouse (USB) (Réinitialisation de clavier/souris (USB)) Reset USB (Réinitialisation de l'USB) Reset Video Engine (Réinitialisation du moteur vidéo)	Maintenance
SSH/Telnet Access (Accès SSH/Telnet)	SSH/Telnet connection (Connexion SSH/Telnet) (Les comptes utilisateurs ayant cette permission peuvent envoyer des commandes SSH/Telnet sur le réseau local)	-
SSL Certificate Management (Gestion du certificat SSL)	SSL Certificate (Certificat SSL)	Configuration

Permission configurable	Caractéristique	Onglet
Security Settings (Paramètres de sécurité)	Encryption (Chiffrement)	Configuration
	User Logon Policy (Politique de connexion utilisateur)	Configuration
	Power Button Lockout (Verrouillage du bouton de mise sous tension)	Configuration
	User Lockout (Verrouillage utilisateur)	Configuration
User/Group Management (Gestion des utilisateurs/groupes)	Users (Utilisateurs)	Configuration
	Groups (Groupes) : Management (Gestion)	Configuration
	Groups (Groupes) : Permissions	Configuration
Virtual Media Upload (Téléchargement d'un média virtuel)	Listed Virtual Media (Médias virtuels listés)	System Control (Contrôle système)

Table 6-2. console matérielle : Permissions configurables

IPMI Out-of-Band Connection Permissions (Permissions Connexions hors bande IPMI)	
IPMI Privilege Level (Niveau de privilège IPMI)	<p>Valeurs possibles :</p> <ul style="list-style-type: none"> • Pas d'accès (défaut) • Callback (Rappel) • User (Utilisateur) • Operator (Opérateur) • Administrator (Administrateur) • OEM <p>Pour plus de détails sur les niveaux de privilèges IPMI, consultez la spécification IPMI.</p>
SNMP v3 Access (Accès SNMP v3)	<p>Connexion SNMP v3 (Les comptes utilisateurs ayant cette permission peuvent envoyer des commandes SNMP v3 sur le réseau local).</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> • Accès refusé (défaut) • Lecture seule : • Lecture-Ecriture

Table 6-3. IPMI : Privilèges hors bande

6.7.11. Visualisation des membres d'un groupe



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Pour une gestion facile des groupes, vous pouvez afficher les membres de n'importe quel groupe à tout moment. Vous pouvez vouloir utiliser cette fonctionnalité, par exemple, pour vérifier l'appartenance à un groupe après la création ou la modification d'un compte utilisateur.

Prérequis

Vous avez la permission User/Group Management (Gestion utilisateurs/groupes)

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC User Management > Groups (BMC Gestion des utilisateurs - Groupes) pour afficher la page Group Management (Gestion des groupes).
2. Dans la liste Groups (Groupes), sélectionner un groupe. Les membres du groupe apparaissent dans la liste Selected Group Members (Membres du groupe sélectionné).

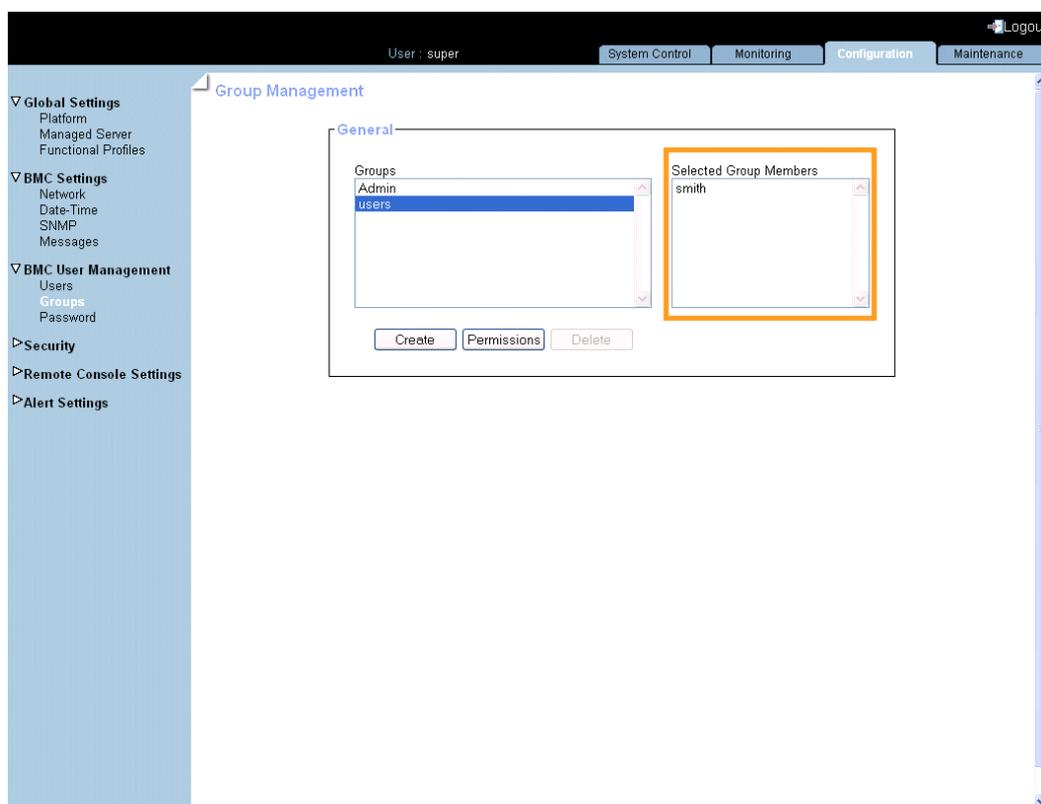


Figure 6-14. Group Management (Gestion des groupes)

6.7.12. Suppression d'un groupe



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Vous pouvez supprimer un groupe vide quand il ne sert plus.



Important Les groupes et les utilisateurs prédéfinis ne peuvent pas être supprimés.

Prérequis

Vous avez la permission User/Group Management (Gestion utilisateurs/groupe)

Il n'y a pas d'utilisateur membre du groupe à supprimer, c'est à dire que les utilisateurs ont été supprimés ou déplacés dans un autre groupe

Procédure

1. Depuis l'onglet Configuration, cliquez sur BMC User Management > Groups (BMC Gestion des utilisateurs - Groupes) pour afficher la page Group Management (Gestion des groupes).
2. Sélectionnez le groupe que vous voulez supprimer dans la liste Groups (Groupes) puis cliquez sur Delete (Supprimer) pour ouvrir la boîte Group Deletion (Suppression d'un groupe).

Note Si le groupe sélectionné contient des utilisateurs, le bouton Delete (Supprimer) n'est pas disponible.

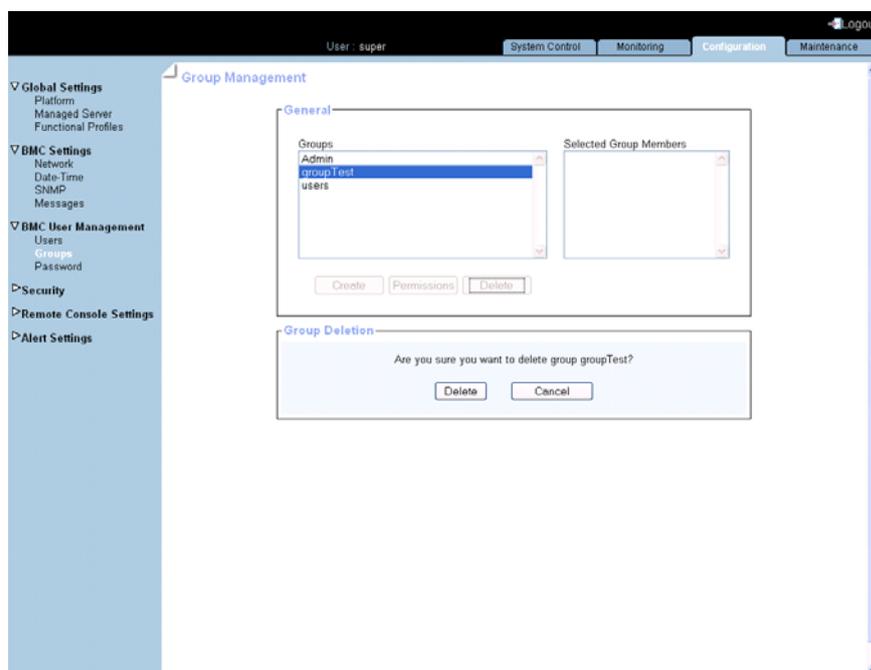


Figure 6-15. Gestion des groupes - Suppression d'un groupe

3. Cliquez sur **Delete** (Supprimer) Le groupe est supprimé et n'apparaît plus dans la boîte **Groups** (Groupes).
4. Utilisez l'utilitaire **KiraTool** , fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir **Sauvegarde des données de configuration**, page 7-13.

6.8. Configuration des paramètres de sécurité



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Pour une sécurité optimale, un ensemble complet de fonctionnalités de sécurité peut être personnalisé pour convenir à vos besoins. Ces fonctionnalités vont de la sécurisation des connexions web au contrôle de l'utilisation du bouton physique de marche/arrêt.

6.8.1. Forçage des connexions HTTPS



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Cette fonctionnalité permet de sécuriser les connexions Web à la console et de contrôler le mode de chiffrement du protocole KVM, qui est activé quand vous utilisez la Console système distante.



Important Par défaut, un certificat générique est délivré pour se connecter à la console avec le protocole HTTPS. Pour une sécurité optimale, il vous est recommandé de générer et d'installer votre propre certificat.

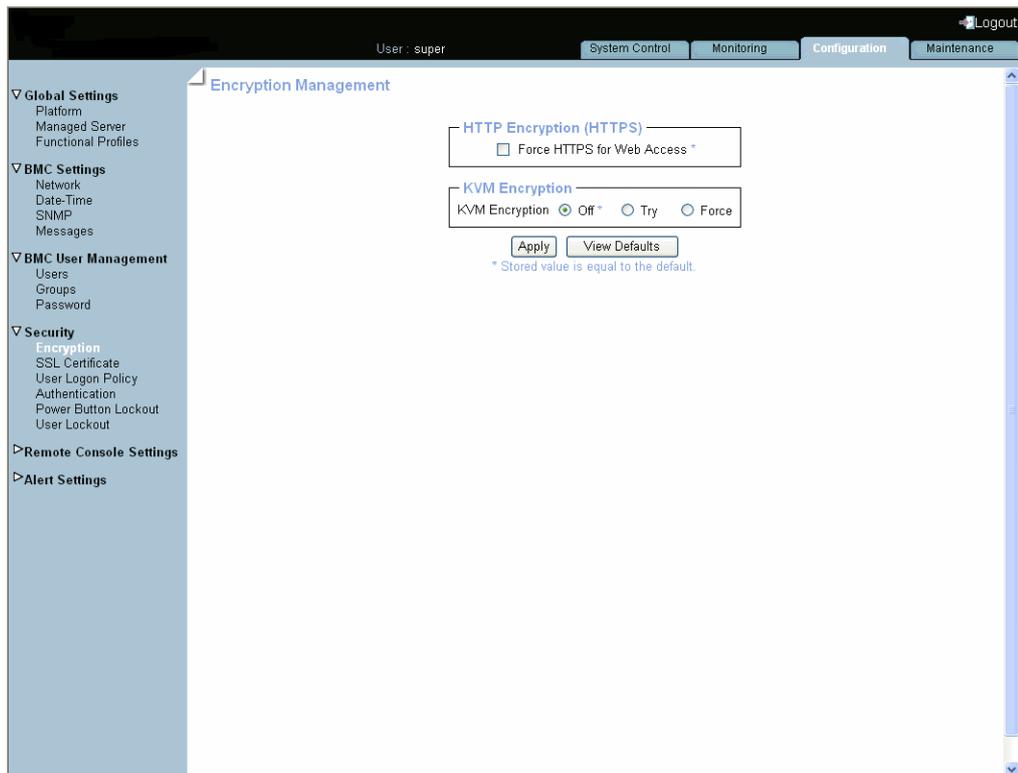
Note Par défaut, les connexions HTTPS utilisent le port 443. Vous pouvez avoir changé cette valeur, comme décrit dans Configuration des paramètres réseau pour l'accès à distance, page 6-6.

Prérequis

Vous avez la permission Security Settings (Paramètres Sécurité)

Procédure

1. Depuis l'onglet Configuration, cliquez sur Security > Encryption (Sécurité - Encryption) pour afficher la page Encryption Management (Gestion des encryptions).



Chiffrement HTTP (HTTPS)	
Force HTTPS for Web Access (Forcer HTTPS pour l'accès Web)	<p>Le protocole HTTPS requiert l'utilisation d'une URL dans un des formats suivants :</p> <ul style="list-style-type: none"> • https://<Adresse IP> • https://<Nom d'hôte> <p>IMPORTANT : Si cette option est sélectionnée, le protocole HTTP (http://<Adresse IP ou nom d'hôte>) ne peut plus être utilisé pour se connecter à la console.</p>
KVM Encryption (Chiffrement KVM)	
KVM Encryption (Chiffrement KVM)	<p>Cette option contrôle le chiffrement du protocole KVM. Ce protocole est utilisé par la Console système distante pour transmettre les données de l'écran à la machine de l'administrateur et les données du clavier et de la souris à l'hôte.</p> <ul style="list-style-type: none"> • Si elle est configurée sur Off, le chiffrement est désactivé. • Si elle est configurée sur Try (Tenter), la Console système distante tente d'établir une connexion chiffrée. Si la connexion chiffrée ne peut pas être établie, une connexion non chiffrée est utilisée à sa place. • Si elle est configurée sur Force (Forcer), la Console système distante tente d'établir une connexion chiffrée. Si la connexion chiffrée ne peut pas être établie, une erreur est transmise.
Bouton View Defaults (Afficher les valeurs par défaut)	Permet d'afficher les valeurs d'usine. Cliquez sur Apply (Appliquer) pour restaurer la configuration d'usine.

Figure 6-16. Gestion du chiffrement - valeurs d'usine

2. Utilisez l'utilitaire KiraTool , fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.
3. Sélectionnez les options requises puis cliquez sur **Apply** (Appliquer).

6.8.2. Obtention et installation d'un nouveau Certificat SSL



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Vous pouvez sécuriser les connexions Web en configurant la console pour utiliser le protocole HTTPS.

Un certificat SSL valide est requis pour utiliser le protocole HTTPS. Par défaut, un certificat temporaire est délivré. Pour une sécurité optimale, il vous est recommandé de générer et d'installer votre propre certificat.

Note Par défaut, les connexions HTTPS utilisent le port 443. Vous pouvez avoir changé cette valeur, comme décrit dans Configuration des paramètres réseau pour l'accès à distance, page 6-6.

Prérequis

Vous avez la permission SSL Certificate Management (Gestion des certificats SSL)

Procédure

1. Depuis l'onglet Configuration, cliquez sur Security > SSL Certificate (Sécurité – Certificats SSL) pour afficher la page SSL Certificate Management (Gestion des certificats SSL).

User: super System Control Monitoring Configuration Maintenance Logout

SSL Certificate Management

Global Settings
Platform
Managed Server
Functional Profiles

BMC Settings
Network
Date-Time
SNMP
Messages

BMC User Management
Users
Groups
Password

Security
Encryption
SSL Certificate
User Login Policy
Authentication
Power Button Lockout
User Lockout

Remote Console Settings

Alert Settings

Certificate Signing Request (CSR)

Common Name

Organizational Unit

Organization

Locality/City

State/Province

Country (ISO Code)

Email

Challenge Password

Confirm Challenge Password

Key Length (bits) 1024

* Stored value is equal to the default.

Certificate Signing Request (CSR) (Demande de signature de certificat)	
Common Name (Nom usuel)	“Nom de domaine pleinement qualifié” (FQDN) (exemple : hostName.DomainName.Tp-LevelDomain) Si le Nom usuel est différent du nom réseau, un avertissement de sécurité s'affiche quand une connexion HTTPS accède au système.
Organizational Unit (Unité d'organisation)	En général le nom du département (au sein de votre organisation) qui utilise le système (exemple : Recherche et Développement).
Organization (Organisation)	Nom de votre organisation.
Locality/City (Localité/Ville)	Nom de la ville.
State/Province (État/Province)	Nom de votre pays, province ou région.
Country (ISO Code) (Pays (Code ISO))	Code ISO de votre pays (exemple : FR pour France).
E-Mail (Courrier)	En général l'adresse mail de l'administrateur.
Challenge Password (Vérifier mot de passe)	Selon votre autorité de certification, vous pouvez devoir définir une vérification du mot de passe pour autoriser des changements ultérieurs au certificat (exemple : révocation du certificat). La longueur minimum de ce mot de passe est de 4 caractères.
Confirm Challenge Password (Confirmer la vérification du mot de passe)	
Key Length (bits) (Longueur de clé (bits))	Longueur de la clé générée en bits. Généralement 1024 bits. Des clés plus longues peuvent ralentir le temps de réponse de la connexion .

Figure 6-17. SSL Certificate Management (Gestion du certificat SSL)

2. Complétez les champs puis cliquez sur **Create** (Créer) pour générer votre CSR
3. Cliquez sur **Download** (Télécharger) pour enregistrer le CSR sur votre ordinateur et pour l'envoyer à l'autorité de certification, qui va vérifier vos informations, générer un Certificat signé et vous le renvoyer.
4. Quand vous recevez votre certificat signé, utilisez la boîte **Certificate Upload** (Téléchargement de certificat) pour installer le certificat.
5. Utilisez l'utilitaire **KiraTool**, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

6.8.3. Configuration de la politique de connexion



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Cette page permet de définir comment une session utilisateur sera gérée en termes du nombre de sessions ouvertes, de vieillissement de mot de passe et de délai d'inactivité.

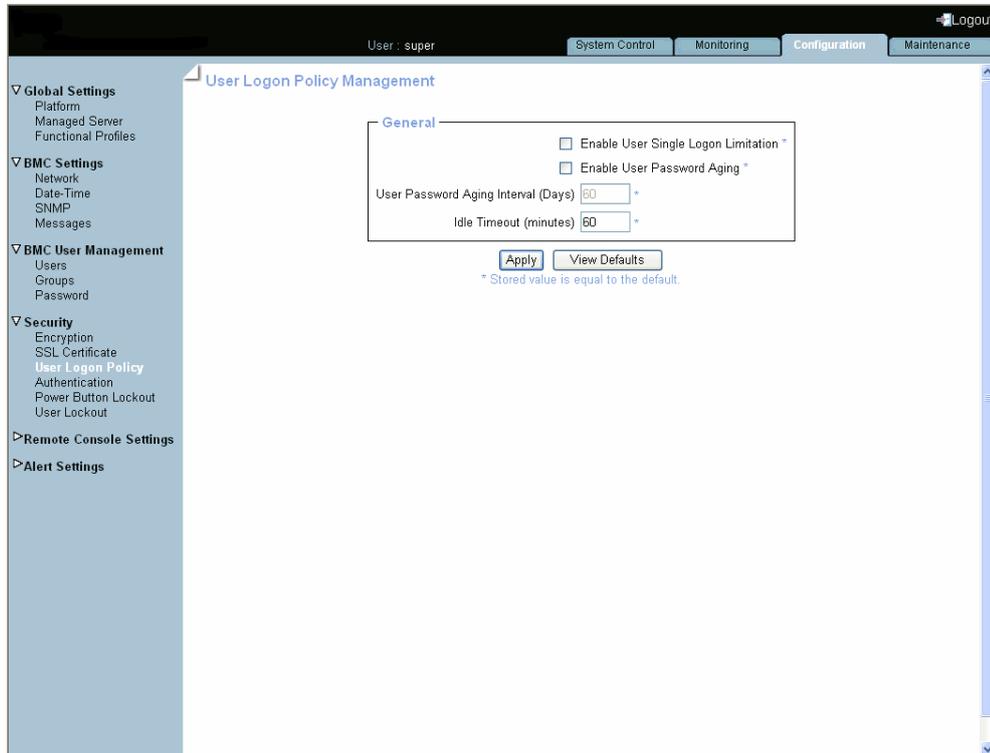
Prérequis

Vous avez la permission **Security Settings** (Paramètres Sécurité)

Vous vous connectez avec le compte utilisateur que vous voulez configurer

Procédure

1. Depuis l'onglet **Configuration**, cliquez sur **Security > User Logon Policy** (Sécurité - Politique de connexion utilisateur) pour afficher la page **User Logon Policy Management** (Gestion de la politique de connexion utilisateur).



Général	
Enable User Single Logon (Activer une connexion unique pour l'utilisateur)	Lorsque cette case est cochée, le compte utilisateur courant est limité à une connexion pour une unique session : une fois connecté, il n'est pas possible de se reconnecter à la console avec le même compte utilisateur.
Enable User Password Aging (Activer le vieillissement du mot de passe utilisateur)	Quand cette case est cochée, l'utilisateur doit changer son mot de passe dans l'intervalle indiqué.
User Password Aging Interval (Days) (Intervalle de vieillissement du mot de passe utilisateur (Jours))	Intervalle de changement du mot de passe, en jours.
Idle Timeout (Délai d'inactivité) (Minutes)	Temps après lequel l'utilisateur est automatiquement déconnecté, en minutes.
Bouton View Defaults (Afficher les valeurs par défaut)	Permet d'afficher les valeurs d'usine. Cliquez sur Apply (Appliquer) pour restaurer la configuration d'usine.

Figure 6-18. Gestion de la politique de connexion utilisateur - valeurs d'usine

2. Cochez ou décochez les cases suivant vos besoins puis cliquez sur Apply (Appliquer).
3. Utilisez l'utilitaire KiraTool , fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

6.8.4. Gestion de l'authentification



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Par défaut, la console est configurée pour utiliser son propre mécanisme d'authentification locale (Local Authentication) pour authentifier et connecter les utilisateurs. Vous pouvez utiliser ce mécanisme et créer manuellement des groupes et des comptes utilisateurs ou utiliser le serveur LDAP ou RADIUS de votre organisation pour utiliser les comptes utilisateurs existants.



- **Si vous sélectionnez la gestion d'authentification LDAP, la base de données LDAP n'est utilisée que pour la vérification du mot de passe. Les permissions utilisateurs et la configuration privée sont toujours enregistrés localement. Vous devez créer des comptes utilisateurs via la console (page User Management (Gestion de l'utilisateur))**
- **Le compte utilisateur par défaut "super" peut toujours être utilisé, indépendamment de la configuration de l'authentification.**

Prérequis

Vous avez la permission Authentication Settings (Paramètres d'authentification)

Pour la gestion de l'authentification LDAP ou RADIUS, vous avez configuré le serveur DNS depuis la page Enterprise Network Settings (Paramètres du réseau d'entreprise)

Pour la gestion de l'authentification RADIUS, vous avez déclaré la console en tant que client RADIUS (nom et adresse IP) et vous avez défini le partage secret

Procédure

1. Depuis l'onglet Configuration, cliquez sur Security > Authentication (Sécurité - Authentification) pour afficher la page Authentication Management (Gestion des authentifications).

The screenshot shows the 'Authentication Management' configuration page. The interface includes a top navigation bar with 'System Control', 'Monitoring', 'Configuration', and 'Maintenance' tabs. A left sidebar lists various settings categories: Global Settings, BMC Settings, BMC User Management, Security, Remote Console Settings, and Alert Settings. The 'Security' section is expanded to show 'Authentication' settings.

The main configuration area is titled 'Authentication Management' and contains a 'General' section with two radio buttons: 'Local Authentication' (selected) and 'LDAP'. The LDAP configuration fields include:

- User LDAP Server: [Text Field]
- Enable Secure LDAP:
- Port: [389]
- Secure LDAP Port: [636]
- Certificate File: [Text Field] [Parcourir...]
- LDAP server Base DN: [Text Field]
- LDAP Server Type: [Generic LDAP Server]
- Login-name Attribute: [Text Field]
- User-entry ObjectClass: [Text Field]
- User Search Subfilter: [Text Field]
- Active Directory Domain: [Text Field]

Below the LDAP section is a 'RADIUS' section with a table for server configuration:

	Server	Shared Secret	Auth. Port	Acc. Port	Timeout (sec.)	Retries
1.	[Text Field]	[Text Field]	[1812]	[1813]	[1]	[3]

Global Authentication Type: [PAP]

Buttons: [Apply] [View Defaults]

* Stored value is equal to the default.

Général	
Local Authentication (Authentification locale)	Cochez pour activer l'authentification de la console locale.
LDAP	Cochez pour activer l'authentification du serveur LDAP.
• User LDAP Server (Serveur LDAP utilisateur)	Entrez le nom d'hôte du serveur LDAP ou l'adresse IP.
• Enable Secure LDAP (Activer le protocole LDAP sécurisé)	Sélectionnez pour activer l'authentification du serveur LDAP sécurisé.
• Port	Entrez le numéro de port du serveur LDAP utilisé pour des demandes d'authentification.
• Secure LDAP Port (Port LDAP sécurisé)	Entrez le numéro de port du serveur LDAP sécurisé utilisé pour des demandes d'authentification.
• Certificate File (Fichier certificat)	Recherchez pour sélectionner le certificat de connexion sécurisé fourni par l'administrateur du serveur LDAP sécurisé.
• LDAP Server Base DN (Base DN du serveur LDAP)	Entrez le nœud de démarrage pour chercher les comptes utilisateurs. Exemple : dc=users,dc=domain,dc=com
• LDAP Server Type (Type de serveur LDAP)	Entrez le type de serveur LDAP : <ul style="list-style-type: none"> • Novell Directory Service si vous utilisez Novell eDirectory. • Microsoft Active Directory. • Serveur LDAP générique si vous utilisez un autre répertoire LDAP.
• Login-name Attribute (Attribut du nom de connexion)	Si vous avez sélectionné Novell Directory Service ou Microsoft Active Directory, laissez ces champs vides pour utiliser le répertoire par défaut. <ul style="list-style-type: none"> • Logon Name Attribute (Attribut du nom de connexion) : L'attribut LDAP est utilisé comme nom d'utilisateur pour se connecter au répertoire LDAP Exemple : cn. • User Entry Object Class (Classe d'objet d'entrée utilisateur) : classe d'objet qui identifie un utilisateur dans le répertoire Exemple : organizationalPerson.
• User-entry ObjectClass (Classe d'objet d'entrée utilisateur)	Si vous avez sélectionné Novell Directory Service ou Microsoft Active Directory, laissez ces champs vides pour utiliser le répertoire par défaut. <ul style="list-style-type: none"> • Logon Name Attribute (Attribut du nom de connexion) : L'attribut LDAP est utilisé comme nom d'utilisateur pour se connecter au répertoire LDAP Exemple : cn. • User Entry Object Class (Classe d'objet d'entrée utilisateur) : classe d'objet qui identifie un utilisateur dans le répertoire Exemple : organizationalPerson.
• User Search Subfilter (Sous-filtre de recherche utilisateur)	Restreint la recherche à certains comptes d'utilisateur. (exemple : (&(objectClass=person)(ou=System Validation)))

Général	
<ul style="list-style-type: none"> Active Directory Domain (Domaine Active Directory) 	(Microsoft Active Directory uniquement) : Le domaine Active Directory tel qu'il est configuré dans votre serveur Active Directory. Exemple : users.domain.com
RADIUS	Cochez pour activer l'authentification RADIUS
<ul style="list-style-type: none"> Server (Serveur) 	Entrez le nom d'hôte du serveur RADIUS ou l'adresse IP.
<ul style="list-style-type: none"> Shared Secret (Secret partagé) 	Un secret partagé est un texte utilisé comme un mot de passe entre le client RADIUS et le serveur RADIUS. Vous pouvez utiliser tout caractère alphanumérique standard et spécial. Un secret partagé peut comprendre jusqu'à 128 caractères et contenir des lettres minuscules et majuscules (A-Z,a-z), des chiffres (0-9) et d'autres symboles (tous les caractères non définis comme des lettres ou des chiffres) comme un point d'exclamation (!) ou une astérisque (*).
<ul style="list-style-type: none"> Auth. Port (Port d'authentification) 	Entrez le numéro de port du serveur RADIUS pour écouter les demandes d'authentification (1812 par défaut).
<ul style="list-style-type: none"> Acc. Port (Port de comptes) 	Entrez le numéro de port du serveur RADIUS pour écouter les demandes d'authentification (1813 par défaut).
<ul style="list-style-type: none"> Temporisation (sec.) 	Entrez la durée maximale d'attente de la fin de la demande en secondes. Si la tâche demandée n'est pas terminée dans cette intervalle, elle est annulée.
<ul style="list-style-type: none"> Retries (Tentatives) 	Entrez le nombre maximum d'essais si une demande ne peut être terminée.
<ul style="list-style-type: none"> Global Authentication Type (Type d'authentification globale) 	Sélectionnez le type d'authentification utilisé par le serveur RADIUS.
<ul style="list-style-type: none"> More Entries (Entrées supplémentaires) 	Si vous utilisez plusieurs serveurs RADIUS, cliquez sur ce bouton pour ajouter des configurations d'authentification.
Bouton View Defaults (Afficher les valeurs par défaut)	Permet d'afficher les valeurs d'usine. Cliquez sur Apply (Appliquer) pour restaurer la configuration d'usine.

Figure 6-19. Paramètres d'authentification - valeurs d'usine

- Suivant vos besoins, cliquez sur **Local Authentication** (Authentification locale), **LDAP** ou **RADIUS**, complétez les champs appropriés puis cliquez **Apply** (Appliquer).
- Utilisez l'utilitaire **KiraTool**, fourni sur le CD **Resource and Documentation**, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir **Sauvegarde des données de configuration**, page 7-13.

6.8.5. Activation/désactivation du bouton de mise sous tension du LCP



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

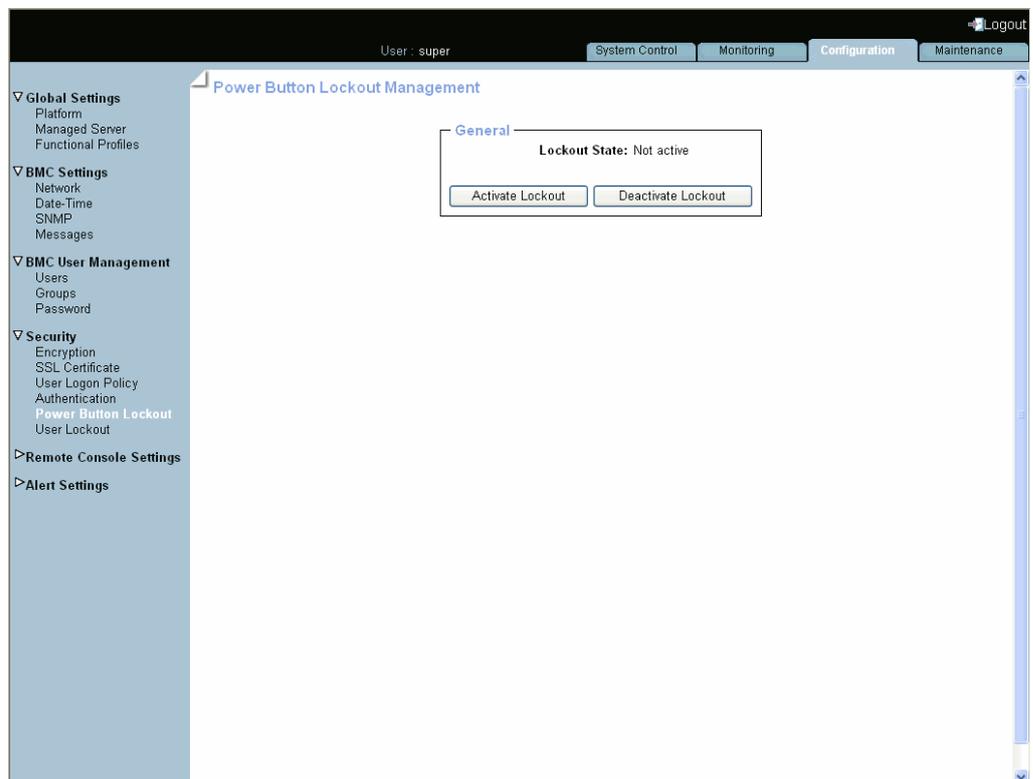
Le serveur est équipé d'un bouton de mise sous tension physique situé sur le panneau de contrôle local (LCP). Ce bouton de mise sous tension peut être verrouillé pour empêcher toute manipulation non autorisée.

Prérequis

Vous avez la permission Security Settings (Paramètres Sécurité)

Procédure

1. Depuis l'onglet Configuration, cliquez sur Security > Power Button Lockout (Sécurité - Verrouillage du bouton d'alimentation) pour afficher la page Power Button Lockout Management (Gestion du verrouillage du bouton d'alimentation).



Général	
Lockout State (État du verrouillage)	2 valeurs possibles : <ul style="list-style-type: none"> • Actif : le bouton de mise sous tension est verrouillé. • Non actif : le bouton de mise sous tension est déverrouillé.
Activate Lockout (Activer le verrouillage)	Désactive le bouton de mise sous tension.
Deactivate Lockout (Désactiver le verrouillage)	Active le bouton de mise sous tension.

Figure 6-20. Power Button Lockout Management (Gestion du verrouillage du bouton de mise sous tension)

2. Cliquez sur **Activate Lockout** (Activer le verrouillage) ou **Deactivate Lockout** (Désactiver le verrouillage), selon vos besoins.

6.8.6. Configuration du verrouillage d'un compte d'utilisateur



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

La fonction de verrouillage désactive un compte utilisateur si un certain nombre d'échecs de connexion se produit à cause de mots de passe erronés.

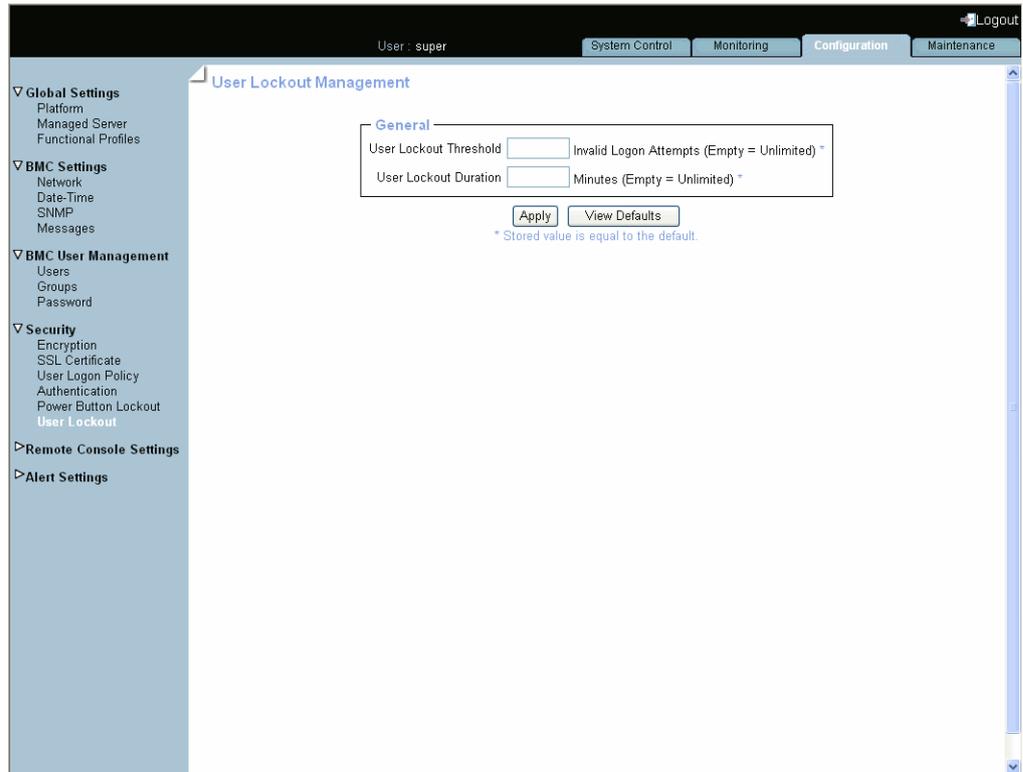
Prérequis

Vous avez la permission **Security Settings** (Paramètres Sécurité)

Vous vous êtes connecté avec le compte utilisateur à configurer

Procédure

1. Depuis l'onglet **Configuration**, cliquez sur **Security > User Lockout** (Sécurité - Verrouillage utilisateur) pour afficher la page **User Lockout Management** (Gestion du verrouillage des utilisateurs).



Général	
User Lockout Threshold (Seuil de verrouillage utilisateur)	Nombre maximum de tentatives de connexion invalides avant verrouillage du compte utilisateur. Note : Si vous laissez ce champ vide, le compte utilisateur ne sera jamais verrouillé.
User Lockout Duration (Durée de verrouillage utilisateur)	Entrez une durée en minutes pendant laquelle le compte utilisateur doit rester verrouillé. Une fois ce temps passé, le compte utilisateur est déverrouillé automatiquement. Note : Si vous laissez ce champ vide, un compte utilisateur verrouillé le reste jusqu'à ce que vous le déverrouilliez manuellement.
Bouton View Defaults (Afficher les valeurs par défaut)	Permet d'afficher les valeurs d'usine. Cliquez sur Apply (Appliquer) pour restaurer la configuration d'usine.

Figure 6-21. Gestion du verrouillage des utilisateurs - valeurs d'usine

2. Complétez les champs puis cliquez sur Apply (Appliquer).
3. Utilisez l'utilitaire KiraTool , fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

6.9. Configuration des alertes



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

La fonction de transmission des alertes permet de transmettre les événements sélectionnés en tant qu'alertes à un ou plusieurs gestionnaires SNMP et/ou destinataires de mails.

Quand vous configurez la transmission d'alertes pour la première fois, vous devez :

- Configurez la chaîne de communauté du serveur de gestion des événements et les adresses IP du serveur de mail et de l'expéditeur. Pour plus de détails, consultez Configuration des serveurs SNMP et SMTP, page 6-51
- Configurez l'adresse (ou les adresses) IP du serveur de gestion des événements et/ou l'adresse (ou les adresses) des destinataires des mails. Pour plus de détails, consultez Configuration des destinations LAN, page 6-52
- Configurez la/les politique(s) de transmission des alertes. Pour plus de détails, consultez Configuration des politiques d'alertes, page 6-55
- Sélectionnez les événements que vous voulez transmettre. Pour plus de détails, consultez Gestion des filtres d'événements prédéfinis, page 6-58 et Customisation d'un filtre d'événement, page 6-60.

Note Cette section explique comment configurer la fonctionnalité de transmission des alertes pour une utilisation courante. Les utilisateurs avancés peuvent consulter la *Spécification IPMI* officielle pour des informations sur les options avancées de transmission des alertes.



Important La transmission des alertes à la console iCare doit être configurée directement depuis l'interface de la console iCare. Consultez le manuel *iCare Console User's Guide* pour plus de détails.

6.9.1. Configuration des serveurs SNMP et SMTP



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Pour pouvoir transmettre des événements tels que des alertes à des gestionnaires SNMP et/ou des destinataires de mails, vous devez fournir des détails sur le serveur de gestion des événements et sur le serveur de mails.

Prérequis

Vous avez la permission Alert Settings & Clear SEL (Configuration d'alertes & effacement du SEL)

Procédure

1. Depuis l'onglet Configuration, cliquez sur Alert Settings > General (Paramètres d'alerte - Globaux) pour ouvrir la page General Settings (Paramètres globaux).

The screenshot displays the 'General Settings' page for alert configuration. On the left, a sidebar lists various configuration categories, with 'Alert Settings' expanded to show 'General'. The main area contains two alert configuration sections: 'Lan Alert' (Event Trap) and 'Email Alert'. The 'Event Trap' section has a 'Community String' field set to 'public'. The 'Email Alert' section has 'SMTP Server' and 'Email Sender Address' fields, with an 'Apply' button below them. The top navigation bar shows 'Configuration' as the active tab, and the user 'super' is logged in.

LAN Alert (Alerte LAN)	
Community String (Nom de communauté)	Si vous voulez utiliser la messagerie de gestion des événements PET, entrez la même valeur de chaîne de communauté que celle utilisée par le serveur de gestion SNMP. Valeur par défaut : public.
SMTP Server and Email Sender Address (Serveur SMTP et adresse mail expéditeur)	Si vous voulez utiliser la messagerie Email alert (Alerte mail), entrez : <ul style="list-style-type: none"> • SMTP Server (Serveur SMTP) : nom ou adresse IP du serveur mail SMTP sortant, utilisé pour envoyer les messages d'alertes mails. • Email Sender Address (Adresse mail de l'expéditeur) : l'adresse de l'expéditeur du serveur de mail telle qu'elle apparaît dans l'entête du mail.

Figure 6-22. Paramètres globaux des alertes

2. Complétez les champs requis puis cliquez sur Apply (Appliquer).
3. Utilisez l'utilitaire KiraTool, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

6.9.2. Configuration des destinations LAN



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Pour pouvoir envoyer des événements en tant qu'alertes à des gestionnaires SNMP ou des destinataires de mails, vous devez configurer les adresses IP du serveur de gestion des événements correspondant et/ou les adresses mails des destinataires. Ces adresses sont également appelées destinations LAN.



Important Ne configurez pas les paramètres d'alertes si vous utilisez la console iCare: la transmission des alertes et des messages est configurée automatiquement pendant la création de l'arborescence des ressources (découverte des ressources) à travers la console iCare.

Prérequis

Vous avez la permission Alert Settings & Clear SEL (Configuration d'alertes & effacement du SEL)

Procédure

1. Depuis l'onglet Configuration, cliquez sur Alert Settings > LAN Destinations (Paramètres d'alerte – Destinations LAN) pour ouvrir la page LAN Destination Settings (Paramètres de destination LAN).

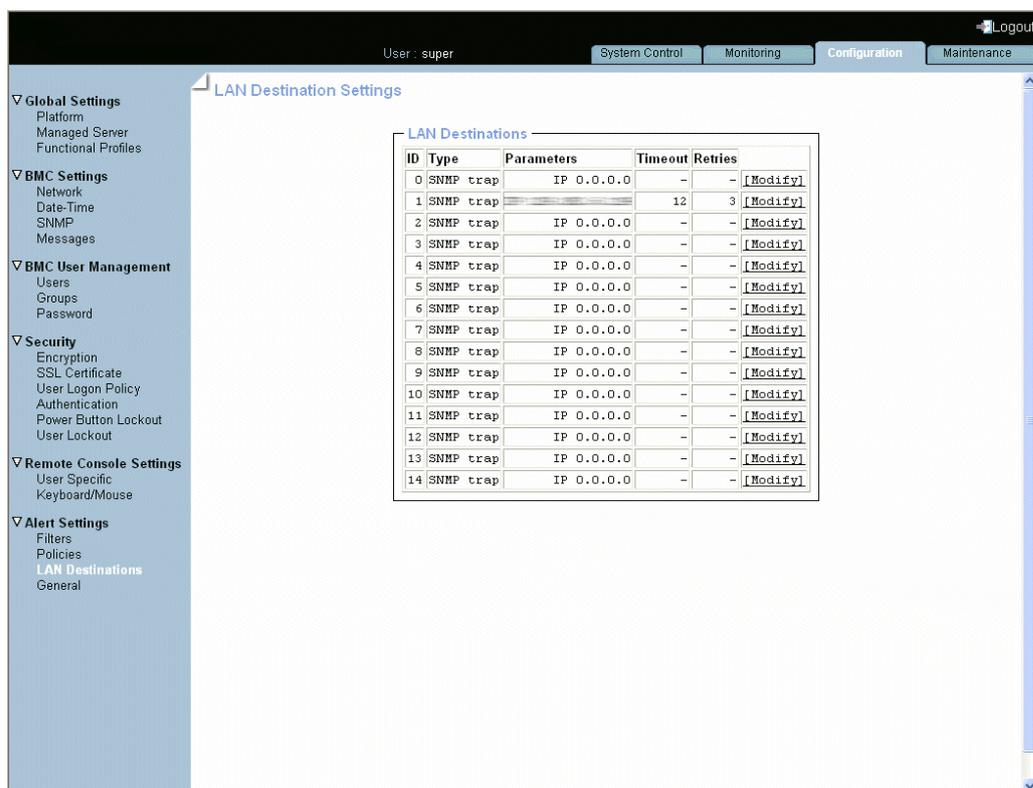
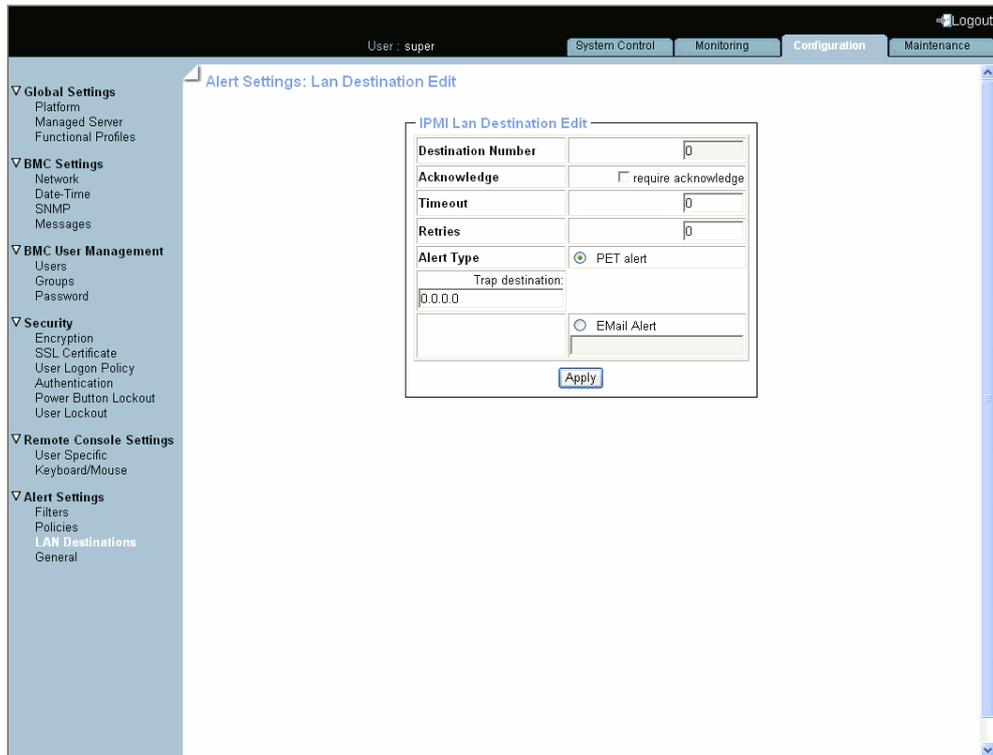


Figure 6-23. LAN Destination Settings (Paramètres de destination LAN)

2. Sélectionnez la première ligne de destination LAN libre (IP 0.0.0.0) et cliquez sur Modify (Modifier), pour afficher les Alert Settings (Paramètres d'alertes) : Page LAN Destination Edit (Édition de la Destination LAN).



IPMI LAN Destination Edit (Édition de la Destination LAN IPMI).	
Destination Number (Numéro de destination)	Lecture seule. Numéro prédéfini utilisé pour identifier la destination vers laquelle les messages d'alertes doivent être envoyés.
Acknowledge (Accuser réception)	Alertes PET uniquement. Sélectionnez cette option si vous voulez un accusé de réception des messages d'alertes.
Timeout (Expiration du délai)	Alertes PET uniquement. Temps d'attente de l'accusé de réception en secondes avant de réessayer.
Retries (Tentatives)	Alertes PET uniquement. Nombre de tentatives à effectuer avant d'abandonner.
Alert Type (Type d'alerte)	Format des messages d'alertes et méthodes : <ul style="list-style-type: none"> • PET alert (Alerte PET) (Gestion des événements plateforme) : envoie une alerte PET à l'adresse d'interruption indiquée. • Email alert (Alerte mail) : génère une alerte mail à l'adresse mail indiquée.
Trap destination (Destination d'interruption)	Alertes PET uniquement. Adresse IP du gestionnaire SNMP. Exemple : 192.x.x.x.
EMail Alert (Alerte mail)	Alertes mail uniquement. Adresse mail du destinataire. Exemple : john.smith@bull.net

Figure 6-24. Configuration des alertes : édition de la Destination LAN

3. Complétez les champs requis puis cliquez sur Apply (Appliquer).
4. Utilisez l'utilitaire KiraTool, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

6.9.3. Configuration des politiques d'alertes



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Les politiques d'alerte permettent de définir les stratégies de messagerie des alertes.

Note Certaines fonctions décrites ci-dessous s'adressent à des utilisateurs avancés. Pour des détails sur les options avancées de transmission des alertes, consulter la *Spécification IPMI* officielle.

Prérequis

Vous avez la permission Alert Settings & Clear SEL (Configuration d'alertes & effacement du SEL)

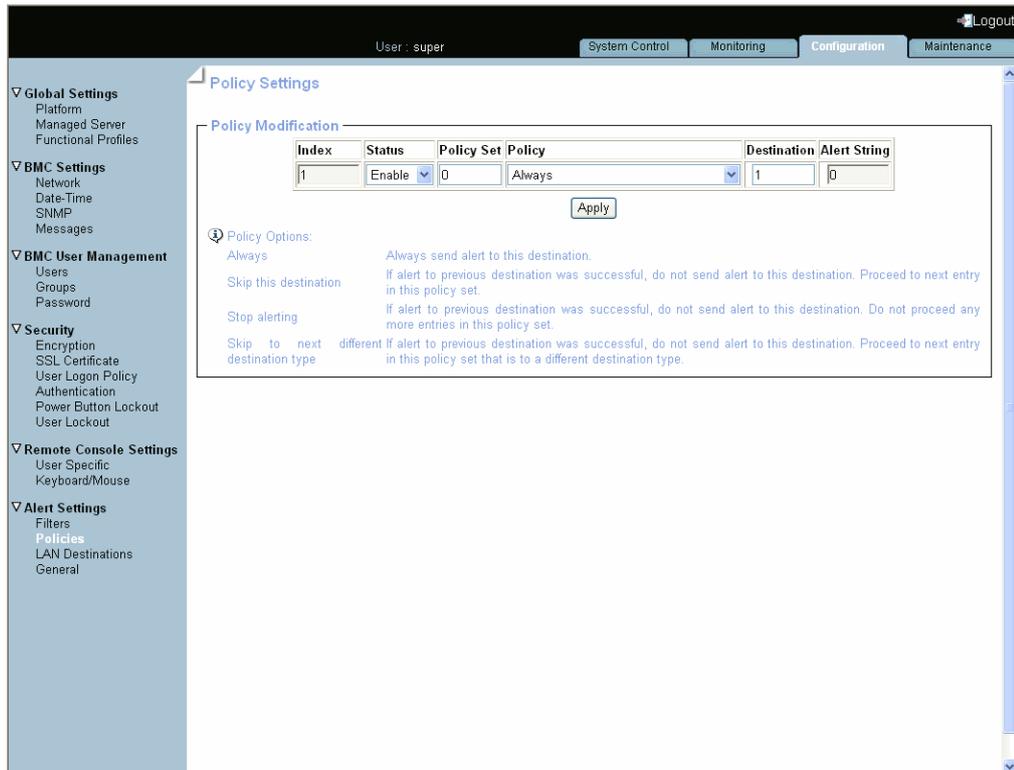
Procédure

1. Depuis l'onglet Configuration, cliquez sur Alert Settings > Politiques (Paramètres d'alerte - Politiques) pour ouvrir la page Policy Settings (Paramètres des politiques).

Index	Status	Policy Set	Policy	Channel No.	Destination	Alert String
1	Enabled	0	Always	LAN (1)	1	0 [Modify]
2	Disabled	0	Always	0	0	0 [Modify]
3	Disabled	0	Always	0	0	0 [Modify]
4	Disabled	0	Always	0	0	0 [Modify]
5	Disabled	0	Always	0	0	0 [Modify]
6	Disabled	0	Always	0	0	0 [Modify]
7	Disabled	0	Always	0	0	0 [Modify]
8	Disabled	0	Always	0	0	0 [Modify]
9	Disabled	0	Always	0	0	0 [Modify]
10	Disabled	0	Always	0	0	0 [Modify]
11	Disabled	0	Always	0	0	0 [Modify]
12	Disabled	0	Always	0	0	0 [Modify]
13	Disabled	0	Always	0	0	0 [Modify]
14	Disabled	0	Always	0	0	0 [Modify]
15	Disabled	0	Always	0	0	0 [Modify]
16	Disabled	0	Always	0	0	0 [Modify]
17	Disabled	0	Always	0	0	0 [Modify]
18	Disabled	0	Always	0	0	0 [Modify]
19	Disabled	0	Always	0	0	0 [Modify]

Figure 6-25. Paramètres des politiques d'alerte

2. Sélectionnez la première politique d'alerte libre désactivée puis cliquez sur **Modify** (Modifier) pour afficher la page **Policy Modification** (Modification de la politique).



Page Policy Modification (Modification de la politique)	
Index	Lecture seule.
Status (État)	<p>Deux valeurs possibles :</p> <ul style="list-style-type: none"> • Disable (Désactivé) (valeur par défaut) : la politique d'alerte n'est pas appliquée quand un événement se produit. • Enable (Activé) : la politique d'alerte est appliquée quand un événement se produit, suivant la stratégie sélectionnée dans la liste déroulante Policy (Politique) et le numéro de destination indiqué dans le champ Destination.
Policy Set (Ensemble de Politiques)	<p>Les politiques peuvent être regroupées dans différents ensembles de politiques, le cas échéant. Cette fonction est destinée à des utilisateurs avancés.</p> <p>Un seul ensemble de politiques, Policy Set 0, est implémenté pour les filtres d'événements prédéfinis.</p> <p>Pour des détails sur les options avancées de transmission des alertes, consulter la <i>Spécification IPMI officielle</i>.</p>

Page Policy Modification (Modification de la politique)	
Policy (Politique)	<p>Cette liste déroulante permet de définir une stratégie de messagerie d'événements pour la politique courante.</p> <p>Cette stratégie dépend des stratégies définies pour les politiques précédentes qui appartiennent au même ensemble de politiques.</p> <p>Suivant la stratégie que vous voulez appliquer, sélectionnez une des valeurs suivantes :</p> <ul style="list-style-type: none"> • Always (Toujours) : toujours envoyer l'alerte à cette destination. • Skip this destination (Passer cette destination) : si l'alerte a déjà été envoyée à une destination précédente par une politique précédente, ignorer cette destination et passer à la destination suivante dans le tableau. • Stop alerting (Arrêter les alertes) : si l'alerte a déjà été envoyée à une destination précédente par une politique précédente, ignorer cette destination et toutes les destinations suivantes dans le tableau. • Skip to next different destination type (Passer au type de destination différent suivant) : si l'alerte a déjà été envoyée à une destination précédente par une politique précédente, ignorez cette destination et passez à la destination suivante en utilisant une méthode de transmission différente (PET alert (Alerte PET) ou Email alert (Alerte mail)).
Destination	<p>Entrez le numéro prédéfini utilisé pour identifier la destination à laquelle les messages doivent être envoyés.</p> <p>Note :</p> <p>Ce numéro correspond au numéro dans la colonne ID de la page LAN Destination Settings (Paramètres de destination réseau).</p>
Alert String (Nom d'alerte)	0 Lecture seule.

Figure 6-26. Paramètres des politiques d'alerte - Modification

3. Complétez les champs requis puis cliquez sur **Apply** (Appliquer).
4. Utilisez l'utilitaire KiraTool, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir Sauvegarde des données de configuration, page 7-13.

Note **Traitement de la transmission des messages d'événements**

Quand un événement se produit, les entrées du tableau de filtres sont analysées suivant leurs numéros d'index : de 1 jusqu'au dernier numéro d'index dans la liste. Si plusieurs filtres d'événements activés correspondent à l'événement, le filtre ayant le numéro d'ensemble de politique le plus bas est sélectionné pour transmettre l'alerte.

Si plusieurs filtres d'événements activés correspondent à l'événement dans l'ensemble de politiques sélectionné, le filtre ayant la sévérité la plus haute est sélectionné pour transmettre l'alerte.

Si plusieurs filtres d'événements correspondent à l'événement dans l'ensemble de politiques sélectionné et s'ils ont tous la même sévérité, le filtre ayant l'index le plus bas est sélectionné pour transmettre l'alerte.

6.9.4. Gestion des filtres d'événements prédéfinis



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Plusieurs filtres d'événements sont prédéfinis à l'usine et activés par défaut. Ces filtres prédéfinis, listés dans le tableau des filtres, couvrent tous les événements potentiels. Ils ne peuvent pas être modifiés, mais ils peuvent être activés ou désactivés selon vos besoins. Le dernier filtre de la liste des filtres prédéfinis couvre tous les événements.

Pour plus de détails, voir Description des filtres d'alertes prédéfinis, page A-2.

Note Vous pouvez aussi définir des filtres d'événements personnalisés ou "configurables". Il s'agit d'une fonction avancée. Pour des détails sur les options avancées de transmission des alertes, vous pouvez consulter la *Spécification IPMI* officielle et Customisation d'un filtre d'événement, page 5-4



Important Si vous désactivez des filtres, les événements correspondants ne seront pas transmis à la console iCare.

Prérequis

Vous avez la permission Alert Settings & Clear SEL (Configuration d'alertes & effacement du SEL)

Procédure

1. Depuis l'onglet Configuration, cliquez sur Alert Settings > Filters (Paramètres d'alerte - Filtres) pour ouvrir la page Filter Settings (Paramètres de filtres).

Index	Status	Filter Type	Action	Policy Set	Severity	Generator ID	Sensor Type	Sensor No.	Trigger	Offset Mask	Data 1	Data 2	Data 3	
1	Enabled	Predefined	Alert	0	Information	ff ff	22	0f	6f ff ff	00 ff 00	ff 00 00	ff 00 00	ff 00	[Modify]
2	Enabled	Predefined	Alert	0	Information	ff ff	14	ff	ff ff ff	00 ff 00	ff 00 00	ff 00 00	ff 00	[Modify]
3	Enabled	Predefined	Alert	0	Information	ff ff	08	ff	6f 01 00	00 ff 00	ff 00 00	ff 00	[Modify]	
4	Enabled	Predefined	Alert	0	Non-recoverable	ff ff	08	ff	6f 02 00	00 ff 00	ff 00 00	ff 00	[Modify]	
5	Enabled	Predefined	Alert	0	Non-critical	ff ff	08	ff	6f 10 00	00 ff 00	ff 00 00	ff 00	[Modify]	
6	Enabled	Predefined	Alert	0	Information	ff ff	08	ff	ef 01 00	00 ff 00	ff 00 00	ff 00	[Modify]	
7	Enabled	Predefined	Alert	0	OK	ff ff	08	ff	ef 12 00	00 ff 00	ff 00 00	ff 00	[Modify]	
8	Enabled	Predefined	Alert	0	Information	ff ff	09	ff	0b 01 00	00 ff 00	ff 00 00	ff 00	[Modify]	
9	Enabled	Predefined	Alert	0	Non-critical	ff ff	09	ff	0b 12 00	00 ff 00	ff 00 00	ff 00	[Modify]	
10	Enabled	Predefined	Alert	0	Non-recoverable	ff ff	09	ff	0b 20 00	00 ff 00	ff 00 00	ff 00	[Modify]	
11	Enabled	Predefined	Alert	0	Non-recoverable	ff ff	02	ff	05 02 00	00 ff 00	ff 00 00	ff 00	[Modify]	
12	Enabled	Predefined	Alert	0	Information	ff ff	02	ff	85 02 00	00 ff 00	ff 00 00	ff 00	[Modify]	
13	Enabled	Predefined	Alert	0	Non-recoverable	ff ff	07	ff	6f 02 04	00 ff 00	ff 00 00	ff 00	[Modify]	
14	Enabled	Predefined	Alert	0	Information	ff ff	07	ff	6f 80 01	00 ff 00	ff 00 00	ff 00	[Modify]	
15	Enabled	Predefined	Alert	0	Information	ff ff	07	ff	ef 82 01	00 ff 00	ff 00 00	ff 00	[Modify]	
16	Enabled	Predefined	Alert	0	OK	ff ff	07	ff	ef 82 01	00 ff 00	ff 00 00	ff 00	[Modify]	
17	Enabled	Predefined	Alert	0	Information	ff ff	07	ff	ef 82 01	00 ff 00	ff 00 00	ff 00	[Modify]	

Figure 6-27. Gestion des filtres prédéfinis

2. Sélectionnez le filtre prédéfini souhaité, en utilisant le tableau dans Description des filtres d'alertes prédéfinis, page A-2, puis cliquez sur **Modify** (Modifier) pour afficher la boîte **Filter Modification** (Modification de filtre).

The screenshot shows the 'Filter Modification' dialog box within the BMC configuration interface. The interface includes a top navigation bar with 'System Control', 'Monitoring', 'Configuration', and 'Maintenance' tabs. A left sidebar lists various settings categories like Global Settings, BMC Settings, BMC User Management, Security, Remote Console Settings, and Alert Settings. The 'Filter Modification' dialog is centered, containing the following fields and options:

- Filter No.:** 1
- Status:** Enable (dropdown menu)
- Filter Type:** Predefined Filter
- Action:** Alert (checked), Reset, Power Off, Power Cycle (checkboxes)
- Alert Policy:** 0
- Event Severity:** information (dropdown menu)
- Generator ID:** 0xff, 0xff
- Sensor Type:** 0x22
- Sensor No.:** 0x0f
- Event Trigger:** 0x0f
- Data 1 Offset Mask:** Mask bits 7:0 0xff, Mask bits 15:8 0xff
- Event Data 1 (AND mask, compare1, compare2):** 0x00, 0xff, 0x00
- Event Data 2 (AND mask, compare1, compare2):** 0x00, 0xff, 0x00
- Event Data 3 (AND mask, compare1, compare2):** 0x00, 0xff, 0x00

An 'Apply' button is located at the bottom of the dialog.

Filter Modification (Modification de filtre)

Filter No. (N° du filtre)	Lecture seule, suivant l'ordre dans la liste des filtres.
Status (État)	Deux valeurs possibles : <ul style="list-style-type: none"> • Disable (Désactivé) (valeur par défaut) : le filtre n'est pas pris en compte lorsqu'un événement se produit. • Enable (Activé) : l'action indiquée dans le champ Action est exécutée si un événement correspond aux paramètres du filtre.
Filter Type (Type de filtre)	Lecture seule : Filtre prédéfini
Action	Lecture seule : Alert (Alerte). <ul style="list-style-type: none"> • Alert (Alerte) : l'événement est envoyé aux destinations spécifiées (pour des détails, voir Configuration des destinations LAN, page 6-52) • Reset (Réinitialisation) : le serveur est réinitialisé. • Power Off (Arrêt) : le serveur est arrêté. • Power Cycle (Cycle démarrage/arrêt) : le serveur est redémarré.
Alert Policy (Politique des alertes)	Lecture seule : 0.
Event Severity (Sévérité des événements)	Lecture seule, suivant la sévérité prédéfinie.

Filter Modification (Modification de filtre)	
Generator ID (ID du générateur)	Lecture seule. Pour plus de détails, consulter la Spécification IPMI officielle.
Sensor Type (Type de capteur)	
Sensor No. (N° de capteur)	
Event Trigger (Déclencheur d'événements)	
Data 1 Offset Mask (Données 1 Masque d'offset)	
Event Data 1 (AND mask, compare1, compare2) (Événement Données 2 (ET masque, compare1, compare2))	
Event Data 2 (AND mask, compare1, compare2) (Événement Données 2 (ET masque, compare1, compare2))	
Event Data 3 (AND mask, compare1, compare2) (Événement Données 2 (ET masque, compare1, compare2))	

Figure 6-28. Modification des filtres prédéfinis

3. Dans la liste déroulante **Status** (État), sélectionnez, soit **Enable** (Activé), soit **Disable** (Désactivé), selon vos besoins, puis cliquez **Apply** (Appliquer).
4. Utilisez l'utilitaire **KiraTool**, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir **Sauvegarde des données de configuration**, page 7-13.

6.9.5. Customisation d'un filtre d'événement



AVERTISSEMENT

Si le système fait partie d'un cluster de calcul, consultez la documentation livrée avec la suite logicielle du cluster pour les instructions d'installation. Il est conseillé de n'utiliser les pages de configuration qu'en lecture seule et de ne pas modifier les données de configuration, sauf indication contraire de la documentation de la suite logicielle du cluster.

Vous pouvez utiliser les filtres d'événements configurables pour créer un filtre d'événement personnalisé, par exemple si vous voulez définir une autre sévérité pour le filtre ou si vous voulez associer le filtre à un autre ensemble de politiques.

Quand vous définissez un filtre d'événements configurable, vous devez désactiver le filtre d'événements prédéfini correspondant pour vous assurer que votre filtre d'événements configurable est appliqué.

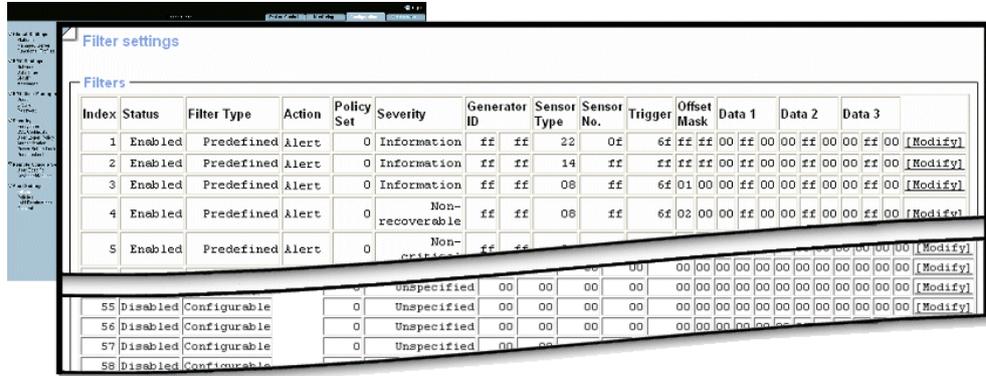
Note Vous êtes invités à consulter la *Spécification IPMI* officielle pour des informations sur les options avancées de transmission des alertes.

Prérequis

Vous avez la permission Alert Settings & Clear SEL (Configuration d'alertes & effacement du SEL)

Procédure

1. Depuis l'onglet Configuration, cliquez sur Alert Settings > Filters (Paramètres d'alerte - Filtres) pour ouvrir la page Filter Settings (Paramètres de filtres).

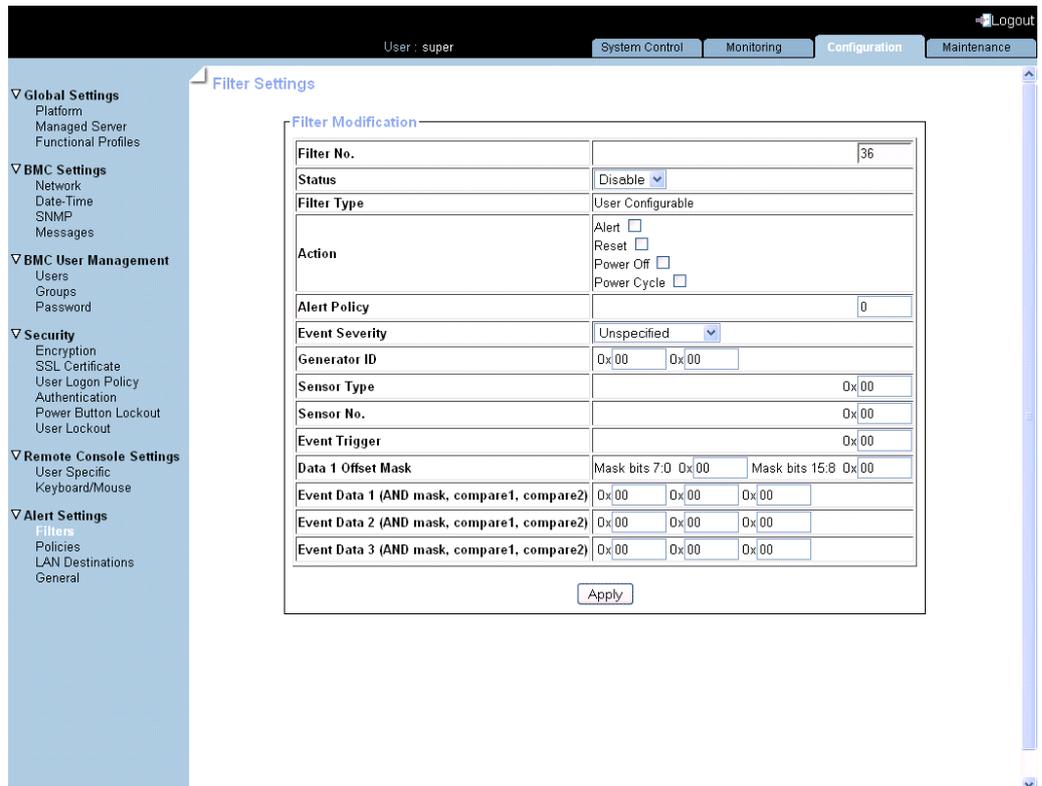


The screenshot shows the 'Filter settings' page with a table of filters. The table has columns for Index, Status, Filter Type, Action, Policy Set, Severity, Generator ID, Sensor Type, Sensor No., Trigger, Offset Mask, Data 1, Data 2, and Data 3. Each row has a '[Modify]' link at the end.

Index	Status	Filter Type	Action	Policy Set	Severity	Generator ID	Sensor Type	Sensor No.	Trigger	Offset Mask	Data 1	Data 2	Data 3	
1	Enabled	Predefined	Alert	0	Information	ff ff	22	0f	6f	ff ff	00 ff	00 ff	00 ff	[Modify]
2	Enabled	Predefined	Alert	0	Information	ff ff	14	ff	ff	ff ff	00 ff	00 ff	00 ff	[Modify]
3	Enabled	Predefined	Alert	0	Information	ff ff	08	ff	6f	01 00	00 ff	00 ff	00 ff	[Modify]
4	Enabled	Predefined	Alert	0	Non-recoverable	ff ff	08	ff	6f	02 00	00 ff	00 ff	00 ff	[Modify]
5	Enabled	Predefined	Alert	0	Non-recoverable	ff ff	ff	ff	ff	ff ff	00 ff	00 ff	00 ff	[Modify]
55	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00	00 00	00 00	00 00	[Modify]
56	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00	00 00	00 00	00 00	[Modify]
57	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00	00 00	00 00	00 00	[Modify]
58	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00	00 00	00 00	00 00	[Modify]

Figure 6-29. Personnalisation d'un filtre d'événement

2. Sélectionnez le premier filtre configurable libre dans la liste et cliquez sur Modify (Modifier) pour afficher la boîte Filter Modification (Modification du filtre).



The screenshot shows the 'Filter Modification' dialog box. The dialog has fields for Filter No. (36), Status (Disable), Filter Type (User Configurable), Action (Alert, Reset, Power Off, Power Cycle), Alert Policy (0), Event Severity (Unspecified), Generator ID (0x00 0x00), Sensor Type (0x00), Sensor No. (0x00), Event Trigger (0x00), Data 1 Offset Mask (Mask bits 7:0 0x00, Mask bits 15:8 0x00), Event Data 1 (AND mask, compare1, compare2) (0x00 0x00 0x00), Event Data 2 (AND mask, compare1, compare2) (0x00 0x00 0x00), and Event Data 3 (AND mask, compare1, compare2) (0x00 0x00 0x00). There is an 'Apply' button at the bottom.

Filter No.	36
Status	Disable
Filter Type	User Configurable
Action	<input type="checkbox"/> Alert <input type="checkbox"/> Reset <input type="checkbox"/> Power Off <input type="checkbox"/> Power Cycle
Alert Policy	0
Event Severity	Unspecified
Generator ID	0x00 0x00
Sensor Type	0x00
Sensor No.	0x00
Event Trigger	0x00
Data 1 Offset Mask	Mask bits 7:0 0x00 Mask bits 15:8 0x00
Event Data 1 (AND mask, compare1, compare2)	0x00 0x00 0x00
Event Data 2 (AND mask, compare1, compare2)	0x00 0x00 0x00
Event Data 3 (AND mask, compare1, compare2)	0x00 0x00 0x00

Filter Modification (Modification de filtre)	
Filter No. (N° du filtre)	Numéro du filtre (champ en lecture seule).
État	<p>Deux valeurs possibles :</p> <ul style="list-style-type: none"> • Disable (Désactivé) (valeur par défaut) : le filtre n'est pas pris en compte lorsqu'un événement se produit. • Enable (Activé) : l'action indiquée dans le champ Action est exécutée si un événement correspond aux paramètres du filtre.
Filter Type (Type de filtre)	Ce champ en lecture seule affiche User Configurable (Configurable par l'utilisateur) pour spécifier que vous éditez un filtre d'événements configurable.
Action	<p>Valeurs possibles :</p> <ul style="list-style-type: none"> • Alert (Alerte) : l'événement est envoyé aux destinations spécifiées (pour des détails, voir Configuration des destinations LAN, page 6-52) • Reset (Réinitialisation) : le serveur est réinitialisé. • Power Off (Arrêt) : le serveur est arrêté. • Power Cycle (Cycle démarrage/arrêt) : le serveur est arrêté puis redémarré.
Alert Policy (Politique des alertes)	<p>Valeur par défaut : 0.</p> <p>Les politiques peuvent être regroupées dans différents ensembles de politiques, le cas échéant. Cette fonction est destinée à des utilisateurs avancés.</p> <p>Un seul ensemble de politiques, Policy Set 0, est implémenté pour les filtres d'événements prédéfinis.</p> <p>Pour des détails sur les options avancées de transmission des alertes, consulter la <i>Spécification IPMI officielle</i>.</p>
Event Severity (Sévérité des événements)	Sélectionnez la valeur de la sévérité que vous voulez appliquer quand l'événement correspond aux paramètres du filtre.
Generator ID (ID du générateur)	<p>Ces champs permettent de spécifier l'événement que vous voulez filtrer. Il est conseillé de copier les valeurs saisies pour le filtre d'événement prédéfini correspondant que vous personnalisez.</p> <p>Pour plus de détails, consulter la <i>Spécification IPMI officielle</i> ou votre support technique.</p>
Sensor Type (Type de capteur)	
Sensor No. (N° de capteur)	
Event Trigger (Déclencheur d'événements)	
Data 1 Offset Mask (Données 1 Masque d'offset)	
Event Data 1 (AND mask, compare1, compare2) (Événement Données 2 (ET masque, compare1, compare2))	
Event Data 2 (AND mask, compare1, compare2) (Événement Données 2 (ET masque, compare1, compare2))	

Filter Modification (Modification de filtre)	
Event Data 3 (AND mask, compare1, compare2) (Événement Données 2 (ET masque, compare1, compare2)	Ces champs permettent de spécifier l'événement que vous voulez filtrer. Il est conseillé de copier les valeurs saisies pour le filtre d'événement prédéfini correspondant que vous personnalisez. Pour plus de détails, consulter la <i>Spécification IPMI</i> officielle ou votre support technique.

Figure 6-30. Filtres configurables - Modification

3. Complétez les champs requis puis cliquez sur **Apply** (Appliquer).
4. Utilisez l'utilitaire **KiraTool**, fourni sur le CD Resource and Documentation, pour sauvegarder les données de configuration en cas de besoin. Pour plus de détails, voir *Sauvegarde des données de configuration*, page 7-13.

Chapitre 7. Utilisation des fonctionnalités de maintenance

Ce chapitre explique les opérations de maintenance que vous pouvez effectuer depuis la console matérielle et comment utiliser les utilitaires fournis dans le *CD-ROM Resource and Documentation*. Il comprend les rubriques suivantes :

- Informations sur le contrôleur de gestion, page 7-2
- Récupération des informations sur les FRU, page 7-3
- Mise à jour du firmware, page 7-5
- Opérations de réinitialisation, page 7-6
- Activation/désactivation du voyant d'identification, page 7-8
- Exclusion/inclusion des processeurs, page 7-9
- Affichage des utilisateurs connectés, page 7-12
- Sauvegarde des données de configuration, page 7-13
- Restauration des données de configuration, page 7-14

Note La console matérielle peut être utilisée pour effectuer des mises à jour de firmwares. Ces opérations ne peuvent être effectuées que par du personnel de maintenance qualifié et ne sont pas documentées dans ce guide. Contactez votre Ingénieur Support Technique pour plus d'informations.

7.1. Informations sur le contrôleur de gestion

Vous pouvez afficher et/ou enregistrer dans un fichier XML les informations concernant le contrôleur de gestion intégré et le firmware. Cette fonctionnalité est particulièrement utile pour la maintenance et le dépannage (vérification de la version de firmware actuelle avant une mise à niveau ou envoi du fichier XML à l'équipe support, par exemple).

Procédure

1. Depuis l'onglet **Maintenance**, cliquez sur **Hardware Information > Management Controller** (Informations matérielles - Contrôleur de gestion) pour afficher la page **Management Controller Information** (Informations sur le contrôleur de gestion).

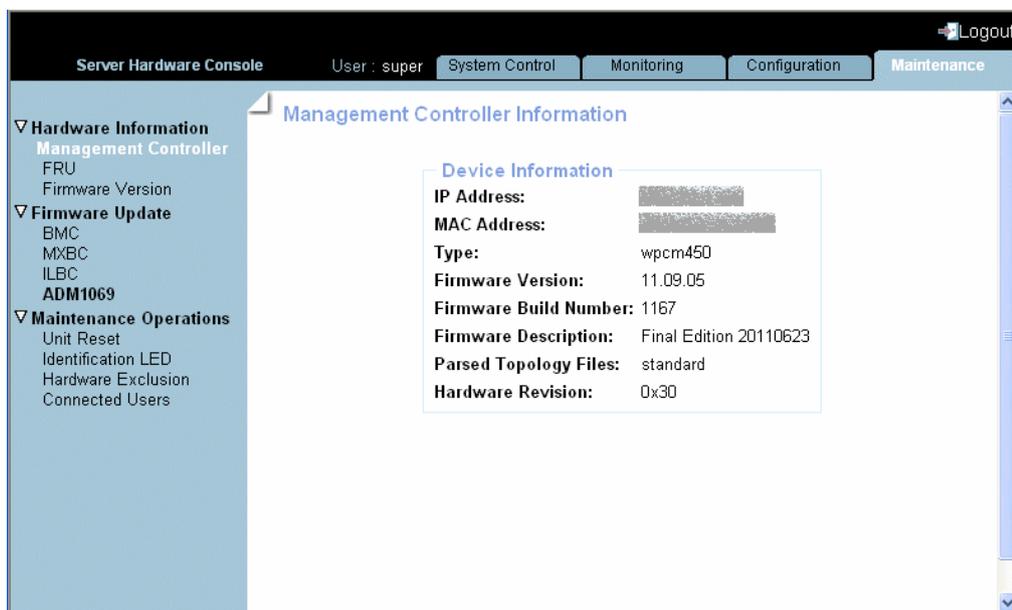


Figure 7-1. Management Controller Information (Informations sur le contrôleur de gestion)

Note Les valeurs **Firmware Version** (Version du firmware) et **Firmware Build Number** (Numéro de build du firmware) identifient la version de firmware et le numéro de build actuels.

7.2. Récupération des informations sur les FRU

Les informations conformes au standard IPMI gravées sur la FRU (Field Replaceable Unit) peuvent être affichées en ligne et/ou enregistrées dans un fichier XML et téléchargées pour une analyse hors ligne et pour l'archivage. Cette fonction est particulièrement utile à l'équipe de maintenance.

Procédure

1. Depuis l'onglet **Maintenance**, cliquez sur **Hardware Information > FRU (Informations matérielles - FRU)** pour afficher la page **FRU Information (Informations sur le FRU)**. Comme les informations sur les FRU doivent être collectées pour tous les composants du système, la page peut prendre quelques minutes à charger.

The screenshot shows the 'FRU Information' page in a web interface. The page has a navigation menu on the left with 'Hardware Information' expanded. The main content area displays 'FRU Information' with a 'Get Identity Card' button. Below this are four expandable tables: Platform, Modules, Boards, and Processors. Each table has a 'plus' icon on the left to expand it. The Platform table shows 'System' with description 'System Chassis'. The Modules table shows 'Module' with description 'Drawer module'. The Boards table shows five entries: PDB (Power Management), ILB (System Board), MTB (Processor Board), LCP (Front Panel Board), and PS_0 (Power Supply). The Processors table shows four entries: PROC_0, PROC_1, PROC_2, and PROC_3.

Figure 7-2. FRU Information (Informations sur les FRU)

Note Le bouton 'plus' à côté du nom d'une FRU indique que la ligne peut être étendue pour afficher des informations supplémentaires sur la FRU. Notez que les boutons 'plus' situés à côté des noms des processeurs sont affichés uniquement quand le serveur est démarré.

2. Pour enregistrer et télécharger les informations sur les FRU au format XML, cliquez sur **Get Identity Card (Obtenir l'identité de la carte)** et suivez les instructions à l'écran.

7.3. Affichage des versions des firmwares

Cette fonctionnalité est particulièrement utile pour la maintenance et le dépannage (vérification de la version de firmware actuelle avant une mise à niveau ou envoi des informations à l'équipe support, par exemple).

Procédure

- Depuis l'onglet Maintenance, cliquez sur Hardware Information > Firmware Version (Informations matérielles – Version du firmware) pour afficher la page Firmware Information (Informations sur le firmware).

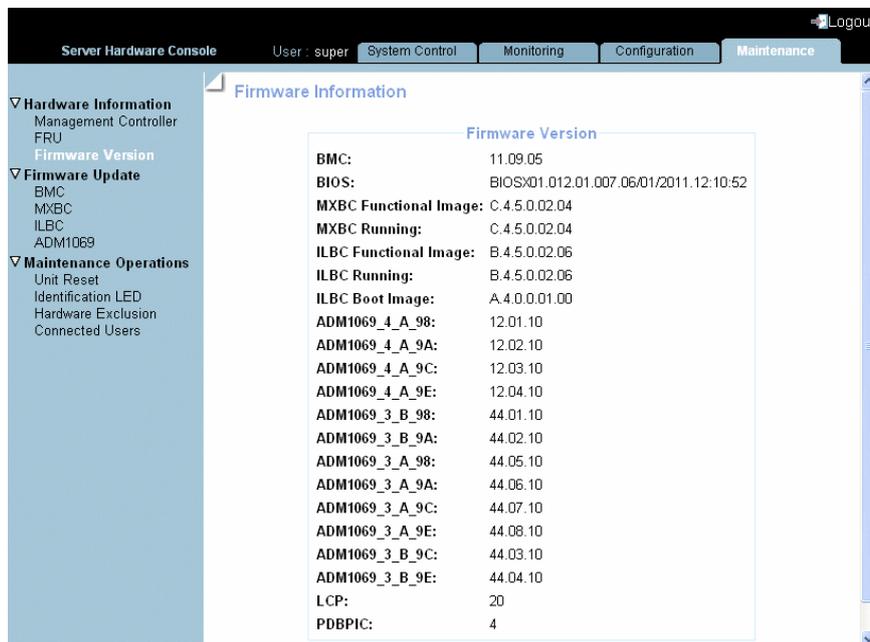


Figure 7-3. Affichage des informations sur le firmware - Exemple d'un serveur

Note Selon le modèle de serveur, d'autres types d'images de micrologiciel peuvent être affichées.

Note Pour certains firmwares, plusieurs types d'images sont affichés :

- Image fonctionnelle MXBC : image MXBC chargée dans la SPI Flash EEPROM
 - Image en cours MXBC : image MXBC chargée dans la FPGA RAM associée
 - Image fonctionnelle ILBC : image ILBC chargée dans la SPI Flash EEPROM
 - Image en cours ILBC : image ILBC chargée dans la FPGA RAM associée
 - Image Boot ILBC : image boot ILBC chargée dans la SPI Flash EEPROM
-

7.4. Mise à jour du firmware

Les firmwares des cartes listées ci-après peuvent être mis à jour pour installer de nouvelles fonctionnalités ou pour garantir l'intégrité du système après une opération de maintenance.

- Contrôleur de gestion intégré (BMC)
- Carte Mémoire et Xeon (MXBC)
- Carte I/O Legacy Board (ILBC)
- ADM 1069
- Images de l'interface FPGA PCIe (FPIF IMGA and FPIF IMGB)
- Panneau de contrôle local (LCP)



AVERTISSEMENT

Seul le personnel de support qualifié est autorisé à mettre à jour les firmwares du serveur. Ces opérations comportent des risques et ne sont pas documentées dans ce guide.

Contactez votre Ingénieur Support Technique pour plus d'informations.

7.5. Opérations de réinitialisation

Le contrôleur de gestion intégré, les clavier/souris virtuels, l'USB et l'écran vidéo peuvent être réinitialisés quand vous en avez besoin, par exemple, si le système est bloqué ou si les clavier/souris virtuels ou l'écran ne répondent plus.

Note Le contrôleur de gestion intégré est automatiquement réinitialisé après une mise à jour du firmware de la BMC.

Prérequis

Reset Management Controller (Réinitialisation du contrôleur de gestion) : vous avez la permission Maintenance/Board Reset (Maintenance/Réinitialisation Cartes)

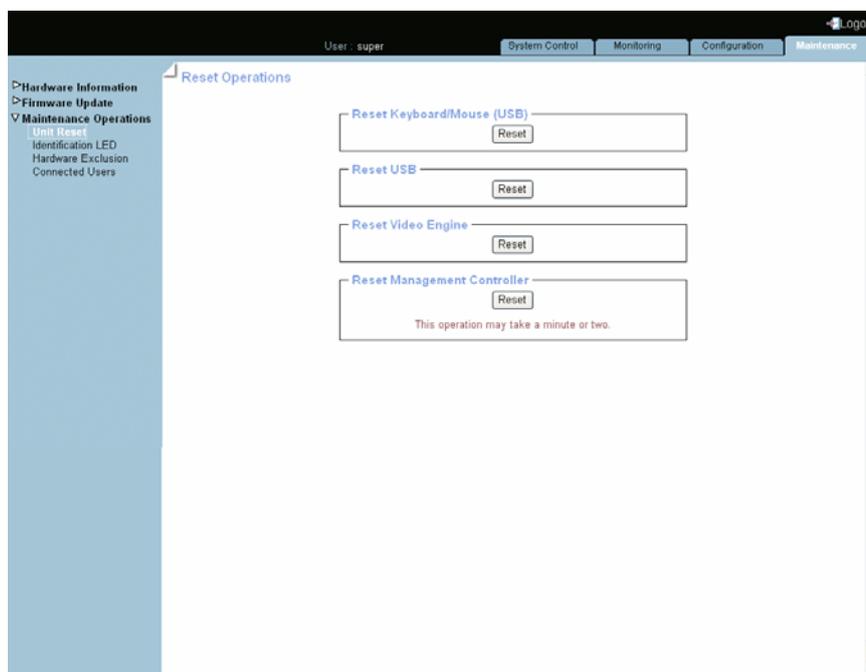
Réinitialisation Clavier/Souris (USB), Moteur vidéo : vous avez la permission Remote Console Access (Accès à la console distante)

Tous les utilisateurs se sont déconnectés de la console

Procédure

Note La commande Reset Management Controller (Réinitialisation du contrôleur de gestion) déconnectera tous les utilisateurs connectés.

1. Depuis l'onglet Maintenance, cliquez sur Maintenance Operations > Unit Reset (Opérations de maintenance - Réinitialisation de l'unité) pour ouvrir la page Reset Operations (Opérations de réinitialisation).



Caractéristique	Explication
Bouton Reset Keyboard/Mouse (USB) (Réinitialisation du clavier/souris (USB))	Réinitialise les clavier/souris virtuels.
Bouton Reset USB (Réinitialisation de l'USB)	Réinitialise l'USB virtuel.
Bouton Reset Video Engine (Réinitialisation du moteur vidéo)	Réinitialise l'écran virtuel.
Bouton Reset Management Controller (Réinitialisation du contrôleur de gestion)	Arrête et redémarre le contrôleur de gestion intégré.

Figure 7-4. Reset Operations (Opérations de réinitialisation)

2. Cliquez sur le bouton **Reset** (Réinitialisation) correspondant.

7.6. Activation/désactivation du voyant d'identification

Le serveur est équipé de deux voyants d'identification, situés à l'avant et à l'arrière du tiroir. Ces deux voyants d'identification bleus donnent une indication visuelle du tiroir en cours de maintenance.

Prérequis

Vous avez la permission **Alert Settings & Clear SEL** (Configuration d'alertes & effacement du SEL)

Procédure

1. Depuis l'onglet **Maintenance**, cliquez sur **Maintenance Operations > Identification LED** (Opérations de maintenance - Voyant d'identification) pour ouvrir la page **Identification LED Management** (Gestion des voyants d'identification).

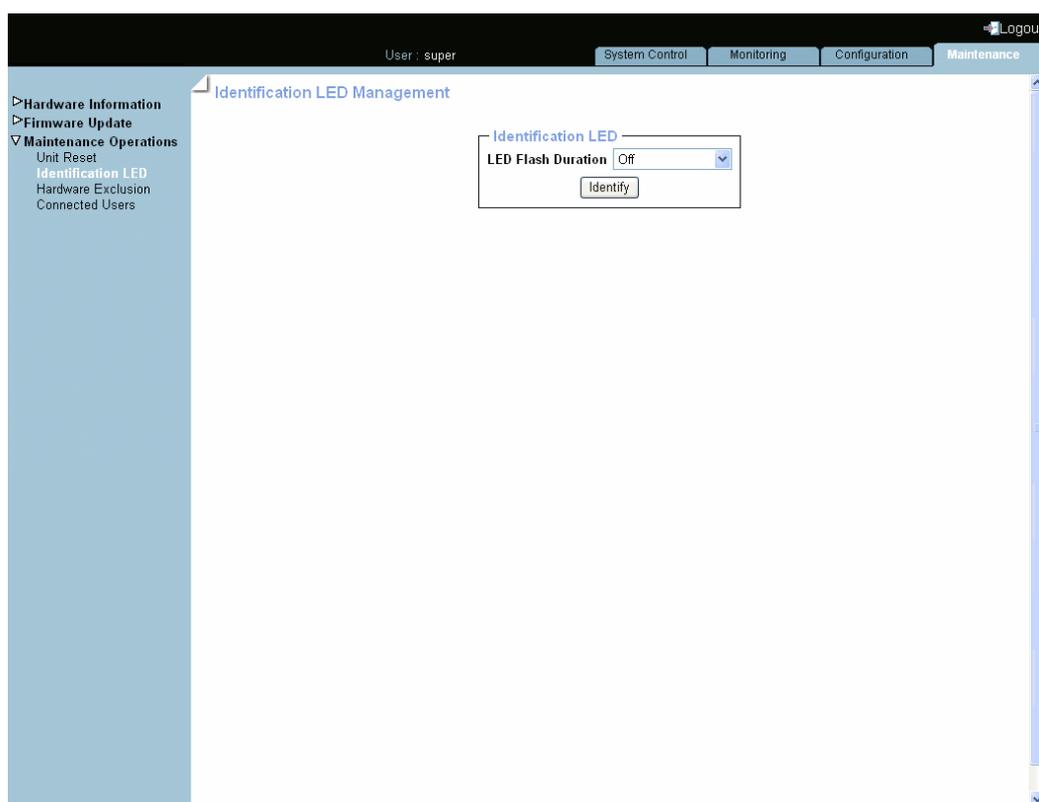


Figure 7-5. Identification LED Management (Gestion des voyants d'identification)

2. Sélectionnez dans la liste déroulante **LED Flash Duration** (Durée du flash du voyant) la valeur souhaitée puis cliquez sur **Identify** (Identifier).

7.7. Exclusion/inclusion des processeurs

La console vous permet d'exclure et d'inclure statiquement des processeurs : le serveur doit être arrêté pour sélectionner les processeurs à exclure/inclure, la modification étant prise en compte au prochain démarrage.

Note Les processeurs ne sont exclus que logiquement. Ils demeurent sous tension pour assurer le fonctionnement du système.

Prérequis

Vous avez la permission **Maintenance/Board Reset** (Maintenance/Réinitialisation Cartes)
Le serveur est arrêté

Procédure



Important L'exclusion de processeurs est une tâche spéciale que vous ne devez effectuer qu'en cas de défaillance.

1. Depuis l'onglet **System Control** (Contrôle du système), vérifiez que le serveur est mis en mode veille (standby) en sélectionnant **Power Management** (Gestion de l'alimentation) et en cliquant le bouton **Refresh** (Rafraîchir) dans la boîte **Power Information** (Information sur l'alimentation).
Si l'état de l'alimentation est **Off**, allez à l'étape 2, sinon arrêtez d'abord le système, puis allez à l'étape 2.
2. Depuis l'onglet **Maintenance**, cliquez sur **Maintenance Operations > Hardware Exclusion** (Opérations de maintenance – Exclusions de matériel) pour ouvrir la page **Hardware Exclusions** (Exclusions de matériel).

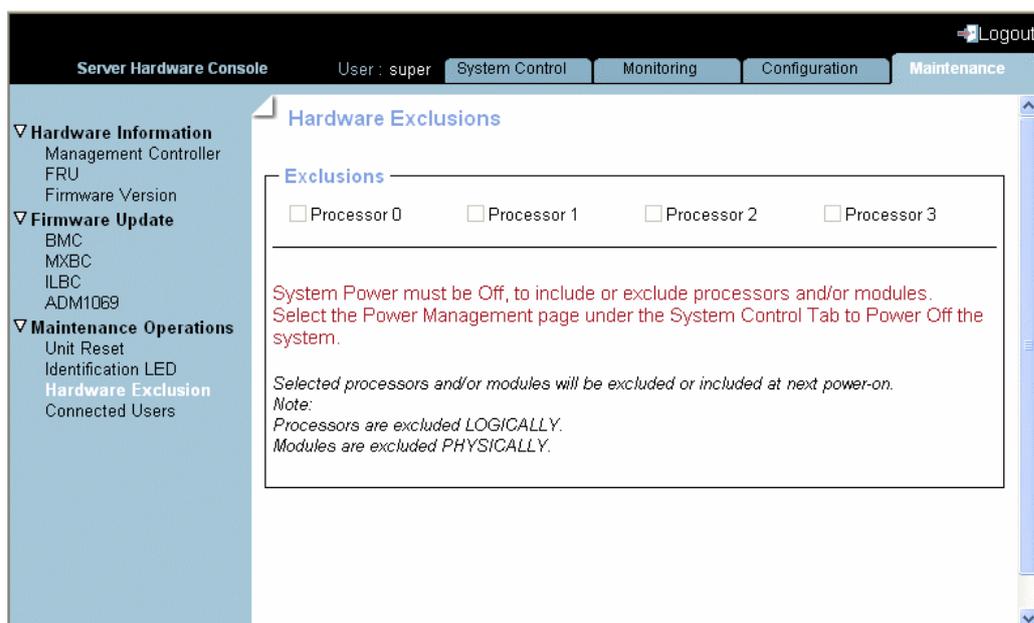


Figure 7-6. Exclusions de matériel



Important Si le serveur n'est pas démarré en mode veille (standby), un message est affiché vous demandant d'y procéder. Allez à l'étape 1.

3. Cochez la ou les case(s) correspondant au(x) processeur(s) à exclure ou décochez celle(s) correspondant au(x) processeur(s) à inclure, puis cliquez sur Apply (Appliquer).
4. Démarrez le serveur pour appliquer la modification.

7.8. Inclusion/Exclusion d'un module du serveur

La console vous permet d'exclure et d'inclure statiquement des module du serveurs : le module du serveur doit être arrêté pour sélectionner les composants à exclure/inclure et la modification est prise en compte au prochain démarrage.

Note Les modules sont exclus physiquement.

Prérequis

Vous avez la permission Maintenance/Board Reset (Maintenance/Réinitialisation Cartes)
Le serveur est arrêté

Procédure



Important L'exclusion de module du serveurs est une tâche spéciale que vous ne devez effectuer qu'en cas de défaillance.

1. Depuis l'onglet Power Control (Contrôle de l'alimentation), vérifiez que le module du serveur est arrêté en mode veille (standby) en sélectionnant Power Management (Gestion de l'alimentation) et en cliquant le bouton Refresh (Rafraîchir) dans la boîte Power Information (Information sur l'alimentation).
Si l'état de l'alimentation est Off, allez à l'étape 2, sinon arrêtez d'abord le système, puis allez à l'étape 2.
2. Depuis l'onglet Maintenance, cliquez sur Maintenance Operations > Hardware Exclusion (Opérations de maintenance – Exclusions de matériel) pour ouvrir la page Hardware Exclusions (Exclusions de matériel).

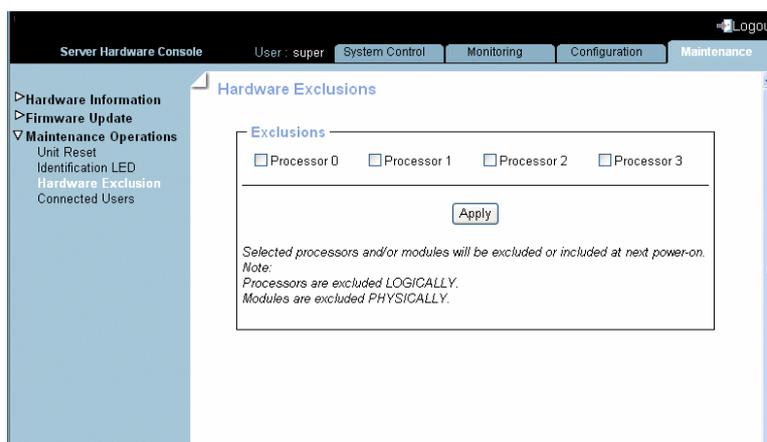


Figure 7-7. Exclusion/inclusion des modules



Important Si le module du serveur n'est pas démarré en mode veille (standby), un message est affiché vous demandant d'y procéder. Allez à l'étape 1.

3. Cochez la ou les case(s) correspondant au(x) module du serveurs à exclure ou décochez celle(s) correspondant au(x) module(s) à inclure, puis cliquez sur Apply (Appliquer).
4. Démarrez le module du serveur pour appliquer la modification.

7.9. Affichage des utilisateurs connectés

Vous pouvez voir si d'autres utilisateurs sont connectés à la console avant d'effectuer des tâches de configuration ou avant une intervention de maintenance.



Important Suivant le type de connexion, l'adresse IP affichée peut correspondre à un serveur proxy.

Procédure

- Depuis l'onglet Maintenance, cliquez sur Maintenance Operations > Connected Users (Opérations de maintenance - Utilisateurs connectés) pour ouvrir la page Connected Users Information (Information sur les utilisateurs connectés).

Connected Users	Connected IP Address	Session Type	Current Activity
super		Web	Active
super		Remote Console	Active

ⓘ According to HTTP connection type, the Connected IP Address may be that of a remote host or of a proxy server.

Figure 7-8. Connected Users Information (Informations sur les utilisateurs connectés)

7.10. Sauvegarde des données de configuration

Note La sauvegarde des données de configuration est une tâche administrative qui nécessite des permissions étendues. Vous devez utiliser le compte utilisateur **super** par défaut.



Important Suivez les instructions énoncées dans la documentation de l'outil *KiraTool* se trouvant sur le *CD-ROM Resource and Documentation* pour sauvegarder les données.

1. Assurez-vous que l'utilitaire *KiraTool* est installé.
 2. Consultez la documentation *KiraTool* disponible sur le *CD-ROM Resource and Documentation*.
 3. Depuis l'outil *KiraTool*, lancez la commande de sauvegarde comme décrit dans la documentation.
 4. Notez soigneusement le nom du fichier de sauvegarde et transmettez-le à l'administrateur du système. Le fichier sera utilisé pour restaurer les données de la configuration, quand nécessaire.
-



Important Deux opérations peuvent s'avérer nécessaires pour sauvegarder respectivement :

- les données de configuration (**cfg backup conf**)
 - les données de configuration des alertes (**cfg backup pef**)
-

7.11. Restauration des données de configuration

Note La restauration des données de configuration est une tâche administrative qui nécessite des permissions étendues. Vous devez utiliser le compte utilisateur *super* par défaut.



Important Suivez les instructions énoncées dans la documentation de l'outil *KiraTool* se trouvant sur le *CD-ROM Resource and Documentation* pour restaurer les données.

1. Assurez-vous que l'utilitaire *KiraTool* est installé.
 2. Demandez le nom du fichier de sauvegarde et le chemin à l'administrateur du système.
 3. Consultez la documentation *KiraTool* disponible sur le *CD-ROM Resource and Documentation*.
 4. Depuis l'outil *KiraTool*, lancez la commande de sauvegarde comme décrit dans la documentation.
-



Important Deux opérations peuvent s'avérer nécessaires pour restaurer respectivement :

- les données de configuration (**cfg backup conf**)
 - les données de configuration des alertes (**cfg restore pef**)
-

Annexe A. Dépannage du serveur

Ce chapitre décrit comment dépanner le serveur. Il comprend les rubriques suivantes :

- Description des filtres d'alertes prédéfinis, page A-2
- Messages du System Event Log (SEL), page A-9

A.1. Description des filtres d'alertes prédéfinis

Cette annexe liste les filtres d'événements prédéfinis. Un ensemble de filtres prédéfinis, couvrant tous les événements matériels pouvant survenir pendant le fonctionnement du système, sont disponibles pour la transmission des alertes à un SNMP Trap Manager (Gestionnaire d'interruptions SNMP), tel que Bull System Manager (BSM) ou à un destinataire de mail.

Description des filtres d'alertes prédéfinis

Pour information, les jeux de filtres suivants sont disponibles, selon le type de composant et le modèle de serveur :

Type de composant	Index de filtre
Power system board	1
Sub-chassis	2, 35, 36
Power supply	3, 4, 5, 6, 7
Power unit	8, 9, 10, 40
System board (ILB)	11, 12, 23, 47
Processor board (MXB)	11, 12, 23, 47
Processor	11, 12, 13, 14, 15, 16, 44
Fan device / Cooling unit	17, 18, 19, 20, 21, 23, 47
Power distribution board (PDB)	23, 47
Ultra capacitor	23, 45, 46, 47, 48, 49, 50
Control panel (LCP)	23, 47
Embedded Management Controller (BMC)	24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 37, 39, 41, 42, 43
Memory	38
External Environment	22, 23, 47
Tous	51

-
- Notes**
- Les filtres prédéfinis ne sont pas modifiables, ils ne peuvent être qu'activés ou désactivés. A la livraison du système, tous les filtres prédéfinis sont activés.
 - Si un filtre prédéfini ne vous convient pas, vous pouvez créer un filtre personnalisé. Dans ce cas, vous devez désactiver le filtre prédéfini correspondant afin de vous assurer que le filtre personnalisé est utilisé.
-

L'utilisation et la configuration des filtres d'événements sont expliquées dans Configuration des alertes, page 6-50.

Le tableau suivant détaille les événements associés à chaque filtre prédéfini.

N°	Composant	Source	Description de l'événement	Sévérité	Signification
1	Power system board	ACPI Pwr State	S0/G0: working	Information	Le système est démarré.
1	Power system board	ACPI Pwr State	S4/S5 : soft off	Information	Le système est arrêté.
2	Sub-chassis	Power button	Button pressed	Information	Le bouton de mise sous tension a été pressé.
3	Power supply	PS_X	Presence detected	Information	L'alimentation PS_X est présente.
4	Power supply	PS_X	Power supply failure detected	Non-recoverable	Une panne a été détectée sur l'alimentation PS_X.
5	Power supply	PS_X	Power supply input lost or out of range	Non-critical	Une panne secteur a été détectée par l'alimentation PS_X.
6	Power supply	PS_X	Presence detected	Information	L'alimentation PS_X n'est pas ou plus présente.
7	Power supply	PS_X	Power supply failure detected	Return to OK	La panne précédente sur l'alimentation PS_0 a disparu.
7	Power supply	PS_X	Power supply input lost	Return to OK	L'entrée secteur de l'alimentation PS_0 est maintenant correcte.
8	Power unit	Pwr Redundancy	Fully redundant	Information	Les trois alimentations sont sous tension et fonctionnent.
9	Power unit	Pwr Redundancy	Redundancy lost	Non-critical	Deux alimentations sont sous tension et fonctionnent.
9	Power unit	Pwr Redundancy	Non redundant: Sufficient resources from Insufficient resources	Non-critical	Deux alimentations sont sous tension et fonctionnent.
10	Power unit	Pwr Redundancy	Non redundant: Insufficient resources	Non-recoverable	Une seule alimentation est sous tension et fonctionne.
11	System board (ILB)	ILB_X	Limit exceeded	Non-recoverable	Cette tension est hors de la plage tolérée.
11	Processor board (MTB)	MTB_X	Limit exceeded	Non-recoverable	Cette tension est hors de la plage tolérée.
11	Processor board (MXB)	MXB_X	Limit exceeded	Non-recoverable	Cette tension est hors de la plage tolérée.
11	Processor	PX_X	Limit exceeded	Non-recoverable	Cette tension est hors de la plage tolérée.
12	System board (ILB)	ILB_X	Limit exceeded	Information	Cette tension est maintenant correcte.
12	Processor board (MTB)	MTB_X	Limit exceeded	Information	Cette tension est maintenant correcte.
12	Processor board (MXB)	MXB_X	Limit exceeded	Information	Cette tension est maintenant correcte.
12	Processor	PX_X	Limit exceeded	Information	Cette tension est maintenant correcte.
13	Processor	PROC_X	Thermal trip	Non-recoverable	PROC_X a atteint la limite de température la plus élevée et s'est arrêté.
14	Processor	PROC_X	Processor presence detected	Information	PROC_X est présent.
14	Processor	PROC_X	Processor disabled	Information	PROC_X est désactivé.
15	Processor	PROC_X	Thermal trip	Information	PROC_X fonctionne normalement.
15	Processor	PROC_X	Processor presence detected	Information	PROC_X est absent.

N°	Composant	Source	Description de l'événement	Sévérité	Signification
15	Processor	PROC_X	Processor disabled	Information	PROC_X est activé.
16	Processor	PROC_X	Processor automatically throttled	Return to OK	PROC_X fonctionne normalement.
17	Cooling unit	FANPR_X Redund.	Fully redundant	Information	Les deux ventilateurs de la paire de ventilateurs sont alimentés et fonctionnent.
18	Cooling unit	FANPR_X Redund.	Redundancy lost	Non-critical	Un seul ventilateur de la paire de ventilateurs est alimenté et fonctionne.
19	Cooling unit	FANBX_X Redund.	Non redundant: Insufficient resources	Non-recoverable	Aucun ventilateur ne fonctionne dans la paire de ventilateurs.
20	Cooling unit	FANUNIT_X Pres	Device removed / Device absent	Non-recoverable	Le bloc ventilateur n'est pas ou n'est plus présent.
20	Fan device	FAN_X Presence	Device removed / Device absent	Non-recoverable	Dans la paire de ventilateurs #X le ventilateur#Y n'est pas ou n'est plus présent.
21	Cooling unit	FANUNIT_X Pres	Device inserted / Device present	Return to OK	Le bloc ventilateur est (maintenant) présent.
21	Fan device	FAN_X Presence	Device inserted / Device present	Return to OK	Dans la paire de ventilateurs #X le ventilateur #Y est (maintenant) présent.
22	External Environment	Ambient Temp.	At or above upper critical threshold (going high)	Non-recoverable	La température extérieure est supérieure au seuil défini. Par défaut, un démarrage a été effectué.
23	Cooling unit	ROTOR_XY Speed	At or below lower critical threshold (going low)	Return to OK	Dans le bloc ventilateur #X, la vitesse du rotor #Y est maintenant à vitesse normale.
23	Fan device	FAN_X Speed	At or below lower critical threshold (going low)	Return to OK	Dans la paire de ventilateurs #X le ventilateur #Y est maintenant à vitesse normale.
23	System board (ILB)	ILB Temperature	At or below lower critical threshold (going low)	Return to OK	La température de l'ILB est maintenant normale.
23	System board (ILB)	ILB Temperature	At or above upper critical threshold (going high)	Return to OK	La température de l'ILB est maintenant normale.
23	Processor board (MTB)	MTB Temperature	At or below lower critical threshold (going low)	Return to OK	La température de la MTB est maintenant normale.
23	Processor board (MTB)	MTB Temperature	At or above upper critical threshold (going high)	Return to OK	La température de la MTB est maintenant normale.
23	Processor board (MXB)	MXB Temperature	At or below lower critical threshold (going low)	Return to OK	La température de la MXB est maintenant normale.
23	Processor board (MXB)	MXB Temperature	At or above upper critical threshold (going high)	Return to OK	La température de la MXB est maintenant normale.
23	Power distribution board (PDB)	PDB Temperature	At or below lower critical threshold (going low)	Return to OK	La température de la PDB est maintenant normale.
23	Power distribution board (PDB)	PDB Temperature	At or above upper critical threshold (going high)	Return to OK	La température de la PDB est maintenant normale.

N°	Composant	Source	Description de l'événement	Sévérité	Signification
23	Ultra capacitor	Ultra Capa Température	At or below lower critical threshold (going low)	Return to OK	La température de l'UltraCapa est maintenant normale.
23	Ultra capacitor	Ultra Capa Température	At or above upper critical threshold (going high)	Return to OK	La température de l'UltraCapa est maintenant normale.
23	Ultra capacitor	UC XX V	At or below lower critical threshold (going low)	Return to OK	Cette tension est maintenant correcte.
23	Ultra capacitor	UC XX V	At or above upper critical threshold (going high)	Return to OK	Cette tension est maintenant correcte.
23	Ultra capacitor	UC VCAP	At or above upper critical threshold (going high)	Return to OK	Cette tension est maintenant correcte.
23	Ultra capacitor	UC VCAP	At or above upper critical threshold (going high)	Return to OK	Cette tension est maintenant correcte.
23	Ultra capacitor	UC VBOOST	At or below lower critical threshold (going low)	Return to OK	Cette tension est maintenant correcte.
23	Ultra capacitor	UC VBOOST	At or above upper critical threshold (going high)	Return to OK	Cette tension est maintenant correcte.
23	Ultra capacitor	UC VREF	At or below lower critical threshold (going low)	Return to OK	Cette tension est maintenant correcte.
23	Ultra capacitor	UC VREF	At or above upper critical threshold (going high)	Return to OK	Cette tension est maintenant correcte.
23	Control panel (LCP)	Température LCP	At or below lower critical threshold (going low)	Return to OK	La température de la LCP est maintenant normale.
23	Control panel (LCP)	Température LCP	At or above upper critical threshold (going high)	Return to OK	La température de la LCP est maintenant normale.
23	External Environment	Ambient Temp.	At or above upper critical threshold (going high)	Return to OK	La température extérieure est maintenant normale.
24	BMC	Chipset Error	Transition to Critical from less severe	Non-recoverable	Une erreur non corrigible de chipset s'est produite.
24	BMC	Chipset Error	Transition to Non-Recoverable	Non-recoverable	Une erreur non corrigible de chipset s'est produite
25	BMC	Processor Error	Transition to Critical from less severe	Non-recoverable	Une erreur non corrigible de processeur s'est produite.
25	BMC	Processor Error	Transition to Non-Recoverable	Non-recoverable	Une erreur fatale de processeur s'est produite.
26	BMC	Version Change	Management (Gestion) controller firmware change was successful.	Information	Un événement changement de version s'est produit.
26	BMC	Version Change	System firmware change was successful	Information	Un événement changement de version s'est produit.

N°	Composant	Source	Description de l'événement	Sévérité	Signification
26	BMC	Version Change	Programmable hardware change was successful	Information	Un événement changement de version s'est produit.
27	BMC	Version Change	Management (Gestion) controller firmware change was unsuccessful	Non-critical	Un événement changement de version s'est produit.
27	BMC	Version Change	System firmware change was unsuccessful	Non-critical	Un événement changement de version s'est produit.
27	BMC	Version Change	Programmable hardware change was unsuccessful	Non-critical	Un événement changement de version s'est produit.
28	BMC	SEL	Sel log full	Non-critical	Il n'y a plus de place pour un nouvel événement dans le journal SEL.
28	BMC	SEL	Sel almost full	Non-critical	Le journal SEL est plein à 75%.
29	BMC	System Event	Un événement de démarrage du système a eu lieu	Non-recoverable	Voir Messages SEL : BMC.
30	BMC	Watchdog	Timeout - no specific action	Critical	Expiration du délai pendant étape d'initialisation du BIOS qui provoque l'action configurée.
30	BMC	Watchdog	Timeout followed by hard reset	Critical	Expiration du délai pendant étape d'initialisation du BIOS qui provoque l'action configurée.
30	BMC	Watchdog	Timeout followed by Power Down	Critical	Expiration du délai pendant étape d'initialisation du BIOS qui provoque l'action configurée.
30	BMC	Watchdog	Timeout followed by Power Cycle	Critical	Expiration du délai pendant étape d'initialisation du BIOS qui provoque l'action configurée.
31	BMC	Platform Security Violation Attempt	Out-of-band access password violation	Non-critical	Un accès IPMI "out of band" a échoué à cause d'une violation de mot de passe.
32	BMC	System Event	Entry added to auxiliary log	Information	Une erreur machine corrigée a été consignée par le BIOS dans la zone non volatile.
33	BMC	System Event	Entry added to auxiliary log	Critical	Une erreur machine non corrigée a été consignée par le BIOS dans la zone non volatile.
34	BMC	System Event	Entry added to auxiliary log	Non-recoverable	Une erreur machine fatale a été consignée par le BIOS dans la zone non volatile.
35	Sub-chassis	Mod. Intrusion	General chassis intrusion	Critical	Le boîtier est ouvert.
36	Sub-chassis	Mod. Intrusion	General chassis intrusion	Return to OK	Le boîtier est maintenant fermé.
37	BMC	Chipset Error	Transition to OK	Return to OK	Retour à une température normale.
38	Memory	DIMM_XX	Correctable ECC threshold reached	Warning	Seuil ECC corrigible atteint sur DIMM_XX.
39	BMC	Chipset Error	Informational	Information	Une erreur corrigible de chipset s'est produite.
40	Power unit	Pwr Consumption	Power Consumption Level	Information	Cet événement n'apparaît pas dans le journal SEL

N°	Composant	Source	Description de l'événement	Sévérité	Signification
41	BMC	Version Change	Firmware or software change	Information	Récupération du BIOS
42	BMC	System Boot Init	Initiated by hard reset	Information	System Boot Init
42	BMC	System Boot Init	OS / run-time software initiated hard (warm)reset	Information	System Boot Init
42	BMC	System Boot Init	System restart	Information	System Boot Init
43	BMC	Arrêt de l'OS	OS graceful stop	Information	Arrêt de l'OS
43	BMC	Arrêt de l'OS	OS graceful shutdown	Information	Arrêt de l'OS
44	Processor	Proc_X	Processor automatically throttled	Critical	PROC_X dérive lentement vers la limite de température ou de consommation d'énergie.
45	Ultra Capacitor	UC VCAP	At or above upper non recoverable threshold (going high)	Non-recoverable	Cette tension est hors de la plage acceptable. Le module est arrêté et désactivé.
46	Ultra Capacitor	UC VCAP	At or above upper non recoverable threshold (going high)	Return to OK	Cette tension est maintenant normale.
47	Cooling unit	ROTOR_XY Speed	At or below lower critical threshold (going low)	Critical	Dans le bloc ventilateur #X, la vitesse du rotor #Y est inférieure à la vitesse minimum requise.
47	Fan device	FAN_X Speed	At or below lower critical threshold (going low)	Critical	Dans la paire de ventilateurs # X la vitesse du ventilateur #Y est inférieure à la vitesse minimum requise.
47	System board (ILB)	ILB Temperature	At or below lower critical threshold (going low)	Critical	La température de l'ILB est inférieure à la valeur minimum.
47	System board (ILB)	ILB Temperature	At or above upper critical threshold (going high)	Critical	La température de l'ILB est supérieure à la valeur maximum.
47	Processor board (MXB)	MXB Temperature	At or below lower critical threshold (going low)	Critical	La température de la carte MXB est inférieure à la valeur minimum.
47	Processor board (MXB)	MXB Temperature	At or above upper critical threshold (going high)	Critical	La température de la MXB est supérieure à la valeur maximum.
47	Power (Démarrage) distribution board (PDB)	PDB Temperature	At or below lower critical threshold (going low)	Critical	La température de la PDB est inférieure à la valeur minimum.
47	Power (Démarrage) distribution board (PDB)	PDB Temperature	At or above upper critical threshold (going high)	Critical	La température de la MXB est supérieure à la valeur maximum.
47	Power (Démarrage) distribution board (PDB)	UltraCapa Temp.	At or below lower critical threshold (going low)	Critical	La température de l'ultra condensateur est inférieure à la valeur minimum.
47	Power (Démarrage) distribution board (PDB)	UltraCapa Temp.	At or above upper critical threshold (going high)	Critical	La température de l'ultra condensateur est supérieure à la valeur maximum.
47	Control panel (LCP)	LCP Temperature	At or below lower critical threshold (going low)	Critical	La température du LCP est inférieure à la valeur minimum.

N°	Composant	Source	Description de l'événement	Sévérité	Signification
47	Control panel (LCP)	LCP Temperature	At or above upper critical threshold (going high)	Critical	La température du LCP est supérieure à la valeur maximum.
47	External Environment	Ambient Temp.	At or above upper non-critical threshold (going high)	Critical	La température extérieure est supérieure au seuil non critique.
47	Ultra Capacitor	Ultra Capa Temperature	At or below lower critical threshold (going high)	Critical	La température de l'UltraCapa est inférieure à la valeur minimum.
47	Ultra Capacitor	Ultra Capa Temperature	At or above upper critical threshold (going high)	Critical	La température de l'UltraCapa est supérieure à la valeur maximum.
47	Ultra Capacitor	UC XX V	At or below lower critical threshold (going high)	Critical	Cette tension est hors de la plage acceptable.
47	Ultra Capacitor	UC XX V	At or above upper critical threshold (going high)	Critical	Cette tension est hors de la plage acceptable.
47	Ultra Capacitor	UC VCAP	At or above upper critical threshold (going high)	Critical	Cette tension est hors de la plage acceptable. L'UltraCap a été désactivée.
47	Ultra Capacitor	UC VBOOST	At or below lower critical threshold (going high)	Critical	Cette tension est hors de la plage acceptable.
47	Ultra Capacitor	UC VBOOST	At or above upper critical threshold (going high)	Critical	Cette tension est hors de la plage acceptable.
47	Ultra Capacitor	UC VREF	At or below lower critical threshold (going high)	Critical	Cette tension est hors de la plage acceptable.
47	Ultra Capacitor	UC VREF	At or above upper critical threshold (going high)	Critical	Cette tension est hors de la plage acceptable.
48	Ultra capacitor	UC Failure	Battery failed	Critical	Un défaut a été détecté sur l'UltraCapa (surtension, sous-tension mémorisée ou timeout du chargeur)
49	Ultra Capacitor	UC Failure	Battery failed	Return to OK	L'Ultra Capacitor est maintenant normal
50	Ultra capacitor	UC Power Outage	State asserted	Information	Panne de courant
51	Tous	Tous	Tous	Unspecified	Tous les événements sont prélevés

Table A-1. Filtres d'événements prédéfinis

A.2. Messages du System Event Log (SEL)

Cette annexe liste les messages du System Event Log (SEL) et explique les actions de récupération, le cas échéant. Il comprend les rubriques suivantes :

- Messages SEL : External Environment, page A-10
- Messages SEL : Power system board, page A-10
- Messages SEL : Sub-chassis, page A-11
- Messages SEL : Power Supply, page A-12
- Messages SEL : Power Unit, page A-13
- Messages SEL : ILB, page A-15
- Messages SEL : MTB/MXB, page A-27
- Messages SEL : Processor, page A-30
- Messages SEL : Fan device / Cooling unit, page A-41
- Messages SEL : PDB, page A-43
- Messages SEL : Ultra Capacitor, page A-44
- Messages SEL : LCP (Panneau de contrôle local), page A-53
- Messages SEL : BMC, page A-54
- Messages SEL : Memory, page A-62
- Etapes de démarrage : BMC, page A-62
- Etapes de démarrage : SMC, page A-65

Note Les rubriques suivantes listent la totalité des messages qui peuvent être enregistrés dans le SEL, quel que soit le modèle de serveur. Certaines entrées peuvent ne pas être pertinentes pour votre système.

A.2.1. Messages SEL : External Environment

Ambient Temperature: At or above upper critical threshold (going high)

Description	La température extérieure est supérieure au seuil défini. Par défaut, un arrêt a été effectué.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	22.
Actions	Vérifiez les conditions environnementales (ventilateurs, climatisation).
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Ambient Temperature: At or above upper critical threshold (going high)

Description	La température extérieure est maintenant normale.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Ambient Temperature: At or above upper non-critical threshold (going high)

Description	La température extérieure est supérieure au seuil non critique.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Vérifiez les conditions environnementales (ventilateurs, climatisation).
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Ambient Temperature: At or above upper non-critical threshold (going high)

Description	La température extérieure est maintenant normale.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.2. Messages SEL : Power system board

ACPI Pwr State: S0/G0 working

Description	Le système est démarré.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	1.
Actions	Aucune.
Commentaires	Notez qu'il n'y a pas de déassertion. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ACPI Pwr State: S4/S5 soft off

Description	Le système est arrêté.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	1.
Actions	Aucune.
Commentaires	Notez qu'il n'y a pas de déassertion. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.3. Messages SEL : Sub-chassis

Sub-Chassis: Button pressed

Description	Le bouton de mise sous tension a été pressé.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	2.
Actions	Aucune.
Commentaires	Notez qu'il n'y a pas de déassertion. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Sub-Chassis: General chassis intrusion

Description	Le boîtier est ouvert.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	35.
Actions	Fermez le boîtier.
Commentaires	Notez qu'il n'y a pas de déassertion. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Sub-Chassis: General chassis intrusion

Description	Le boîtier est maintenant fermé.
Sévérité	Return to OK.
Direction	Assertion.
Numéro du filtre	36.
Actions	Aucune.
Commentaires	Notez qu'il n'y a pas de déassertion. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.4. Messages SEL : Power Supply

PS_X: Presence detected

Description	L'alimentation PS_X est présente.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	3.
Actions	Aucune.
Commentaires	X=0, 1 ou 2. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PS_X: Presence detected

Description	L'alimentation PS_X n'est pas ou plus présente.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	6.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X=0, 1 ou 2. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PS_X: Power supply failure detected

Description	Une panne a été détectée sur l'alimentation PS_X.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	4.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X=0, 1 ou 2. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PS_X: Power supply failure detected

Description	La panne précédente sur l'alimentation PS_X a disparu.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	7.
Actions	Aucune.
Commentaires	X=0, 1 ou 2. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PS_X: Power supply input lost or out of range

Description	Une panne secteur été détectée par l'alimentation PS_X.
Sévérité	Non-critical.
Direction	Assertion.
Numéro du filtre	5.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X=0, 1 ou 2. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PS_X: Power supply input lost or out of range

Description	L'entrée secteur de l'alimentation PS_X est maintenant correcte.
Sévérité	Retour à la normale.
Direction	Deassertion.
Numéro du filtre	7.
Actions	Aucune.
Commentaires	X=0, 1 ou 2. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.5. Messages SEL : Power Unit

Pwr Redundancy: Fully redundant

Description	Les trois alimentations sont alimentés et fonctionnent.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	8.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Pwr Redundancy: Redundancy lost

Description	Deux alimentations sont alimentés et fonctionnent.
Sévérité	Non critical.
Direction	Assertion.
Numéro du filtre	9.
Actions	Dans une configuration redondante : Si le problème persiste, contactez votre ingénieur Support Technique. Dans une configuration non redondante : Aucune
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Pwr Redundancy: Non redondant. Sufficient resources from insufficient resources

Description	Deux alimentations sont alimentés et fonctionnent.
Sévérité	Non critical.
Direction	Assertion.
Numéro du filtre	9.
Actions	Dans une configuration redondante : Si le problème persiste, contactez votre ingénieur Support Technique. Dans une configuration non redondante : Aucune
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Pwr Redundancy: Non redondant. Insufficient resources

Description	Une seule alimentation est sous tension et fonctionne.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	10.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Pwr Consumption: Power Consumption Level

Description	Cet événement n'apparaît pas dans le journal SEL
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	40.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.6. Messages SEL : ILB

ILB 0.9V SD: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 0.9V SD: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 0.9V VID: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 0.9V VID: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 0.9V S MNG: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 0.9V S MNG: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 0.9V XDP: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 0.9V XDP: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.0V S GBE: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.0V S GBE: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.05V ICH: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.05V ICH: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.1V IOH0: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.1V IOH0: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.1V IOH1: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.1V IOH1: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.1V SL: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.1V SL: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.2V IB: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.2V IB: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1,2V VID: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1,2V VID: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.5V LEG: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.5V LEG: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Actions	Aucune.
Numéro du filtre	12.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.8V: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.8V: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	None (Aucune)
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.8V S: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1.8V S: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1,8V XDP: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 1,8V XDP: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 2,5V IB: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 2,5V IB: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 3,3V: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 3,3V: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 3,3V S: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 3,3V S: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 3,3V SL: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 3,3V SL: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 5V LEG: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 5V LEG: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 5V S LEG: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 5V S LEG: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 12V: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB 12V: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB Temperature: At or below lower critical threshold (going low)

Description	La température de la carte ILB est inférieure à la valeur minimum requise.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Vérifiez les conditions environnementales (ventilation, climatisation). Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB Temperature: At or above higher critical threshold (going high)

Description	La température de la carte ILB est supérieure à la valeur maximum permise.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Vérifiez les conditions environnementales (ventilation, climatisation). Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB Temperature: At or below lower critical threshold (going low)

Description	La température de la carte ILB est maintenant correcte.
Sévérité	Return to OK
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ILB Temperature: At or above higher critical threshold (going high)

Description	La température de la carte ILB est maintenant correcte.
Sévérité	Return to OK
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.7. Messages SEL : MTB/MXB

MTB/MXB 1.2V: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

MTB/MXB 1.2V: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

MTB/MXB 3.3V SD: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

MTB/MXB 3.3V SD: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

MTB/MXB 3.3V SL: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

MTB/MXB 3.3V SL: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

MTB/MXB 5V: Limit Exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

MTB/MXB 5V: Limit Exceeded

Description	Cette tension est maintenant correcte.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

MTB/MXB Temperature: At or below lower critical threshold (going low)

Description	La température de la carte MTB/MXB est inférieure à la valeur minimum requise.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Vérifiez les conditions environnementales (ventilation, climatisation). Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

MTB/MXB Temperature: At or above upper critical threshold (going high)

Description	La température de la carte MTB/MXB est supérieure à la valeur maximum permise.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Vérifiez les conditions environnementales (ventilation, climatisation). Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

MTB/MXB Temperature: At or below lower critical threshold (going low)

Description	La température de la carte MTB/MXB est maintenant correcte.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

MTB/MXB Temperature: At or above upper critical threshold (going high)

Description	La température de la carte MTB/MXB est maintenant correcte.
Sévérité	Return to OK
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.8. Messages SEL : Processor

Proc_X: Thermal trip

Description	PROC_X a atteint la température limite supérieure et s'est arrêté.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	13.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Proc_X: Thermal trip

Description	PROC_X fonctionne normalement.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	15.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Proc_X: Processor presence detected

Description	PROC_X est présent.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	14.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Proc_X: Processor presence detected

Description	PROC_X est absent.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	15.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Proc_X: Processor disabled

Description	PROC_X est désactivé.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	14.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Proc_X: Processor disabled

Description	PROC_X est activé.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	15.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Proc_X: Processor automatically throttled

Description	PROC_X dérive lentement vers la limite de température ou de consommation d'énergie.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	44.
Actions	Vérifiez les conditions environnementales (ventilation, climatisation). Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Proc_X: Processor automatically throttled

Description	PROC_X fonctionne normalement.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	16.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 1,1V: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 1,1V: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 1.8V: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 1.8V: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 1.8V MB0: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 1.8V MB0: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Numéro du filtre	12.
Direction	Deassertion.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 1.8V MB1: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 1.8V MB1: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Numéro du filtre	12.
Direction	Deassertion.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 3.3V CHAB: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 3.3V CHAB: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Numéro du filtre	12.
Direction	Deassertion.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 3.3V CHCD: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 3.3V CHCD: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 3.3V TKW: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 3.3V TKW: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 3.3V CPU: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 3.3V CPU: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 12V ARARAT: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX 12V ARARAT: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VCACHE: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VCACHE: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VCORE: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VCORE: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VIO: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VIO: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VCC 0: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VCC 0: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VCC 1: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Numéro du filtre	11.
Direction	Assertion.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VCC 1: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VTT 0: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VTT 0: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VTT 1: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Numéro du filtre	11.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VTT 1: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VDD 0: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VDD 0: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VDD 1: Limit exceeded

Description	Cette tension est hors de la plage acceptable.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	11.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PX VDD 1: Limit exceeded

Description	Cette tension est maintenant normale.
Sévérité	Information.
Direction	Deassertion.
Numéro du filtre	12.
Actions	Aucune.
Commentaires	X= de 0 à 3. Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.9. Messages SEL : Fan device / Cooling unit

FANPR_X Redund: Fan pair_X Fully redundant

Description	Les deux ventilateurs dans la paire de ventilateurs sont alimentés et fonctionnent.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	17.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

FANPR_X Redund: Fanpair_X Redundancy lost

Description	Un seul ventilateur de la paire de ventilateurs est alimenté et fonctionne.
Sévérité	Non-critical.
Direction	Assertion.
Numéro du filtre	18.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

FANPR_X Redund: Fanpair_X Non redundant: Insufficient resources

Description	Aucun ventilateur dans la paire de ventilateurs ne fonctionne.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	19.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

FAN_Y Presence: Device removed / Device absent

Description	Dans la paire de ventilateurs #X, le ventilateur #Y n'est pas ou n'est plus présent.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	20.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

FAN_Y Presence: Device inserted / Device present

Description	Dans la paire de ventilateurs #X, le ventilateur #Y est (maintenant) présent.
Sévérité	Return to OK.
Direction	Assertion.
Numéro du filtre	21.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

FAN_Y Speed: At or below lower critical threshold (going low)

Description	Dans la paire de ventilateurs #X, la vitesse du ventilateur #Y est inférieure à la vitesse minimum requise.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

FAN_Y Speed: At or below lower critical threshold (going low)

Description	Dans la paire de ventilateurs #X, le ventilateur #Y est maintenant à la vitesse normale.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

FANUNIT_X Presence: Device removed / Device absent

Description	Le bloc ventilateur #X n'est pas ou n'est plus présent.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	20.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

FANUNIT_X Presence: Device inserted / Device present

Description	Le bloc ventilateur #X est (maintenant) présent.
Sévérité	Return to OK.
Direction	Assertion.
Numéro du filtre	21.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ROTOR_XY Speed: At or below lower critical threshold (going low)

Description	Dans le bloc de ventilateurs #X, la vitesse du rotor #Y est inférieure à la vitesse minimum requise.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

ROTOR_XY Speed: At or below lower critical threshold (going low)

Description	Dans le bloc de ventilateurs #X, la vitesse du rotor #Y est maintenant normale.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.10. Messages SEL : PDB

PDB Temperature: At or below lower critical threshold (going low)

Description	La température de la carte PDB est inférieure à la valeur minimum requise.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Vérifiez les conditions environnementales (ventilation, climatisation). Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PDB Temperature: At or above higher critical threshold (going high)

Description	La température de la carte PDB est supérieure à la valeur minimum requise.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Vérifiez les conditions environnementales (ventilation, climatisation). Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PDB Temperature: At or below lower critical threshold (going low)

Description	La température de la carte PDB est maintenant normale.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

PDB Temperature: At or above higher critical threshold (going high)

Description	La température de la carte PDB est maintenant normale.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.11. Messages SEL : Ultra Capacitor

UC Failure: Battery failed

Description	Un défaut a été détecté sur l'UltraCapa (surtension, sous-tension mémorisée ou timeout du chargeur).
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	48.
Actions	Remplacer l'Ultra Capa et la carte PDBL.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC Failure: Battery failed

Description	L'UltraCapa est maintenant normale.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	49.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Disponibilité UC Device Disabled

Description	L'ultra condensateur a été désactivé suite à une erreur autre ou à une requête opérateur.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	50.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Disponibilité UC Device Enabled

Description	L'ultra condensateur est maintenant disponible.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	50.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Ultra Capa Temperature: At or below lower critical threshold (going low)

Description	La température de l'ultra condensateur est inférieure à la valeur minimum requise.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Vérifiez les conditions environnementales (ventilation, climatisation). Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Ultra Capa Temperature: At or above higher critical threshold (going high)

Description	La température de l'ultra condensateur est supérieure à la valeur minimum requise.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Vérifiez les conditions environnementales (ventilation, climatisation). Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Ultra Capa Temperature: At or below lower critical threshold (going low)

Description	La température de l'ultra condensateur est maintenant normale.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Ultra Capa Temperature: At or above higher critical threshold (going high)

Description	La température de l'ultra condensateur est maintenant normale.
Sévérité	Return to OK
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC Power Outage: State asserted

Description	Panne de courant.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	50.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC 3.3V At or below lower critical threshold (going low)

Description	Cette tension est hors de la plage acceptable.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Remplacez la carte PDB/PDBL.Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC 3.3V : At or above higher critical threshold (going high)

Description	Cette tension est hors de la plage acceptable.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Remplacez la carte PDB/PDBL.Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC 3.3V : At or below lower critical threshold (going low)

Description	Cette tension est maintenant correcte.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC 3.3V : At or above higher critical threshold (going high)

Description	Cette tension est maintenant correcte.
Sévérité	Return to OK
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC 5V At or below lower critical threshold (going low)

Description	Cette tension est hors de la plage acceptable.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Remplacez la carte PDB/PDBL.Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC 5V : At or above higher critical threshold (going high)

Description	Cette tension est hors de la plage acceptable.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Remplacez la carte PDB/PDBL.Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC 5V : At or below lower critical threshold (going low)

Description	Cette tension est maintenant correcte.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC 5V : At or above higher critical threshold (going high)

Description	Cette tension est maintenant correcte.
Sévérité	Return to OK
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC 12V At or below lower critical threshold (going low)

Description	Cette tension est hors de la plage acceptable.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Remplacez la carte PDB/PDBL.Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC 12V : At or above higher critical threshold (going high)

Description	Cette tension est hors de la plage acceptable.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Remplacez la carte PDB/PDBL.Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC 12V : At or below lower critical threshold (going low)

Description	Cette tension est maintenant correcte.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC 12V : At or above higher critical threshold (going high)

Description	Cette tension est maintenant correcte.
Sévérité	Return to OK
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC VCAP: At or above upper non-recoverable threshold (going high)

Description	Surtension sur la tension VCAP de l'ultra condensateur.
Sévérité	Non recoverable.
Direction	Assertion.
Numéro du filtre	45.
Actions	Le module a été arrêté et exclu. Le démarrage sera refusé. Pour des raisons de sécurité, déconnectez l'alimentation secteur.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC VCAP: At or above upper critical threshold (going high)

Description	Surtension sur la tension VCAP de l'ultra condensateur.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Le module a été arrêté et exclu. Le démarrage sera refusé. Pour des raisons de sécurité, déconnectez l'alimentation secteur.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC VCAP: At or above upper non-recoverable threshold (going high)

Description	La tension VCAP de l'ultra condensateur est maintenant normale.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	46.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC VCAP: At or above upper critical threshold (going high)

Description	La tension VCAP de l'Ultra Capa est maintenant normale.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC VBOOST : At or below lower critical threshold (going low)

Description	Cette tension est hors de la plage acceptable.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Remplacez la carte PDB/PDBL.Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC VBOOST : At or above higher critical threshold (going high)

Description	Cette tension est hors de la plage acceptable.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Remplacez la carte PDB/PDBL.Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC VBOOST : At or below lower critical threshold (going low)

Description	Cette tension est maintenant correcte.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC VBOOST : At or above higher critical threshold (going high)

Description	Cette tension est maintenant correcte.
Sévérité	Return to OK
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC VREF : At or below lower critical threshold (going low)

Description	Cette tension est hors de la plage acceptable.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Remplacez la carte PDB/PDBL.Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC VREF : At or above higher critical threshold (going high)

Description	Cette tension est hors de la plage acceptable.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Remplacez la carte PDB/PDBL.Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC VREF : At or below lower critical threshold (going low)

Description	Cette tension est maintenant correcte.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

UC VREF : At or above higher critical threshold (going high)

Description	Cette tension est maintenant correcte.
Sévérité	Return to OK
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.12. Messages SEL : LCP (Panneau de contrôle local)

LCP Temperature: At or below lower critical threshold (going low)

Description	La température de la carte LCP est inférieure à la valeur minimum requise.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Vérifiez les conditions environnementales (ventilation, climatisation). Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

LCP Temperature: At or above higher critical threshold (going high)

Description	La température de la carte LCP est supérieure à la valeur maximum permise.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	47.
Actions	Vérifiez les conditions environnementales (ventilation, climatisation). Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

LCP Temperature: At or below lower critical threshold (going low)

Description	La température de la carte LCP est maintenant normale.
Sévérité	Return to OK.
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

LCP Temperature: At or above higher critical threshold (going high)

Description	La température de la carte LCP est maintenant normale.
Sévérité	Return to OK
Direction	Deassertion.
Numéro du filtre	23.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.13. Messages SEL : BMC

Chipset error : Transition to Critical from less severe

Description	Une erreur de chipset non corrigible s'est produite.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	24.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Chipset error : Transition to Non-Recoverable

Description	Une erreur de chipset non corrigible s'est produite.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	24.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Chipset error : Transition to OK

Description	Retour à une température normale.
Sévérité	Return to OK.
Direction	Assertion.
Numéro du filtre	37.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Chipset error : Informational

Description	Une erreur de chipset corrigible s'est produite.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	39.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Processor Error: Transition to Critical from less severe

Description	Une erreur processeur non corrigible s'est produite.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	25.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Processor Error: Transition to Non-Recoverable

Description	Une erreur processeur non corrigible s'est produite.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	25.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Version Change: Management controller firmware change was successful

Description	Un événement changement de version s'est produit.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	26.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Version Change: Management controller firmware change was unsuccessful

Description	Un événement changement de version s'est produit.
Sévérité	Non-critical.
Direction	Deassertion.
Numéro du filtre	27.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Version Change: System firmware change was successful

Description	Un événement changement de version s'est produit.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	26.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Version Change: System firmware change was unsuccessful

Description	Un événement changement de version s'est produit.
Sévérité	Non-critical.
Direction	Deassertion.
Numéro du filtre	27.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Version Change: Programmable hardware change was successful

Description	Un événement changement de version s'est produit.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	26.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Version Change: Programmable hardware change was unsuccessful

Description	Un événement changement de version s'est produit.
Sévérité	Non-critical.
Direction	Deassertion.
Numéro du filtre	27.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Version Change: Firmware or software change

Description	Récupération du BIOS.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	41.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Sel: Sel log full

Description	Il n'y a plus de place pour un nouvel événement dans le journal SEL.
Sévérité	Non-critical.
Direction	Assertion.
Numéro du filtre	28.
Actions	Videz le journal SEL.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Sel: Sel log almost full

Description	Le journal SEL est plein à 75%.
Sévérité	Non-critical.
Direction	Assertion.
Numéro du filtre	28.
Actions	Videz le journal SEL dès que possible.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

System Event

Description	<p>Un événement de démarrage du système a eu lieu</p> <p>Données d'événement 2 [7:5] Classe de message 0 Processeur 0 erreur 1 Processeur 1 erreur 2 Processeur 2 erreur 3 Processeur 3 erreur 4 ILB erreur d'alimentation 5 erreur FPGA 6 erreur Système / Environnement 7 erreur logicielle</p> <p>[4:0] BMC/SMC étape n° : 0-31 voir Etapes de démarrage : BMC, page A-62 et Etapes de démarrage : SMC, page A-65</p> <p>Données d'événement 3 [7:6] Séquence n° 0 Séquence d'arrêt hors 1 Séquence de démarragesous 2 Séquence de réinitialisation 3 rfu</p> <p>[5:0] Erreur n° : 0-63 voir Opération de récupération dans le manuel <i>bullx S6030 Service Guide</i> ou le <i>bullx S6010 Service Guide</i>.</p>
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	29.
Actions	Voir Opération de récupération dans le manuel <i>bullx S6030 Service Guide</i> ou le <i>bullx S6010 Service Guide</i> .
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

System Event : Undetermined system hardware failure

Description	Surtension sur la tension VCAP de l'UltraCapa. Le module a été arrêté et exclu. Le démarrage sera refusé.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	29.
Actions	Pour des raisons de sécurité, déconnectez l'alimentation secteur.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Watchdog: Timeout – No specific action

Description	Expiration du délai pendant une étape d'initialisation du BIOS qui provoque l'action configurée.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	30.
Actions	Vérifiez les autres événements, puis consultez les codes POST du BIOS.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Watchdog: Timeout followed by hard reset

Description	Expiration du délai pendant une étape d'initialisation du BIOS qui provoque l'action configurée.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	30.
Actions	Vérifiez les autres événements, puis consultez les codes POST du BIOS.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Watchdog: Timeout followed by Power Down

Description	Expiration du délai pendant une étape d'initialisation du BIOS qui provoque l'action configurée.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	30.
Actions	Vérifiez les autres événements, puis consultez les codes POST du BIOS.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Watchdog: Timeout followed by power Cycle

Description	Expiration du délai pendant une étape d'initialisation du BIOS qui provoque l'action configurée.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	30.
Actions	Vérifiez les autres événements, puis consultez les codes POST du BIOS.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

Platform Security Violation Attempt: Out-of-band access password violation

Description	Un accès IPMI "out of band" a échoué à cause d'une violation de mot de passe.
Sévérité	Non-critical.
Direction	Assertion.
Numéro du filtre	31.
Actions	Information.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

System Event : Entry added to Auxiliary Log

Description	Une erreur machine corrigée a été consignée par le BIOS dans la zone non volatile.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	32.
Actions	Analysez le journal avec la console iCare.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

System Event : Entry added to Auxiliary Log

Description	Une erreur machine non corrigée a été consignée par le BIOS dans la zone non volatile.
Sévérité	Critical.
Direction	Assertion.
Numéro du filtre	33.
Actions	Analysez le journal avec la console iCare.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

System Event : Entry added to Auxiliary Log

Description	Une erreur machine fatale a été consignée par le BIOS dans la zone non volatile.
Sévérité	Non-recoverable.
Direction	Assertion.
Numéro du filtre	34.
Actions	Analysez le journal avec la console iCare.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

System Boot Init : Initiated by Hard Reset

Description	System Boot Init.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	42.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

System Boot Init : OS / Run-time Software Initiated (Hard/Warm) Reset

Description	System boot init.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	42.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

System Boot Init : System Restart

Description	System boot init.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	42.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

OS Stop : OS Graceful Stop

Description	Arrêt OS.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	43.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

OS Stop : OS Graceful Shutdown

Description	Arrêt OS.
Sévérité	Information.
Direction	Assertion.
Numéro du filtre	43.
Actions	Aucune.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.14. Messages SEL : Memory

DIMM_X: Correctable ECC threshold reached

Description	Le seuil des ECC corrigibles a été atteint sur la DIMM_X
Sévérité	Warning.
Direction	Assertion.
Numéro du filtre	38.
Actions	Si le problème persiste, contactez votre ingénieur Support Technique.
Commentaires	Pour plus d'informations sur les filtres, voir Configuration des alertes, page 6-50.

A.2.15. Etapes de démarrage : BMC

Séquence n° = 1	Etape	Action (carte MTB)	Action (carte MXB)
Démarrage en mode normal	0	[BMC PWR] Structure de composition de la partition du build	[BMC PWR] Structure de composition de la partition du build
	1	[BMC PWR] Démarrage du serveur	[BMC PWR] Démarrage du serveur
	2	[BMC PWR] Réception d'une réponse SMC	[BMC PWR] Réception d'une réponse SMC
	3	[BMC PWR] Mise à jour de la présence matérielle dans SMC	[BMC PWR] Mise à jour de la présence matérielle dans SMC
	4	[BMC PWR] Démarrer les registres scratchpad	[BMC PWR] Démarrer les registres scratchpad
	5	[BMC PWR] Démarrer l'horloge du chien de garde IPMI	[BMC PWR] Démarrer l'horloge du chien de garde IPMI
	6	[BMC PWR] Reprendre l'initialisation du BIOS	[BMC PWR] Reprendre l'initialisation du BIOS
	7	[BMC PWR] Set ACPI legacy on state	[BMC PWR] Set ACPI legacy on state

Séquence n° = 1	Etape	Action (carte MTB)	Action (carte MXB)
Power ON en veille légère	0	[BMC PWR] Démarrage en mode veille légère	[BMC PWR] Démarrage en mode veille légère
	1	[BMC PWR] Réception d'une réponse SMC	[BMC PWR] Réception d'une réponse SMC
	2	[BMC PWR] Set ACPI legacy on state	[BMC PWR] Set ACPI legacy on state
Démarrage en mode veille prolongée	0	[BMC PWR] Démarrage en mode veille prolongée	[BMC PWR] Démarrage en mode veille prolongée
	1	[BMC PWR] Réception d'une réponse SMC	[BMC PWR] Réception d'une réponse SMC
	2	[BMC PWR] Set ACPI legacy on state	[BMC PWR] Set ACPI legacy on state
Démarrer en mode bios nord	0	[BMC PWR] Structure de composition de la partition du build	[BMC PWR] Structure de composition de la partition du build
	1	[BMC PWR] Démarrage du serveur en mode bios nord	[BMC PWR] Démarrage du serveur en mode bios nord
	2	[BMC PWR] Réception d'une réponse SMC	[BMC PWR] Réception d'une réponse SMC
	3	[BMC PWR] Set ACPI legacy on state	[BMC PWR] Set ACPI legacy on state
	4		[BMC PWR] Démarrer les registres scratchpad
	5		[BMC PWR] Démarrer l'horloge du chien de garde IPMI
	6		[BMC PWR] Reprendre l'initialisation du BIOS
	7		[BMC PWR] Set ACPI legacy on state

Séquence n° = 0	Etape	Action (carte MTB)	Action (carte MXB)
Arrêt en mode normal	0	[BMC PWR] Arrêter l'horloge du chien de garde IPMI	[BMC PWR] Arrêter l'horloge du chien de garde IPMI
	1	[BMC PWR] Arrêter le serveur	[BMC PWR] Arrêter le serveur
	2	[BMC PWR] Réception d'une réponse SMC	[BMC PWR] Réception d'une réponse SMC
	3	[BMC PWR] Set ACPI legacy on state	[BMC PWR] Set ACPI legacy on state
Arrêt en veille prolongée	0	[BMC PWR] Arrêter le serveur	[BMC PWR] Arrêter le serveur
	1	[BMC PWR] Réception d'une réponse SMC	[BMC PWR] Réception d'une réponse SMC
	2	[BMC PWR] Set ACPI legacy on state	[BMC PWR] Set ACPI legacy on state
Arrêt en veille prolongée	0	[BMC PWR] Arrêt en veille prolongée	[BMC PWR] Arrêt en veille prolongée
	1	[BMC PWR] Réception d'une réponse SMC	[BMC PWR] Réception d'une réponse SMC
	2	[BMC PWR] Set ACPI legacy on state	[BMC PWR] Set ACPI legacy on state
Arrêter en mode bios nord	0	[BMC PWR] Arrêt du serveur en mode bios nord	[BMC PWR] Arrêt du serveur en mode bios nord
	1	[BMC PWR] Réception d'une réponse SMC	[BMC PWR] Réception d'une réponse SMC
	2	[BMC PWR] Set ACPI legacy on state	[BMC PWR] Set ACPI legacy on state

Séquence n° = 2	Etape	Action (carte MTB)	Action (carte MXB)
Warm Reset (Redémarrage à chaud)	0	[BMC PWR] edémarrer le serveur	[BMC PWR] edémarrer le serveur
	1	[BMC PWR] Réception d'une réponse SMC	[BMC PWR] Réception d'une réponse SMC
	2	[BMC PWR] Démarrer l'horloge du chien de garde IPMI	[BMC PWR] Démarrer l'horloge du chien de garde IPMI
	3	[BMC PWR] Reprendre l'initialisation du BIOS	[BMC PWR] Reprendre l'initialisation du BIOS

A.2.16. Etapes de démarrage : SMC

Séquence n° = 1	Etape	Action (carte MTB)	Action (carte MXB)
Démarrage en mode normal	0	[SMC PWR] Affichage LCP au démarrage	[SMC PWR] Affichage LCP au démarrage
	1	[SMC PWR] Vérifiez que ILBC est chargé	[SMC PWR] Vérifiez que ILBC est chargé
	2	[SMC PWR] Vérifiez la redondance de l'alimentation	[SMC PWR] Démarrer le 12v des alimentations
	3	[SMC PWR] Démarrer le 12v des alimentations	[SMC PWR] Démarrer les ventilateurs
	4	[SMC PWR] Démarrer les ventilateurs	[SMC PWR] Vérifiez les firmwares ADM1069
	5	[SMC PWR] Vérifiez les firmwares ADM1069	[SMC PWR] Charger MTBC FPGA
	6	[SMC PWR] Charger MTBC FPGA	[SMC PWR] Vérifiez que ILBC est chargé
	7	[SMC PWR] Vérifiez que MTBC est chargé	[SMC PWR] Obtenir la configuration du module
	8	[SMC PWR] Configurer le mode réinitialisation FPGA	[SMC PWR] Configurer le mode réinitialisation FPGA
	9	[SMC PWR] Démarrer les tensions de veille légère	[SMC PWR] Configurer les modes FPGA CPU
	10	[SMC PWR] La condition en veille légère est vraie	[SMC PWR] Activer les pilotes d'horloge
	11	[SMC PWR] Impulsion du signal PWRBTN	[SMC PWR] Démarrer les tensions de veille légère
	12	[SMC PWR] Obtenir la configuration du module	[SMC PWR] La condition en veille légère est vraie
	13	[SMC PWR] Configurer les modes FPGA CPU	[SMC PWR] Impulsion du signal PWRBTN
	14	[SMC PWR] Démarrer les tensions principales ILBC	[SMC PWR] Démarrer les tensions principales
	15	[SMC PWR] Démarrer les tensions principales MTBC	[SMC PWR] La condition alimentation principale est vraie
	16	[SMC PWR] La condition alimentation principale est vraie	[SMC PWR] Affichage LCP Démarrage du BIOS
	17	[SMC PWR] Activer les pilotes d'horloge	[SMC PWR] Vérifiez que le signal PLTRST soit déasserté
	18	[SMC PWR] Assertion de l'alimentation XDP bonne	[SMC PWR] La condition d'accès au chipset est vraie
	19	[SMC PWR] La condition d'accès au chipset est vraie	[SMC PWR] Vérifiez le mode processor boot
	20	[SMC PWR] Assertion de l'alimentation IOH bonne	[SMC PWR] Led verte du LCP allumée
	21	[SMC PWR] Affichage LCP Démarrage du BIOS	[SMC PWR] Le serveur est arrêté

Séquence n° = 1	Etape	Action (carte MTB)	Action (carte MXB)
	22	[SMC PWR] Assertion de l'alimentation ICH bonne	[SMC PWR] La condition surveillance est vraie
	23	[SMC PWR] Vérifiez que le signal PLTRST soit déasserté	[SMC PWR] Set OS running
	24	[SMC PWR] La condition d'accès au chipset est vraie	
	25	[SMC PWR] Vérifiez le mode processor boot	
	26	[SMC PWR] Led verte du LCP allumée	
	27	[SMC PWR] Le serveur est arrêté	
	28	[SMC PWR] La condition surveillance est vraie	
	29	[SMC PWR] Set OS running	

Séquence n° = 1	Etape	Action (carte MTB)	Action (carte MXB)
Démarrage en mode veille prolongée	0	[SMC PWR] Le serveur est arrêté	[SMC PWR] Le serveur est arrêté

Séquence n° = 1	Etape	Action (carte MTB)	Action (carte MXB)
Power ON en veille légère	0	[SMC PWR] Affichage LCP au démarrage	[SMC PWR] Affichage LCP au démarrage
	1	[SMC PWR] Vérifiez que ILBC est chargé	[SMC PWR] Vérifiez que ILBC est chargé
	2	[SMC PWR] Démarrer le 12v des alimentations	[SMC PWR] Démarrer le 12v des alimentations
	3	[SMC PWR] Démarrer les ventilateurs	[SMC PWR] Démarrer les ventilateurs
	4	[SMC PWR] Charger MTBC FPGA	[SMC PWR] Charger MTBC FPGA
	5	[SMC PWR] Vérifiez que MTBC est chargé	[SMC PWR] Vérifiez que ILBC est chargé
	6	[SMC PWR] Configurer le mode réinitialisation FPGA	[SMC PWR] Configurer le mode réinitialisation FPGA
	7	[SMC PWR] Démarrer les tensions de veille légère	[SMC PWR] Démarrer les tensions de veille légère
	8	[SMC PWR] La condition en veille légère est vraie	[SMC PWR] La condition en veille légère est vraie
	9	[SMC PWR] Led verte du LCP allumée	[SMC PWR] Led verte du LCP allumée
	10	[SMC PWR] Affichage LCP en veille légère	[SMC PWR] Affichage LCP en veille légère
	11	[SMC PWR] Le serveur est arrêté	[SMC PWR] Le serveur est arrêté

Séquence n° = 1	Etape	Action (carte MTB)	Action (carte MXB)
Démarrer en mode bios nord	0	[SMC PWR] Affichage LCP au démarrage	[SMC PWR] Affichage LCP au démarrage
	1	[SMC PWR] Vérifiez que ILBC est chargé	[SMC PWR] Vérifiez que ILBC est chargé
	2	[SMC PWR] Démarrer le 12v des alimentations	[SMC PWR] Démarrer le 12v des alimentations
	3	[SMC PWR] Démarrer les ventilateurs	[SMC PWR] Démarrer les ventilateurs
	4	[SMC PWR] Vérifiez les firmwares ADM1069	[SMC PWR] Vérifiez les firmwares ADM1069
	5	[SMC PWR] Charger MTBC FPGA	[SMC PWR] Charger MTBC FPGA
	6	[SMC PWR] Vérifiez que MTBC est chargé	[SMC PWR] Vérifiez que ILBC est chargé
	7	[SMC PWR] Configurer le mode réinitialisation FPGA	[SMC PWR] Obtenir la configuration du module
	8	[SMC PWR] Démarrer les tensions de veille légère	[SMC PWR] Configurer le mode réinitialisation FPGA
	9	[SMC PWR] La condition en veille légère est vraie	[SMC PWR] Configurer les modes FPGA CPU
	10	[SMC PWR] Impulsion du signal PWRBTN	[SMC PWR] Activer les pilotes d'horloge
	11	[SMC PWR] Obtenir la configuration du module	[SMC PWR] Démarrer les tensions de veille légère
	12	[SMC PWR] Configurer les modes FPGA CPU	[SMC PWR] La condition en veille légère est vraie
	13	[SMC PWR] Démarrer les tensions principales ILBC	[SMC PWR] Impulsion du signal PWRBTN
	14	[SMC PWR] Démarrer les tensions principales MTBC	[SMC PWR] Démarrer les tensions principales
	15	[SMC PWR] La condition alimentation principale est vraie	[SMC PWR] La condition alimentation principale est vraie
	16	[SMC PWR] Activer les pilotes d'horloge	[SMC PWR] Affichage LCP Démarrage du BIOS
	17	[SMC PWR] Assertion de l'alimentation XDP bonne	[SMC PWR] Vérifiez que le signal PLTRST soit déasserté
	18	[SMC PWR] Assertion de l'alimentation des processeurs bonne	[SMC PWR] La condition d'accès au chipset est vraie
	19	[SMC PWR] Assertion de l'alimentation IOH bonne	[SMC PWR] Vérifiez le mode processor boot
	20	[SMC PWR] Affichage LCP mise à jour du BIOS	[SMC PWR] Led verte du LCP allumée
	21	[SMC PWR] Assertion de l'alimentation ICH bonne	[SMC PWR] Le serveur est arrêté
	22	[SMC PWR] Vérifiez que le signal PLTRST soit déasserté	[SMC PWR] La condition surveillance est vraie

Séquence n° = 1	Etape	Action (carte MTB)	Action (carte MXB)
	23	[SMC PWR] La condition d'accès au chipset est vraie	[SMC PWR] Set OS running
	24	[SMC PWR] Vérifiez le mode processor boot	
	25	[SMC PWR] Led verte du LCP allumée	
	26	[SMC PWR] Le serveur est arrêté	

Séquence n° = 0	Etape	Action (carte MTB)	Action (carte MXB)
Arrêt en mode normal	0	[SMC PWR] Affichage LCP arrêt	[SMC PWR] Affichage LCP arrêt
	1	[SMC PWR] Reset OS running	[SMC PWR] Reset OS running
	2	[SMC PWR] La condition surveillance est fausse	[SMC PWR] La condition surveillance est fausse
	3	[SMC PWR] La condition d'accès au chipset est fausse	[SMC PWR] La condition d'accès au chipset est fausse
	4	[SMC PWR] Déassertion de l'alimentation ICH bonne	[SMC PWR] La condition alimentation principale est fausse
	5	[SMC PWR] Déassertion de l'alimentation IOH bonne	[SMC PWR] Arrêt des tensions principales
	6	[SMC PWR] Déassertion de l'alimentation des processeurs bonne	[SMC PWR] La condition veille légère est fausse
	7	[SMC PWR] Déassertion de l'alimentation XDP bonne	[BMC PWR] Arrêt des tensions de veille légère
	8	[SMC PWR] Désactiver les pilotes d'horloge	[SMC PWR] Désactiver les pilotes d'horloge
	9	[SMC PWR] La condition alimentation principale est fausse	[SMC PWR] Réinitialiser le mode réinitialisation FPGA
	10	[SMC PWR] Arrêt des tensions principales MTBC	[SMC PWR] Arrêter les ventilateurs
	11	[SMC PWR] Arrêter les tensions principales ILBC	[SMC PWR] Arrêter le 12V des alimentations
	12	[SMC PWR] La condition veille légère est fausse	[SMC PWR] Led verte du LCP clignotante
	13	[BMC PWR] Arrêt des tensions de veille légère	[SMC PWR] Le serveur est arrêté
	14	[SMC PWR] Réinitialiser le mode réinitialisation FPGA	
	15	[SMC PWR] Arrêter les ventilateurs	
	16	[SMC PWR] Arrêter le 12v des alimentations	
	17	[SMC PWR] Led verte du LCP clignotante	

Séquence n° = 0	Etape	Action (carte MTB)	Action (carte MXB)
	18	[SMC PWR] Le serveur est arrêté	

Séquence n° = 0	Etape	Action (carte MTB)	Action (carte MXB)
Arrêt en veille prolongée	0	[SMC PWR] Affichage LCP arrêt	[SMC PWR] Affichage LCP arrêt
	1	[SMC PWR] La condition veille légère est fausse	[SMC PWR] La condition veille légère est fausse
	2	[BMC PWR] Arrêt des tensions de veille légère	[BMC PWR] Arrêt des tensions de veille légère
	3	[SMC PWR] Réinitialiser le mode réinitialisation FPGA	[SMC PWR] Réinitialiser le mode réinitialisation FPGA
	4	[SMC PWR] Arrêter les ventilateurs	[SMC PWR] Arrêter les ventilateurs
	5	[SMC PWR] Arrêter le 12v des alimentations	[SMC PWR] Arrêter le 12v des alimentations
	6	[SMC PWR] Led verte du LCP clignotante	[SMC PWR] Led verte du LCP clignotante
	7	[SMC PWR] Le serveur est arrêté	[SMC PWR] Le serveur est arrêté

Séquence n° = 0	Etape	Action (carte MTB)	Action (carte MXB)
Arrêt en veille prolongée	0	[SMC PWR] Le serveur est arrêté	[SMC PWR] Le serveur est arrêté

Séquence n° = 0	Etape	Action (carte MTB)	Action (carte MXB)
Arrêter en mode bios nord	0	[SMC PWR] Affichage LCP arrêt	[SMC PWR] Affichage LCP arrêt
	1	[SMC PWR] La condition d'accès au chipset est fausse	[SMC PWR] Reset OS running
	2	[SMC PWR] Déassertion de l'alimentation ICH bonne	[SMC PWR] La condition surveillance est fausse
	3	[SMC PWR] Déassertion de l'alimentation IOH bonne	[SMC PWR] La condition d'accès au chipset est fausse
	4	[SMC PWR] Déassertion de l'alimentation des processeurs bonne	[SMC PWR] La condition alimentation principale est fausse
	5	[SMC PWR] Déassertion de l'alimentation XDP bonne	[SMC PWR] Arrêt des tensions principales
	6	[SMC PWR] Désactiver les pilotes d'horloge	[SMC PWR] La condition veille légère est fausse
	7	[SMC PWR] La condition alimentation principale est fausse	[SMC PWR] Démarrer les tensions de veille légère
	8	[SMC PWR] Arrêt des tensions principales MTBC	[SMC PWR] Désactiver les pilotes d'horloge

Séquence n° = 0	Etape	Action (carte MTB)	Action (carte MXB)
	9	[SMC PWR] Arrêter les tensions principales ILBC	[SMC PWR] Réinitialiser le mode réinitialisation FPGA
	10	[SMC PWR] La condition veille légère est fausse	[SMC PWR] Arrêter les ventilateurs
	11	[BMC PWR] Arrêt des tensions de veille légère	[SMC PWR] Arrêter le 12v des alimentations
	12	[SMC PWR] Réinitialiser le mode réinitialisation FPGA	[SMC PWR] Led verte du LCP clignotante
	13	[SMC PWR] Arrêter les ventilateurs	[SMC PWR] Le serveur est arrêté
	14	[SMC PWR] Arrêter le 12v des alimentations	
	15	[SMC PWR] Led verte du LCP clignotante	
	16	[SMC PWR] Le serveur est arrêté	

Annexe B. Console Serial-Over-LAN

Cette annexe explique comment configurer et utiliser la console Serial-Over-LAN (SOL). Il comprend les rubriques suivantes :

- Présentation de la console SOL, page B-2
- Utilisation de la console SOL avec ipmitool, page B-3
- Utilisation de la console SOL avec telnet, page B-5

B.1. Présentation de la console SOL

L'outil IPMI Serial-Over-Lan (SOL) fournit un accès réseau au système, via le contrôleur de gestion intégré (BMC) de la carte mère, vous permettant de visualiser à distance la console textuelle et d'effectuer des diagnostics et des tâches de réparation telles que :

- reconfigurer le système d'exploitation ou lancer des utilitaires,
- afficher à distance des séquences de démarrage,
- recevoir des alertes et afficher des messages,
- configurer le BIOS à distance.

Pour plus de détails sur les options de la console SOL, consultez la documentation *ipmitool* livrée sur le *CD-ROM de Ressource et de Documentation* et la documentation *telnet* livrée avec le système d'exploitation.

Note Une seule console SOL peut être ouverte à la fois.



Important SOL nécessite la version BIOS 01.003.00.014 ou supérieure et le firmware Hardware Console Firmware Build Number 1033 ou supérieur.

Il existe deux méthodes pour accéder à la console SOL :

- *ipmitool* pour les systèmes d'exploitation Linux,
 - *telnet* pour les systèmes d'exploitation Linux et Windows.
-



Important Pour pouvoir utiliser la console SOL, vous devez :

- configurer le BIOS,
 - configurer le réseau requis et les permissions SOL depuis le contrôleur de gestion intégré (BMC) console matérielle
 - installer le cas échéant les packages *ipmitool* et *telnet*,
 - procéder aux tâches de configuration nécessaires du système d'exploitation. Pour plus de détails, consultez la documentation livrée avec le système d'exploitation.
-

B.2. Utilisation de la console SOL avec ipmitool

La commande ipmitool peut être utilisée pour se connecter à la console SOL avec un système d'exploitation Linux.

Prérequis

- Le BIOS est configuré
- Le réseau et les permissions SOL sont configurés sur la console matérielle
- Le package ipmitools est installé
- Le système d'exploitation est configuré

Procédure

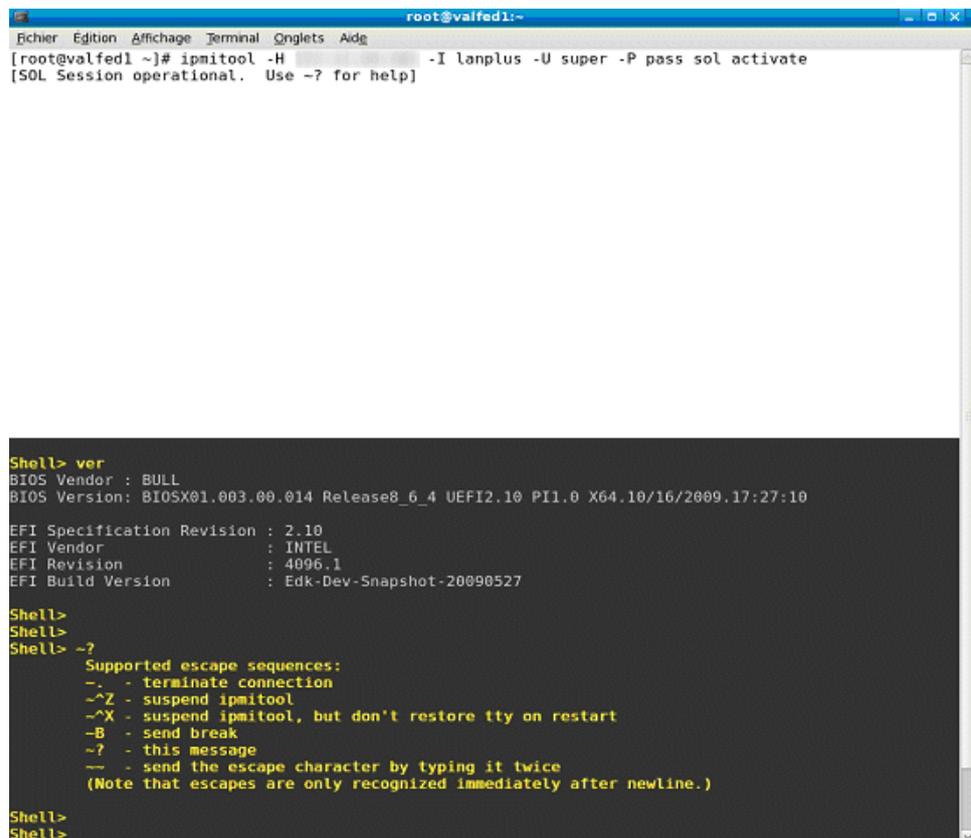
Cette procédure explique comment ouvrir et fermer la console SOL avec la commande ipmitool

1. Ouvrez une session Linux
2. Ouvrez la console SOL en lançant la commande suivante :

```
ipmitool -H <Adresse IP ou nom d'hôte BMC> -I lanplus -U <utilisateur> -P <mot de passe> sol activate
```

Un écran de session SOL s'ouvre.

3. Appuyez sur Entrée pour prendre le contrôle du système distant.
4. Appuyez sur <~ ?> pour afficher l'aide ipmi sol.



```
root@valfed1~# ipmitool -H -I lanplus -U super -P pass sol activate
[SOL Session operational. Use -? for help]

Shell> ver
BIOS Vendor : BULL
BIOS Version: BIOSX01.003.00.014 Release8_6_4 UEFI2.10 PI1.0 X64.10/16/2009.17:27:10

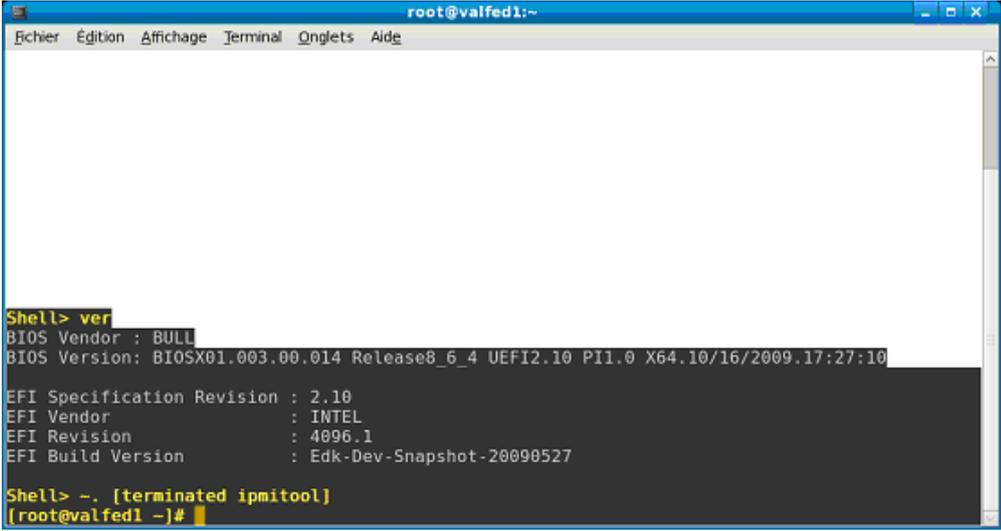
EFI Specification Revision : 2.10
EFI Vendor : INTEL
EFI Revision : 4096.1
EFI Build Version : Edk-Dev-Snapshot-20090527

Shell>
Shell>
Shell> -?
Supported escape sequences:
- . - terminate connection
- ^Z - suspend ipmitool
- ^X - suspend ipmitool, but don't restore tty on restart
- B - send break
- ? - this message
- ~ - send the escape character by typing it twice
(Note that escapes are only recognized immediately after newline.)

Shell>
Shell>
```

Figure B-1. Console SOL - Lancement avec ipmitool

5. Fermez la console SOL en appuyant sur <~.>.



```
root@valfed1:~  
Bichier  Édition  Affichage  Terminal  Onglets  Aide  
  
Shell> ver  
BIOS Vendor : BULL  
BIOS Version: BIOSX01.003.00.014 Release8_6_4 UEF12.10 P11.0 X64.10/16/2009.17:27:10  
EFI Specification Revision : 2.10  
EFI Vendor : INTEL  
EFI Revision : 4096.1  
EFI Build Version : Edk-Dev-Snapshot-20090527  
  
Shell> ~. [terminated ipmitool]  
[root@valfed1 ~]#
```

Figure B-2. Console SOL - Fermeture avec ipmitool

B.3. Utilisation de la console SOL avec telnet

La commande `telnet` peut être utilisée pour se connecter à la console SOL avec un système d'exploitation Linux ou Windows.

Prérequis

Le BIOS est configuré

Le réseau et les permissions SOL sont configurés sur la console matérielle

`telnet` est installé

Le système d'exploitation est configuré

Procédure

Cette procédure explique comment ouvrir et fermer la console SOL avec la commande `telnet`

1. Ouvrez une session Linux ou Windows.
2. Lancez la commande `telnet` sur le Port 23.

Un écran de session telnet s'ouvre.

3. Entrez l'identifiant et le mot de passe du contrôleur de gestion intégré (BMC).

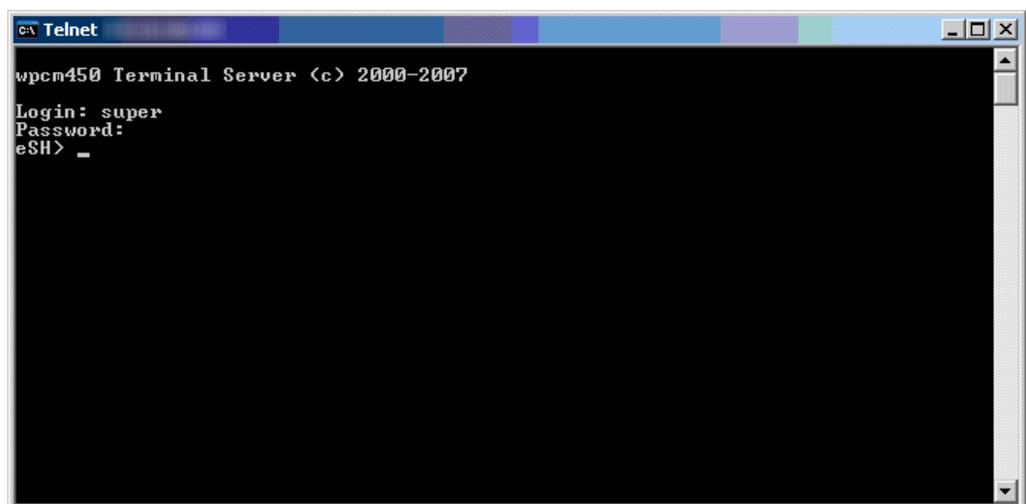
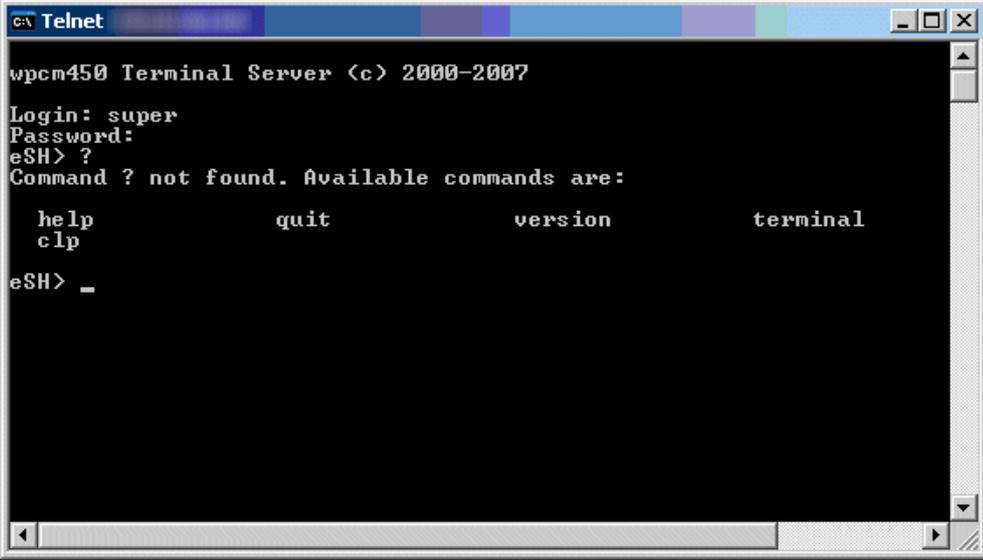


Figure B-3. Session telnet

4. Appuyez sur <?> pour afficher les commandes disponibles



```

c:\ Telnet
wpcm450 Terminal Server (c) 2000-2007
Login: super
Password:
eSH> ?
Command ? not found. Available commands are:

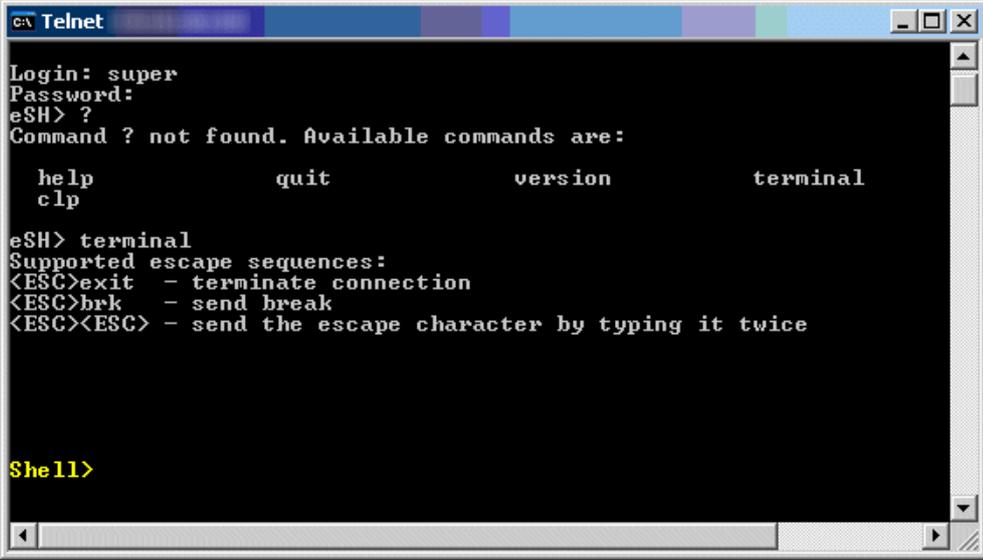
  help          quit          version       terminal
  clp

eSH> _

```

Figure B-4. Commandes telnet

5. Entrez `terminal` et appuyez sur Entrée DEUX fois pour ouvrir la console SOL et prendre le contrôle du système distant.



```

c:\ Telnet
Login: super
Password:
eSH> ?
Command ? not found. Available commands are:

  help          quit          version       terminal
  clp

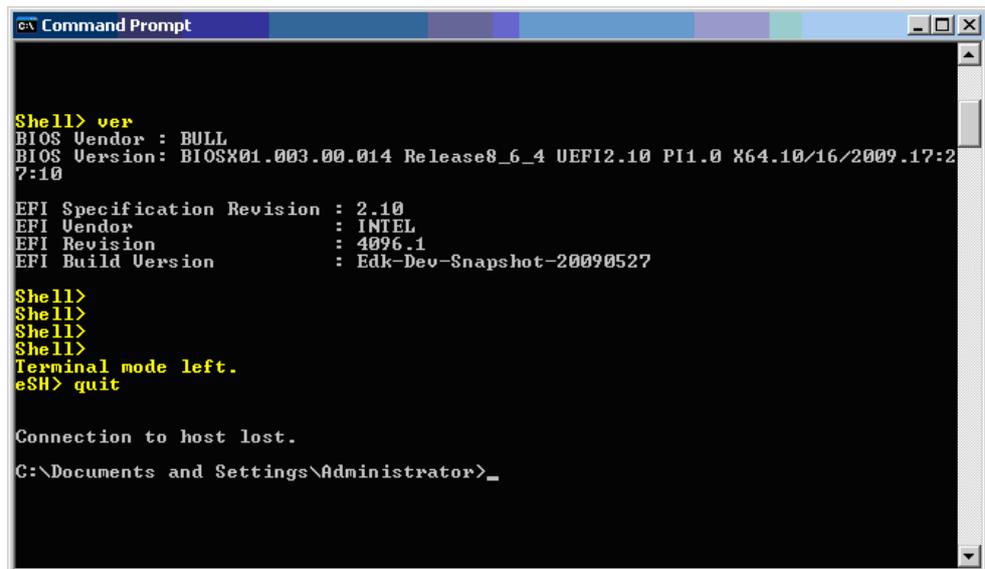
eSH> terminal
Supported escape sequences:
<ESC>exit - terminate connection
<ESC>brk  - send break
<ESC><ESC> - send the escape character by typing it twice

She11>

```

Figure B-5. Console SOL - Lancement avec telnet

6. _Fermez la console SOL en appuyant sur la touche <Échap> et en entrant exit simultanément.
7. Entrez quit pour fermer la session.



```
c:\ Command Prompt

Shell> ver
BIOS Vendor : BULL
BIOS Version: BIOSX01.003.00.014 Release8_6_4 UEFI2.10 PI1.0 X64.10/16/2009.17:27:10

EFI Specification Revision : 2.10
EFI Vendor : INTEL
EFI Revision : 4096.1
EFI Build Version : Edk-Dev-Snapshot-20090527

Shell>
Shell>
Shell>
Shell>
Terminal mode left.
eSH> quit

Connection to host lost.
C:\Documents and Settings\Administrator>_
```

Figure B-6. Console SOL - Fermeture avec telnet

Glossaire

A

ABR

Automatic BIOS Recovery.

ACPI

Advanced Configuration and Power Interface.

Norme industrielle permettant une meilleure gestion de l'alimentation des ordinateurs portables et de bureau. L'ACPI détermine la façon dont le BIOS, le système d'exploitation et les périphériques d'un ordinateur communiquent entre eux concernant la gestion de l'alimentation.

ADM1069

L'ADM1069 Super Sequencer® est un périphérique de supervision / séquençage configurable qui offre une solution mono-puce permettant la surveillance et le séquençage dans des systèmes d'alimentation multiples.

ARU

Add / Removeable Unit. Une unité logique matérielle ou un groupe d'unités logiques, qui peuvent être affichées / traitées par un système d'exploitation, ou par le BIOS, ou par le logiciel de gestion de la plateforme. Une ARU peut être imbriquée et n'est pas nécessairement séparable des autres ARU. Une ARU est également connue sous l'acronyme PMU.

ASR

Automatic Server Restart.

ASIC

Application Specific Integrated Circuit.

B

BCE

Elementary calculation block (bloc de calcul élémentaire).

BCEA

ASIC elementary calculation block (bloc de calcul élémentaire ASIC).

BCEF

FPGA elementary calculation block (bloc de calcul élémentaire FPGA).

BCS

Bull Coherence Switch. C'est le contrôleur de noeuds externes de Bull permettant l'évolution de SMP jusqu'à 16 processeurs. Le BCS assure la cohérence de la mémoire globale et cache, avec un trafic optimisé et des latences, dans les variantes avec IPF et XPF.

BHC

Voir Blade Hardware Console (Console matérielle du Blade).

BIOS

Basic Input / Output System. Programme stocké dans une mémoire flash EPROM ou ROM et qui commande le processus de démarrage du système.

BIST

Built-In Self-Test. Voir POST.

Blade Hardware Console (Console BHC)

Interface graphique utilisateur utilisée pour accéder au logiciel de gestion intégré dans le module lame.

BMC

Baseboard Management Controller. Voir Contrôleur de gestion intégré.

BOOTP

Protocole réseau utilisé par un client réseau pour obtenir une adresse IP depuis une configuration de serveur.

BT

Block Transfer. Une des trois interfaces standardisées IPMI utilisée par le logiciel du système pour transférer des messages IPMI au BMC. Un établissement de liaison par bloc est utilisé pour transférer des données (performance supérieure).

C**Chassis Hardware Console (Console CHC)**

Interface graphique utilisateur utilisée pour accéder au logiciel de gestion intégré dans le module de gestion du châssis.

CHC

Voir Chassis Hardware Console (Console matérielle du châssis).

Clipping | Ecrêtage

Un critère de filtrage d'événements. L'ecrêtage est défini selon un critère Nombre / Temps destiné au routage d'un nombre prédéfini de messages. Les messages identiques sont décomptés et lorsque le nombre de messages indiqué dans la zone Count (Nombre) est atteint dans le délai précisé dans la zone Time (Temps), aucun autre message ne sera sélectionné pour le routage.

CMB

Chassis Management Board.

CMC

Une condition Corrected Memory Check est signalée lorsqu'un matériel corrige une erreur machine ou lorsqu'une condition MCA est corrigée par un firmware. Voir MCA.

CMC

Chassis Management Controller.

CMM

Chassis Management Module.

Contrôleur de gestion intégré

Connu également sous l'acronyme BMC (Baseboard Management Controller). Ce contrôleur, intégré sur la carte principale du système, fournit un accès hors bande à l'instrumentation de la plateforme, aux capteurs et aux effecteurs.

Core | Noyau

Core est le nom abrégé pour le noyau d'exécution de processeur mis en œuvre sur un processeur. Un noyau contient un ou plusieurs threads (processeurs logiques).

CRU

Customer Replaceable Unit. Un composant (carte, module, ventilateur, bloc d'alimentation, etc.) qui est remplacé ou ajouté par l'utilisateur final comme une entité unique.

CSE

Customer Service Engineer.

D**DES**

Data Encryption Standard.

DHCP

Dynamic Host Configuration Protocol.

DMA

Direct Memory Access. Permet l'envoi de données directement depuis un composant (un lecteur de disque, par exemple) vers la mémoire de la carte mère. Le microprocesseur n'intervient pas dans l'amélioration des performances système du transfert de données.

DNS

Domain Name Server.

E**EEPROM**

Electrically Erasable Programmable Read-Only Memory. Type de mémoire qui stocke le mot de passe et les données de configuration.

EFI

Extensible Firmware Interface. Une spécification de l'interface firmware-Système d'exploitation.

EFI Shell

Interface utilisateur simple, interactive qui permet aux pilotes de périphériques EFI d'être chargés, aux applications EFI d'être lancées et au système d'exploitation d'être démarré. De plus, le shell EFI offre un ensemble de commandes de base utilisées pour gérer les fichiers et les variables d'environnement du système. Voir Shell

EMM

System Management Bus. Logiciel intégré dans le module du serveur pour mettre en œuvre les fonctions de gestion et accessible depuis l'interface graphique de la console matérielle.

EPROM

Erasable Programmable Read-Only Memory. Type de mémoire utilisé pour stocker le code du BIOS du système. Ce code n'est pas perdu lors de l'arrêt de l'ordinateur.

ESB

Ethernet Switch Board.

ESM

Ethernet Switch Module.

F**FC-LGA**

Flip-Chip Land Grid Array.

Flash EPROM

Flash Erasable Programmable Read-Only Memory. Type de mémoire utilisé pour stocker le code du firmware du système. Ce code peut être remplacé par un code mis à jour depuis une disquette, mais n'est pas perdu lors de l'arrêt du système.

FPGA

Field Programmable Gate Array.

FQDN

Fully Qualified Domain Name.

FRU

Field Replaceable Unit. Composant (carte, module, ventilateur, bloc d'alimentation, etc.) remplacé ou ajouté par des Ingénieurs Support Technique en tant qu'entité unique.

G**GPU**

Graphical Processing Unit.

GUI

Graphical User Interface.

H

HA

High Availability | Haute disponibilité. Désigne un système ou un composant opérationnel continuellement pendant une longue période de temps.

Hardware | Matériel

Les composants physiques d'un système, notamment le clavier, le moniteur, les lecteurs de disque, les câbles et les cartes de circuit imprimé.

Hardware Partition (Partition matérielle)

Un ensemble de composants matériels qui peut démarrer et lancer une image OS de base.

Hard Partitioning (Partitionnement matériel)

Capacité à scinder une plateforme en plusieurs partitions matérielles plus petites et indépendantes ou à réunir plusieurs partitions matérielles indépendantes pour former une plateforme matérielle unique plus grande.

HPC

High Performance Computing.

HPC Cluster

High Performance Computing Cluster. Un groupe d'ordinateurs reliés pour constituer un ordinateur unique

Host Operating System | Système d'exploitation hôte

Le système d'exploitation qui est démarré à l'initialisation et qui est un Virtual Machine Monitor (VMM) et plusieurs OS invités.

Hot-Plugging | Connexion à chaud

Opération qui consiste à ajouter un composant sans interrompre l'activité du système.

Hot-Swapping | Remplacement à chaud

Opération qui consiste à retirer et à remplacer un composant défectueux sans interrompre l'activité du système.

HT

HyperThreading. Voir Multi-Threading.

I

I2C

Intra Integrated Circuit. Le bus I2C (Inter-IC) est un bus série bifilaire et bidirectionnel qui établit une liaison entre les circuits intégrés (IC). Le bus I2C prend en charge des périphériques d'espaces d'adressage 7 bits et 10 bits et des périphériques qui fonctionnent à différentes tensions.

IB

InfiniBand.

iBMC

Integrated Baseboard Management Controller. Voir Contrôleur de gestion intégré.

iCare

La console iCare (insight Care) est une application d'administration web qui offre des outils pour la maintenance d'unités matérielles.

ICH

Input/Output Hub. Fournit un point de connexion entre divers composants d'E/S et les processeurs Intel.

ICMB

Intelligent Chassis Management Bus. Nom donné à l'architecture, aux spécifications et aux protocoles utilisés pour interconnecter un châssis intelligent via un bus série RS-485 pour la gestion de la plateforme.

ILB / ILBC

I/O Legacy Board / I/O Legacy Board Controller.

INCA

INtegrated Cluster Architecture.

IOH

Input/Output Hub. Un agent QPI Intel qui gère les demandes d'E/S des processeurs.

IPMB

Intelligent Platform Management Bus. Abréviations données à l'architecture et au protocole utilisés pour interconnecter des contrôleurs intelligents via un bus série I2C pour la gestion d'une plateforme.

IPMI

Intelligent Platform Management Interface. Spécification d'Intel qui décrit les mécanismes et les périphériques destinés à décharger complètement l'unité centrale des tâches de gestion du matériel.

J**JOEM**

JTAG Over Ethernet Module.

JTAG

Joint Test Action Group.

K

Pas d'entrée.

L**LAN**

Local Area Network.

LCD

Liquid Crystal Display.

LCP

Local Control Panel. Module comprenant un contrôleur, un afficheur couleur LCD, un voyant vert et un voyant bleu et un bouton de démarrage.

LDAP

Lightweight Directory Access Protocol.

LED

Light Emitting Diode.

Logical Partition | Partition logique

Quand le système d'exploitation de base est un Virtual Machine Monitor, une partition logique est l'environnement logiciel utilisé pour lancer un système d'exploitation invité.

Logical Processor | Processeur logique

Voir Thread.

M**MAC**

Media Access Control.

MCA

Une exception Machine Check Abort se produit quand une condition d'erreur, nécessitant une action corrective, est survenue.

MESCA

Multiple Environments on a Scalable Csi-based Architecture.

MIB

Management Interface Base.

MIMD

Multiple Instruction Multiple Data

Mise en ligne / Mise hors ligne

La mise en ligne et la mise hors ligne sont des opérations logiques dynamiques. La mise en ligne est l'ajout non physique d'une ARU au système d'exploitation en fonctionnement. L'unité en ligne existe déjà dans la configuration comme une unité inactive (présente et connectée). La mise hors ligne est le retrait non physique d'une ARU du système d'exploitation en fonctionnement. L'unité hors ligne reste dans la configuration comme une unité inactive, prête à être mise en ligne.

Mise hors ligne

Voir Mise en ligne / Mise hors ligne.

MMX

MultiMedia eXtensions.

MTB/MTBC

Memory and Tukwila Board / Memory and Tukwila Board Controller.

MTBF

Mean Time Between Failure.

Multicore | Multicoeur

Présence de deux processeurs ou plus sur un seul circuit intégré.

Multi-Threading | Traitement multiprocessus

Capacité d'un processeur à coeur unique à fournir une visibilité logicielle similaire à celle de plusieurs coeurs et à exécuter plusieurs threads qui peuvent paraître simultanés au logiciel, tout en utilisant des ressources matérielles supplémentaires limitées par rapport à un coeur sans multi-threading.

Suivant la conception du coeur, les instructions envoyées pour être exécutées par le coeur dans un cycle donné peuvent être **Hyper-Threading (HT)** - depuis un thread unique, basculant sur un autre thread sur l'apparition d'événements spécifiques (par ex. défauts de cache) ou **Simultaneous Multi-Threading (SMT)** de deux threads.

MXB/MXBC

Memory and Xeon Board / Memory and Xeon Board Controller.

N**Nehalem**

NEHALEM Intel Xeon Processor (8 coeurs par processeur).

NFS

Network File System.

NIC

Network Interface Controller.

NUMA

Non Uniform Memory Access.

NVRAM

Non-Volatile Random Access Memory.

O

OOB | Hors bande

Out Of Band. Accès à la gestion de la plateforme système qui ne franchit pas le système d'exploitation ou d'autres logiciels exécutés sur les processeurs principaux du système géré.

OPMA

Open Platform Management Architecture.

P

PCI

Peripheral Component Interconnect. Architecture de bus prenant en charge des périphériques hautes performances.

PCIe

PCI Express. Dernier standard pour les cartes d'extension PCI.

PDB

Power Distribution Board. Sous-ensemble du module d'alimentation.

PDU | Bloc d'alimentation

Power Distribution Unit. Bus d'alimentation utilisé pour la connexion des composants périphériques.

Platform Event | Événement plateforme

Un événement plateforme est un événement directement issu du firmware (BIOS) ou de la plateforme matérielle, indépendamment de l'état du système d'exploitation ou du matériel de gestion du système.

PEF

Platform Event Filtering | Filtrage des événements plateforme.

Fonction dans IPMI qui permet au BMC de générer une action sélectionnable (par ex. démarrage/arrêt, une réinitialisation, un envoi d'alerte, etc.) quand un événement configurable se produit sur le système de gestion.

PET

Le format Platform Event Trap est utilisé pour envoyer un événement plateforme dans une interruption SNMP. Voir Événement plateforme.

PIROM

Processor Information ROM. La mémoire PIROM contient des informations sur le processeur spécifique où elle réside. Ces informations incluent des en-têtes d'adressage autorisant une programmation flexible et une compatibilité ascendante, des caractéristiques électriques du cache L2 et de base, les numéros de référence et S-spec du processeur ainsi qu'un numéro de processeur 64 bits.

PMU

Physically Manageable Unit | Unité gérable physiquement. Une unité logique matérielle ou un groupe d'unités logiques, qui peuvent être affichées / traitées par un système d'exploitation, ou par le BIOS, ou par le logiciel de gestion de la plateforme. Une PMU peut être imbriquée et n'est pas nécessairement séparable des autres PMU. PMU est également connue sous l'acronyme ARU.

POST

Power On Self Test.

Processor

Chaque processeur contient un ou plusieurs connecteurs dans un seul package. Chaque connecteur contient un ou plusieurs coeurs. Chaque coeur contient un ou plusieurs threads (processeurs logiques). Chaque processeur est hébergé dans un connecteur.

PSMI

Power Supply Management Interface.

PSU

Power Supply Unit. Sous-ensemble du module d'alimentation.

PSWB
PCI SWitch Board.

PSWM
PCI SWitch Module.

PWM
Pulse Width Modulation.

Q

QDR
Quad Data Rate. Technique de signalisation de communication où les données sont transmises en quatre points dans le cycle d'horloge.

QPI
Quick Path Interconnect. Interface Intel point-à-point à grande vitesse, utilisée pour interconnecter des processeurs et des hubs d'E/S, et éventuellement des contrôleurs de nœuds (BCS).

QSB
Quad Switch Board.

QSFP
Quad Small Form-factor Pluggable. Technologie d'interconnexion basse puissance.

QSMB
Quad Switch Module. InfiniBand Switch.

R

RADIUS
Remote Authentication Dial-In User Service.

RAS
Reliability, Availability, Serviceability.

RMII
Reduced Media Independent Interface. Standard qui réduit le nombre de signaux/broches nécessaires pour connecter un circuit intégré Ethernet à une couche physique émetteur-récepteur. Voir MII.

RTC
Real Time Clock.

S

SAS
Serial Attached SCSI. Technologie de transfert de données utilisée pour déplacer des données vers et depuis des périphériques de stockage tels que les disques durs et les lecteurs de bandes.

SATA
Serial ATA. Technologie de bus pour la connexion des disques durs et d'autres périphériques.

SEL
System Event Log. Enregistrement des événements de gestion du système. Les informations stockées incluent le nom de l'événement, la date et l'heure auxquelles l'événement s'est produit ainsi que les données de l'événement. Les données de l'événement peuvent inclure les codes d'erreur POST qui indiquent des erreurs matérielles ou des conflits logiciels dans le système.
Zone de stockage non volatile dans le BMC et les interfaces associées pour le stockage des informations des événements de la plateforme système pour une récupération ultérieure.

Server Hardware Console | Console matérielle du serveur

Interface graphique utilisateur utilisée pour accéder au logiciel de gestion intégré dans le module du serveur.

SHC

Voir Server Hardware Console (Console matérielle du serveur).

Simultaneous Multi-Threading | Multi-threading simultané

Voir Multi-Threading.

SMBIOS

System Management BIOS.

SM-BUS

System Management Bus.

SMI

System Management Interrupt.

SMP

Symmetrical Multi Processor. Traitement de programmes par plusieurs processeurs qui partagent une mémoire et un système d'exploitation communs.

SMT

Simultaneous Multi-Threading.

SMTP

Simple Mail Transfer Protocol.

SNC

Scalable Node Controller. Interface de bus système et contrôleur mémoire du processeur pour le jeu de puces Intel870. Le SNC prend en charge les processeurs Itanium2, la mémoire principale DDR SDRAM, une Firmware Hub Interface supportant plusieurs concentrateurs Firmware et deux processeurs d'interconnexion SPS pour l'accès aux E/S et à la mémoire cohérente sur d'autres noeuds, via le FSS.

SNMP

Simple Network Management Protocol.

SoC

System on Chip.

Socket

Interface multi-coeur d'unité de traitement central.

SOL

Serial Over LAN. Mécanisme qui permet les entrées sorties du bus série d'un système géré à rediriger via une session IPMI sur IP.

SO-DIMM

Small Outline Dual In-line Memory.

SR

Scratch Register. Registres internes du processeur Tukwila et du hub d'E/S utilisés comme zone de travail.

SSH

Secured Shell.

SSL

Secure Socket Layer.

Système d'exploitation de base

Le système d'exploitation qui est démarré à l'initialisation.

T

TELNET

TELEcommunication NETwork. Protocole utilisé dans les réseaux locaux d'entreprise pour fournir des communications interactives bidirectionnelles.

Thread

Un thread ou processeur logique est le contexte d'exécution au sein d'un seul cœur et la visibilité logicielle de multi-threading. Un processeur multi-threading contient un ou plusieurs threads (processeurs logiques).

Thresholding | Seuillage

Critère de filtrage d'événements. Le seuillage est défini selon un critère Nombre / Temps destiné afin de router uniquement les messages significatifs. Les messages identiques sont décomptés et lorsque le nombre de messages indiqué dans la zone Count (Nombre) est atteint dans le délai précisé dans la zone Time (Temps), ce message est sélectionné pour le routage.

TKW

TUKWILA Intel Itanium Processor (4 noyaux par connecteur).

U

UCM

Ultra Capacitor Module.

UVLO

Under Voltage Latch Output. (Sortie de bascule en sous-tension)

V

VMM

Virtual Machine Monitor.

W

WOL

Wake On Lan. Fonction qui offre la possibilité de démarrer un système à distance via une connexion réseau.

X

XCSI

Extended Common System Interface. Interface Bull point-à-point à grande vitesse, utilisée pour interconnecter des serveurs. Les ports XCSI sont situés et gérés dans le BCS (contrôleur de nœuds).

XNC

External Node Controller. Voir BCS.

Y

Pas d'entrée.

Z

Pas d'entrée.

Index

A

- Accès en écriture
 - activer, 4-8
 - désactiver, 4-8
- Activation
 - bouton de mise sous tension, 6-47
 - compte utilisateur, 6-20
 - filtre d'événement prédéfini, 6-58
 - voyant d'identification, 7-8
- Adresse mail du destinataire, configuration, 6-52
- Affichage
 - compte utilisateur, détails, 6-17
 - contrôleur de gestion intégré, informations, 7-2
 - Informations sur les FRU, 7-3
 - journal SEL, 5-4
 - membres du groupe, 6-34
 - messages Board & Security, 5-6
 - utilisateurs connectés, 7-12
- Alertes, configuration initiale, 5-2
- Aperçu, console distante, 4-10
- Arrêt
 - console, 2-1
 - console distante, 4-20
 - secours, 3-10
 - système, 3-8
 - suspendu, 3-10
- Arrêt forcé, secours, 3-12

B

- Bloc d'alimentation, SEL, messages, A-13
- BMC
 - configuration, 6-1
 - contrôleur de gestion intégré, 7-2
 - SEL, messages, A-54
- Boutons
 - console, distant, 4-14
 - distant, console, système, 4-14

C

- Changement, compte utilisateur
 - appartenance au groupe, 6-20
 - détails, 6-18
- Changement du mot de passe, 6-21
- Clearing (Effacement), journal SEL, 5-4
- Commandes
 - alimentation, serveur, 3-1
 - serveur, 1-4
- Composants, serveur, 1-4
- compte utilisateur
 - activer, 6-20
 - changement
 - appartenance au groupe, 6-20

- détails, 6-18
- création, 6-14
- désactiver, 6-20
- détails, affichage, 6-17
- déverrouillage, 6-23
- édition, 6-18
- forçage, changement du mot de passe, 6-21
- suppression, 6-22
- Configuration, 6-12
 - adresse mail du destinataire, 6-52
 - configuration de la politique de connexion, 6-41
 - console, SOL, B-2
 - console système, distant, 4-2
 - destinations LAN, 6-52
 - filtre d'événements configurable, 6-60
 - gestion des événements
 - adresse IP du serveur, 6-52
 - chaîne de communauté, 6-51
 - initiale, 2-8
 - alertes, 5-2
 - messages, 5-2
 - messages Board & Security, 6-12
 - paramètres d'authentification, 6-43
 - paramètres d'identification de la plateforme, 6-2
 - paramètres de sécurité, 6-37
 - paramètres de verrouillage de l'utilisateur, 6-48
 - paramètres spécifiques utilisateur, 4-2
 - politiques d'alerte, 6-55
 - restauration des données, 7-14
 - sauvegarde des données, 7-13
 - serveur
 - BMC, 6-1
 - contrôleur de gestion intégré, 6-1
 - serveur de mail, 6-51
 - transmission des alertes, 6-50
- Connexion
 - dossier local, console distante, 4-19
 - fichier image, console distante, 4-17
 - lecteur local, console distante, 4-15
- Connexions HTTPS, forçage, 6-37
- Connexions sécurisées. *See* Connexions HTTPS
- Console
 - arrêt, 2-1
 - caractéristiques, 2-4
 - démarrage, 2-1
 - distant
 - aperçu, 4-10
 - arrêt, 4-20
 - lancement, 4-10
 - média virtuel, 4-15
 - présentation, 2-4
 - Serial-Over-LAN (SOL), B-1
 - SOL, B-1
 - configuration, B-2

- ipmitool, B-3
- telnet, B-5
- Système à distance, 4-1, 4-2
- console distante
 - aperçu, 4-10
 - arrêt, 4-20
 - connexion
 - dossier local, 4-19
 - fichier image, 4-17
 - lecteur local, 4-15
 - lancement, 4-10
- console matérielle, démarrage, 2-2
- Console système, distant, paramètres, 4-2, 4-6
- Console système distante, 4-1
 - paramètres spécifiques utilisateur, 4-2
- Contrôles de l'alimentation, serveur, 3-1
- Contrôleur de gestion, configuration des messages, 6-12
- Contrôleur de gestion intégré
 - affichage, informations dispositifs, 7-2
 - BMC, 7-2
 - configuration, 6-1
 - enregistrement, informations dispositifs, 7-2
 - SEL, messages, A-54
- Cooling unit, SEL, messages, A-41
- Création
 - compte utilisateur, 6-14
 - groupe, 6-27
- Cycle de démarrage/arrêt forcé, secours, 3-12

D

- Démarrage
 - console, 2-1
 - console matérielle, 2-2
 - système, 3-6
- Désactiver
 - bouton de mise sous tension, 6-47
 - compte utilisateur, 6-20
 - filtre d'événement prédéfini, 6-58
 - voyant d'identification, 7-8
- destinations LAN, configuration, 6-52
- Déverrouillage, compte utilisateur, 6-23
- Déverrouillage d'un utilisateur, 6-23
- Dispositifs, réinitialisation, 7-6
- Distant
 - console
 - média virtuel, 4-15
 - présentation, 4-11
 - système
 - boutons, 4-14
 - menus, 4-12
 - console système, configuration, 4-2
 - système, console, 4-2
 - boutons, 4-14
 - menus, 4-12
 - système, console, 4-2, 4-6
- Données de configuration
 - restauration, 2-9
 - sauvegarde, 2-9
- Dossier local, virtualisation, 4-19

É

- Édition, compte utilisateur, 6-18
- Enregistrement
 - contrôleur de gestion intégré, informations, 7-2
 - Informations sur les FRU, 7-3
- État, alimentation, vérification, 3-4
- Exclusion
 - matériel, 7-9
 - module du serveur, 7-11
 - processeurs, 7-9
- External Environment, SEL, messages, A-10

F

- Fan device, SEL, messages, A-41
- Fichier image, virtualisation, 4-17
- Filters (Filtres), alerte, A-2
- Filtre d'événement prédéfini, activation et désactivation, 6-58
- Filtre d'événements configurable, configuration, 6-60
- Filtres d'alerte
 - description, A-2
 - prédéfinis, A-2
- Filtres d'alertes prédéfinies, description, A-2
- firmware
 - affichage, informations, 7-4
 - mise à jour, 7-5
- Fonctionnalités
 - console, 2-4
 - interface, 2-5
 - serveur, 1-4
- Forçage
 - changement du mot de passe, 6-21
 - Connexions HTTPS, 6-37

G

- Gestion
 - groupes, 6-14
 - permissions, 6-14
 - utilisateurs, 6-14
- Gestion des événements, configuration, 6-51, 6-52
- Glossaire, g-1
- Groupe
 - création, 6-27
 - suppression, 6-35
- Groups (Groupes), gestion, 6-14

H

- Hardware | Matériel, exclusion, 7-9

I

- ILB, SEL, messages, A-15
- Inclusion, module du serveur, 7-11
- Informations sur les firmwares, affichage, 7-4
- Informations sur les FRU, affichage et enregistrement, 7-3

- Initial, configuration, 2-8
 - alertes, 5-2
 - messages, 5-2
- Installation, outil de sauvegarde, 2-9
- Installation d'un certificat SSL, 6-40
- Interface
 - caractéristiques, 2-5
 - permissions, 2-5
- ipmitool, SOL, utilisation, B-3

J

- Journal d'événements, serveur, surveillance, 5-1
- Journal SEL
 - affichage, 5-4
 - effacement, 5-4

L

- Lancement, console distante, 4-10
- Lecteur local, virtualisation, 4-15

M

- Maintenance, caractéristiques, 7-1
- Média, virtuel
 - connexion, 4-15
 - déconnexion, 4-15
- Média virtuel
 - connexion, 4-15
 - déconnexion, 4-15
 - dossier local, 4-19
 - fichier image, 4-17
 - lecteur local, 4-15
- Membres du groupe, affichage, 6-34
- Memory, SEL, messages, A-62
- Menus
 - console, distant, 4-12
 - distant, console, système, 4-12
- Messages
 - configuration initiale, 5-2
 - SEL
 - alimentation, A-12
 - bloc d'alimentation, A-13
 - BMC, A-54
 - carte d'alimentation du système, A-11
 - contrôleur de gestion intégré, A-54
 - external environment, A-10
 - ILB, A-15
 - mémoire, A-62
 - MTB, A-27
 - MXB, A-27
 - Panneau de contrôle local (LCP), A-53
 - PDB, A-43
 - processeur, A-30
 - sous-châssis, A-11
 - ultra capacitor, A-44
 - unité de refroidissement, A-41
 - ventilateur, A-41
 - serveur, surveillance, 5-1
- Messages Board & Security
 - affichage, 5-6
 - configuration, 6-12

- Messages de sécurité
 - affichage, 5-6
 - configuration, 6-12
- Messages SEL, A-9
- Mise à jour, firmware, 7-5
- Modification
 - mot de passe actuel, 6-26
 - paramètres de l'horloge, 6-10
 - paramètres des profils fonctionnels, 6-4
- module du serveur
 - exclusion, 7-11
 - Inclusion, 7-11
- Monitoring (Surveillance)
 - capteurs, 5-2
 - serveur, 5-1
 - journal d'événements, 5-1
 - messages, 5-1
- Mot de passe actuel, modification, 6-26
- Mot de passe utilisateur par défaut, 2-2
- MTB, SEL, messages, A-27
- MXB, SEL, messages, A-27

N

- Nom d'utilisateur par défaut, 2-2
- Notices
 - sécurité, x
 - sécurité électrique, x
 - sécurité laser, xi

O

- Obtention d'un certificat SSL, 6-40
- Outil de sauvegarde, installation, 2-9

P

- Panneau de contrôle local (LCP), SEL, messages, A-53
- Paramètre
 - permissions, 6-28
 - serveur géré, nom, 6-3
- Paramètre Date, modification, 6-10
- Paramètre Heure, modification, 6-10
- Paramètres
 - clavier, console système distante, 4-6
 - souris, console système distante, 4-6
 - spécifique utilisateur, console système distante, 4-2
- Paramètres d'authentification, configuration, 6-43
- Paramètres de l'horloge, modification, 6-10
- Paramètres de sécurité, configuration, 6-37
- Paramètres de verrouillage
 - bouton de mise sous tension, 6-47
 - utilisateur, 6-48
- Paramètres de verrouillage de l'utilisateur, 6-48
- Paramètres spécifiques utilisateur, 4-2
- Password modification (Modification du mot de passe), 6-26
- PDB, SEL, messages, A-43
- Permissions, 6-28
 - gestion, 6-14
 - interface, 2-5

- Permissions du groupe, 6-28
- Permissions utilisateur, 6-28
- Platform (Plateforme), paramètres d'identification, configuration, 6-2
- Politique de connexion, configuration, 6-41
- Politiques d'alerte, configuration, 6-55
- Power (Démarrage)
 - état, vérification, 3-4
 - gestion, 3-2
- Power supply, SEL, messages, A-12
- Power system board, SEL, messages, A-11
- Processeurs, exclusion, 7-9
- Processor, SEL, messages, A-30
- Profils fonctionnels, modification, 6-4

R

- Recommandations, sécurité, xii
- Redémarrage à froid, secours, 3-12
- Redémarrage à froid et vidage de mémoire, secours, 3-12
- Redirection du lecteur
 - activer, 4-8
 - désactiver, 4-8
- Réinitialisation, dispositifs, 7-6
- Reset (Réinitialisation)
 - secours, 3-10, 3-12
 - système, suspendu, 3-10
- Restauration, données de configuration, 2-9, 7-14

S

- Sauvegarde, données de configuration, 2-9, 7-13
- Secours
 - arrêt, 3-10
 - arrêt forcé, 3-12
 - cycle de marche/arrêt forcé, 3-12
 - redémarrage à froid, 3-12
 - redémarrage à froid et vidage de mémoire, 3-12
 - réinitialisation, 3-10, 3-12
 - vider la mémoire, 3-12
- Sécurité
 - notices, x
 - Recommandations, xii
- Sécurité électrique, x
- Sécurité laser, xi

SEL

- alimentation, messages, A-12
- bloc d'alimentation, messages, A-13
- BMC, messages, A-54
- carte d'alimentation du système, messages, A-11
- contrôleur de gestion intégré, messages, A-54
- external environment, messages, A-10
- ILB, messages, A-15
- mémoire, messages, A-62
- MTB, messages, A-27
- MXB, messages, A-27
- Panneau de contrôle local (LCP), messages, A-53
- PDB, messages, A-43
- processeur, messages, A-30
- sous-châssis, messages, A-11
- ultra capacitor, messages, A-44
- unité de refroidissement, messages, A-41
- ventilateur, messages, A-41
- Sensors (Capteurs), surveillance, 5-2
- Serial-Over-LAN (SOL), console, B-1
 - configuration, B-2
 - utilisation
 - ipmitool, B-3
 - telnet, B-5
- Serveur
 - alimentation, 3-1
 - BMC, configuration, 6-1
 - caractéristiques, 1-4
 - composants, 1-4
 - contrôles, 1-4
 - contrôleur de gestion intégré, configuration, 6-1
 - présentation, 1-2
 - surveillance, 5-1
 - Voyants, 1-4
- Serveur de mail, configuration, 6-51
- Serveur géré, nom, paramètre, 6-3
- SOL
 - configuration, console, B-2
 - console, B-1
 - utilisation
 - ipmitool, B-3
 - telnet, B-5
- SSL Certificate (Certificat SSL), obtenir et installer, 6-40
- Sub-chassis, SEL, messages, A-11
- Suppression
 - compte utilisateur, 6-22
 - groupe, 6-35
- Système
 - arrêt, 3-8
 - console, distant
 - boutons, 4-14
 - menus, 4-12
 - console distante
 - aperçu, 4-10
 - arrêt, 4-20
 - lancement, 4-10
 - présentation, 4-11
 - démarrage, 3-6

T

telnet, SOL, utilisation, B-5
Transmission des alertes, configuration, 6-50

U

Ultra Capacitor, Messages SEL, A-44
Users (Utilisateurs), gestion, 6-14
Utilisateurs connectés, affichage, 7-12
Utilisation, SOL
 ipmitool, B-3
 telnet, B-5

V

Vérification, alimentation, état, 3-4
Vider la mémoire, secours, 3-12
Virtualisation
 dossier local, 4-19
 fichier image, 4-17
 lecteur local, 4-15
Voyant d'identification (activation/désactivation), 7-8
Voyants, serveur, 1-4
Vue d'ensemble
 console, 2-4
 console distante, système, 4-11
 serveur, 1-2

Bull Cedoc
357 avenue Patton
BP 20845
49008 Angers Cedex 01
FRANCE

REFERENCE
86 F1 50FD 06