Serveurs Sun Fire V20z et Sun Fire V40z

Guide de gestion des serveurs

Sun Microsystems, Inc.
www.sun.com

Référence n° 819-2919-15
Juillet 2005, révision A

Envoyez vos commentaires sur ce document à : http://www.sun.com/hwdocs/feedback

Papier
recyclable

Adobe PostScript

Table des matières

Préface xxi

Organisation de ce guide xxi

Documentation connexe xxii

Accès à la documentation Sun xxii

Sites web de parties tierces xxiii

Support technique Sun xxiii

Vos commentaires sont les bienvenus xxiii

1. Introduction 1

Présentation 1

Documentation pour les utilisateurs 2

Acronymes 2

Gestion des serveurs 4

Processeur de service 4

Interfaces de gestion de serveurs 6

Intégration SNMP 6

Panneau de l'opérateur 8

Caractéristiques des écrans du panneau de l'opérateur 9

Groupes d'utilisateurs 10

Utilisateurs 11

Fichiers de mots de passe 11
Tâches de gestion de systèmes 12
Configuration initiale du SP 14
Partie I : Assignation des paramètres réseau au SP 14
Assignation des paramètres réseau SP en utilisant DHCP 14
Assignation des paramètres réseau à un SP statique 16
Partie II : Sécurisation du SP 19
Création du compte de gestionnaire initial 19
Partie III : Activation de l'accès IPMI sur le serveur 22
Activation de l'accès IPMI sur un serveur Linux (in-band) 22
Activation de l'accès IPMI sur un serveur x86 Solaris (in-band) 24
Partie IV : Activation de l'accès LAN IPMI 25
Activation de l'accès LAN IPMI sur un serveur Linux (in-band) 25
Activation de l'accès LAN IPMI sur un serveur x86 Solaris (in-band) 26
Autre méthode permettant d'activer l'accès LAN IPMI (out-of-band) 26
Mise à niveau du noyau de Linux 27
Intégration au site 28
Raccordement de serveurs en guirlande 28
Pilotes de plates-formes et applications 32
Mise à jour du logiciel 34
Sélection et configuration du serveur de fichiers 36
Configuration et démarrage de l'application Update Server 37
Identification des packages pour la mise à jour 38
Mise à jour du package de base du SP 39
Mise à jour du package SP Value-Add 40
Mise à jour du BIOS 41
Mise à jour des diagnostics 42
Configuration automatique du SP (méthode optionnelle) 43

Détermination des adresse MAC réseau du SP et de la plate-forme 47
Fonctions de la console Systems Management 48
Configuration des paramètres réseau 48
Démarrage et arrêt du SE de la plate-forme 50
Configuration de la notification d'événements SMTP 51
Configuration des services d'annuaire 53
Mappage de groupes de services d'annuaire 55
Création des fichiers keytab pour ADS 56
Exigences du serveur ADS 56
Exigences du SP ADS 56
Configuration de la date et de l'heure 57
Configuration de SSL 58
Configuration du certificat SSL depuis SM Console 59
Contrôle du statut du système 60
Événements système 64
Icônes des types d'événements 66

2. Gestion de serveurs IPMI 67

Interface de gestion de plate-forme intelligente 67
Contrôleur de gestion de carte de base 68
Facilité de gestion 69
Présentation fonctionnelle 69
Conformité à IPMI et accès au canal LAN 70
Noms d'utilisateur et mots de passe 71
Prise en charge des options d'initialisation du serveur 71
Journal d'événements système 72
Capteurs 72
Détermination de la présence des capteurs 72
Seuils des capteurs 73

Capteurs de température 73
Capteurs de mémoire pour DIMM 73
Capteurs de tension 74
Capteurs des ventilateurs 74
Capteurs des alimentations 74
Contrôleurs de gestion 74
Capteurs variés 75
Filtres d'événements 76
Horloges de surveillance 77
Alertes 77
Détermination du jeu de stratégies d'alerte 77
Lights Out Management (LOM) 78
Description 78
Informations supplémentaires 78
Syntaxe 78
Options 79
Expressions 80
Pilote de périphérique du noyau Linux IPMI 84
Interface LAN pour le BMC 84
Fichiers 85
Affichage du journal d'événements système IPMI 86
Effacement du journal d'événements système IPMI 86
Dépannage d'IPMI 87

3. Gestion de serveurs SNMP 89
Simple Network Management Protocol 89
Intégration SNMP 90
La MIB SNMP 91
Arborescence de la MIB des serveurs Sun Fire V20z et Sun Fire V40z 91

Intégration des MIB avec des consoles de tierces parties 92
Configuration de SNMP sur le serveur 92
Configuration de la gestion out-of-band 93
Agent SNMP du processeur de service 93
Agent proxy 94
Définition du nom de la communauté 94
Agent X 95
Utilisation d'un navigateur de MIB de tierce partie 95
Définition des options de journalisation 96
Déroutements SNMP 96
Configuration des destinations des déroutements SNMP 97
Configuration des destinations SNMP 98
Détails de la MIB du serveur 98
Dépannage SNMP 101

4. Informations de gestion supplémentaires 103
Configuration des fonctions d'écriture de scripts 103
Utilisation des scripts de shell 104
Scripts à distance utilisant SSH 105
Configuration de plusieurs systèmes pour l'utilisation de scripts 105
Génération de clés d'hôte 106
Création de relations d'hôte de confiance 107
Ajout de clés publiques 107
Génération d'une paire de clés d'hôte 108
Configuration d'un client Windows pour l'utilisation de scripts 109
Activation de l'accès SSH en utilisant les hôtes de confiance 110
Génération d'une paire de clés d'hôte sous Windows 111
Activation de l'accès SSH en utilisant des clés publiques 111

Directives pour l'écriture de scripts de commande pour la gestion du serveur 112

Sortie des commandes 112

Autres conseils pour des résultats optimaux 113

Redirection de la console sur une connexion série 114

Serveur basé sur Linux 114

grub 115

LILO 116

getty 117

securetty 118

Serveur basé sur Solaris 118

Activation et désactivation de la redirection de la console du BIOS 119

CD-ROM Network Share Volume (NSV) 120

Structure de NVS 120

Serial Over LAN 122

Activation ou désactivation de la fonction SOL sur le serveur 122

Lancement d'une session SOL 123

Arrêt d'une session SOL 123

Séquences d'échappement pour le terminal de console distant 124

A. Récapitulatif des commandes de gestion de serveurs 125

Utilisation du protocole `ssh` 126

Shell interactif du SP 126

Texte de préface 126

Commandes 127

Codes de retour 129

B. Commandes d'accès 131

Sous-commandes d'accès relatives à config-sharing 132

Sous-commande access enable config-sharing 132

Format 132
Codes de retour 133
Sous-commande access disable config-sharing 133
Format 133
Codes de retour 134
Sous-commande access get config-sharing 134
Format 134
Valeurs 134
Codes de retour 135
Sous-commandes d'accès relatives aux groupes 136
Sous-commande access get group 136
Format 136
Codes de retour 136
Sous-commande access get groups 137
Format 137
Codes de retour 137
Sous-commandes d'accès relatives au mappage 138
Sous-commande access get map 138
Format 138
Codes de retour 139
Sous-commandes access map 139
Format 139
Codes de retour 140
Sous-commande access unmap 140
Format 140
Codes de retour 141
Sous-commandes d'accès relatives aux services d'annuaire 142
Sous-commande access disable service 142

Format 142
Codes de retour 143
Sous-commande access enable service 143
Format 143
Codes de retour 145
Sous-commande access get services 145
Format 145
Codes de retour 146
Sous-commandes d'accès relatives à la confiance 147
Sous-commande access add trust 147
Format 147
Génération de clés d'hôte 148
Codes de retour 149
Sous-commande access delete trust 150
Format 150
Codes de retour 150
Sous-commande access get trusts 151
Format 151
Codes de retour 151
Sous-commandes d'accès relatives aux clés publiques 152
Sous-commande access add public key 152
Format 153
Codes de retour 153
Sous-commande access get public key users 154
Format 154
Codes de retour 154
Sous-commande access delete public key 155
Format 155

Codes de retour 155
Sous-commandes d'accès relatives aux utilisateurs 156
Sous-commande access add user 156
Format 156
Codes de retour 157
Sous-commande access delete user 157
Format 157
Codes de retour 158
Sous-commande access get users 158
Format 158
Codes de retour 159
Sous-commande access update password 159
Format 159
Codes de retour 160
Sous-commande access update user 160
Format 160
Codes de retour 161

C. Commandes de diagnostic 163

Avant de commencer 164
Ne pas accéder au SP quand les diagnostics sont chargés 164
Problèmes connus 164
Message d'erreur bénigne 164
Sous-commande diags cancel tests 165
Format 165
Codes de retour 166
Sous-commande diags get modules 167
Sous-commande diags get state 168
Format 168

Codes de retour 169
Sous-commande diags get tests 169
Format 169
Codes de retour 170
Sous-commande diags run tests 171
Format 171
Codes de retour 172
Sous-commande diags start 173
Format 173
Codes de retour 174
Sous-commande diags terminate 175
Format 175
Codes de retour 175

D. Commandes d'inventaire 177
Sous-commande inventory compare versions 178
Format 178
Codes de retour 179
Sous-commande inventory get hardware 179
Format 179
Codes de retour 181
Sous-commande inventory get software 182
Format 182
Codes de retour 182
Sous-commande inventory get remote software 183
Format 183
Codes de retour 183
Sous-commande inventory get all 184
Format 184

Codes de retour 184

E. Commandes IPMI 185

Sous-commande ipmi disable channel 186

Format 186

Codes de retour 186

Sous-commande ipmi enable channel 187

Format 187

Codes de retour 187

Sous-commande ipmi disable pef 188

Format 188

Codes de retour 188

Sous-commande ipmi enable pef 189

Format 189

Codes de retour 189

Sous-commande ipmi get channels 190

Format 190

Codes de retour 190

Sous-commande ipmi get global enables 191

Format 191

Codes de retour 191

Sous-commande ipmi get sel 192

Format 192

sous-commande ipmi clear sel 194

Sous-commande ipmi set global enable 195

Format 195

Codes de retour 196

Sous-commande ipmi reset 197

Format 197

Codes de retour 197

F. Commandes de la plate-forme 199

Sous-commandes de plate-forme relatives à la console 200

Sous-commande platform console 200

Format 200

Codes de retour 203

Sous-commande platform get console 204

Format 204

Codes de retour 205

Platform Set Console 206

Format 206

Codes de retour 207

Sous-commandes de la plate-forme relatives à l'état du SE 208

Sous-commande platform get os state 209

Format 209

Codes de retour 209

Sous-commandes platform set os state 210

platform set os state reboot 210

platform set os state boot 211

platform set os state shutdown 213

platform set os state update-bios 214

Sous-commandes de la plate-forme relatives à l'état de l'alimentation 216

Sous-commande platform get power state 216

Format 216

Codes de retour 217

Sous-commande platform set power state 217

Format 218

Codes de retour 219

Sous-commande platform get hostname 220
Format 220
Codes de retour 220
Sous-commande platform get mac 221
Format 221
Codes de retour 221
Sous-commande platform get product id 222
Format 222
Codes de retour 222

G. Commandes relatives aux capteurs 223
Sous-commande sensor get 224
Format 224
Codes de retour 226
Sous-commande sensor set 227
Format 227
Codes de retour 229

H. Commandes du processeur de service 231
Sous-commandes du SP relatives à la date 232
Sous-commande sp get date 232
Format 232
Codes de retour 233
Sous-commande sp set date 233
Format 233
Codes de retour 234
Sous-commandes du SP relatives à DNS 234
Sous-commande sp disable dns 234
Codes de retour 235

Sous-commande sp enable dns 235
Format 235
Codes de retour 236
Sous-commande sp get dns 236
Format 236
Codes de retour 237
Sous-commandes du SP relatives aux événements 237
Sous-commande sp delete event 238
Format 238
Codes de retour 238
Sous-commande sp get events 239
Format 239
Codes de retour 240
Sous-commandes du SP relatives au nom de l'hôte 241
Sous-commande sp get hostname 241
Format 241
Codes de retour 242
Sous-commande sp set hostname 242
Format 242
Codes de retour 243
Sous-commandes du SP relatives à IP 244
Sous-commande sp get ip 244
Format 244
Codes de retour 245
Sous-commande sp set ip 245
Format 245
Codes de retour 246
Sous-commandes du SP relatives à l'adresse JNET 247

Sous-commande sp get jnet 247
Format 247
Codes de retour 248
Sous-commande sp set jnet 248
Format 248
Codes de retour 249
Sous-commandes du SP relatives au voyant de localisation 250
Sous-commande sp get locatelight 250
Format 250
Codes de retour 250
Sous-commande sp set locatelight 251
Format 251
Codes de retour 251
Sous-commandes du SP relatives aux fichiers journaux 252
Sous-commande sp get logfile 252
Format 252
Codes de retour 253
Sous-commande sp set logfile 253
Format 253
Codes de retour 254
Sous-commandes diverses du SP 255
Sous-commande create test events du SP 255
Format 256
Codes de retour 256
Sous-commande d'adresse sp get mac 257
Format 257
Codes de retour 257
Sous-commande sp get port80 257

Format 257
Codes de retour 258
Codes de POST du BIOS 258
Codes des blocs d'initialisation pour la ROM Flash 264
Sous-commande du SP relative à la configuration automatique 265
Format 265
Codes de retour 266
Sous-commande sp get status 266
Format 266
Codes de retour 267
Sous-commande sp get tdulog 267
Format 267
Codes de retour 269
Sous-commande sp reboot 269
Format 269
Codes de retour 270
Sous-commande sp reset 270
Format 270
Codes de retour 272
Sous-commandes du SP relatives au montage 273
Sous-commande sp add mount 273
Format 273
Codes de retour 275
Sous-commande sp delete mount 276
Format 276
Codes de retour 276
Sous-commande sp get mount 277
Format 277

Codes de retour 277
Sous-commandes du SP relatives à SMTP 278
Sous-commande sp get smtp server 278
Format 278
Codes de retour 279
Sous-commande sp set smtp server 279
Format 279
Codes de retour 280
Sous-commande sp get smtp subscribers 280
Format 280
Codes de retour 281
Sous-commande sp update smtp subscriber 282
Format 282
Codes de retour 283
Sous-commandes du SP relatives à SNMP 284
Sous-commande sp add snmp-destination 284
Format 284
Codes de retour 285
Sous-commande sp delete snmp-destination 285
Format 285
Codes de retour 286
Sous-commande sp get snmp-destinations 287
Format 287
Codes de retour 287
Sous-commande sp get snmp proxy community 287
Format 287
Codes de retour 288
Sous-commande sp set snmp proxy community 288

Format 288
Codes de retour 289
Sous-commandes du SP relatives à SSL 290
Sous-commande sp disable ssl-required 290
Format 290
Codes de retour 291
Sous-commande sp enable ssl-required 291
Format 291
Codes de retour 292
Sous-commande sp get ssl 292
Format 292
Codes de retour 293
Sous-commande sp set ssl 293
Format 293
Codes de retour 294
Sous-commandes du SP relatives à la mise à jour 295
Sous-commande sp update flash all 295
Format 296
Codes de retour 297
Mises à niveau inférieures 297
Sous-commande sp update flash applications 298
Format 298
Codes de retour 299
Sous-commandes du SP relatives à la mise à jour des diagnostics 300
Format 300
Codes de retour 300

Index 301

Préface

Ce guide explique la gestion des serveurs Sun Fire™ V20z et Sun Fire V40z.

Organisation de ce guide

Le Chapitre 1 présente les différentes solutions à la disposition de l'utilisateur pour gérer les serveurs.

Le Chapitre 2 détaille la gestion des serveurs au moyen de l'interface de gestion de plate-forme intelligente ou IPMI *(Intelligent Platform Management Interface)*.

Le Chapitre 3 détaille la gestion des serveurs au moyen de SNMP *(Simple Network Management Protocol).*

Le Chapitre 4 contient des informations de gestion supplémentaires et indique notamment comment activer la fonction d'écriture de scripts, la redirection de la console sur la connexion série et série-sur-LAN.

L'Annexe A présente l'ensemble des commandes de gestion des serveurs que vous pouvez utiliser pour gérer le serveur. Chacune des annexes suivantes décrit en détail un type de commandes.

L'Annexe B contient la description détaillée des commandes d'accès.

L'Annexe C contient la description détaillée des commandes de diagnostic.

L'Annexe D contient la description détaillée des commandes d'inventaire.

L'Annexe E contient la description détaillée des commandes de l'IPMI.

L'Annexe F contient la description détaillée des commandes de la plate-forme.

L'Annexe G contient la description détaillée des commandes relatives aux capteurs.

L'Annexe H contient la description détaillée des commandes du processeur de service (SP).

Documentation connexe

Application	Titre	Référence
Consignes de sécurité	*Important Safety Information for Sun Hardware Systems*	816-7190-xx
Consignes de sécurité et déclarations de certification de conformité internationales	*Sun Fire V20z and Sun Fire V40z Servers—Safety and Compliance Guide*	817-5251-xx
Installation du matériel et des logiciels	*Serveurs Sun Fire V20z et Sun Fire V40z — Guide d'installation*	817-6137-15
Procédures de maintenance et autres informations	*Serveurs Sun Fire V20z et Sun Fire V40z — Guide de l'utilisateur*	819-2914-15
Installation du-système d'exploitation	*Serveurs Sun Fire V20z et Sun Fire V40z — Guide d'installation du système d'exploitation Linux*	817-6147-15
Dépannage et diagnostic	*Serveurs Sun Fire V20z et Sun Fire V40z — Guide des techniques de dépannage et de diagnostic*	819-2924-12
Informations de dernière minute	*Notes de version des serveurs Sun Fire V20z et Sun Fire V40z*	819-2909-11
Comparaison des modèles de serveurs	*Différences existant entre les versions des serveurs Sun Fire V20z et Sun Fire V40z*	819-4298-10

Accès à la documentation Sun

Vous pouvez visualiser, imprimer ou acquérir une large sélection de documents Sun, dont des versions localisées, à l'adresse suivante :

http://www.sun.com/documentation

Sites web de parties tierces

Sun décline toute responsabilité quant à la disponibilité des sites Web de tiers mentionnés dans ce document. Sun n'avalise pas et n'est pas responsable des contenus, des publicités, des produits ou autres matériaux disponibles sur ou par le biais de ces sites ou ressources. Sun ne pourra en aucun cas être tenue responsable de tout dommage ou perte réel ou présumé causé par ou lié de quelque manière aux contenus, biens et services disponibles sur ou par le biais de ces sites ou ressources.

Support technique Sun

Si vous ne trouvez pas de réponses à vos éventuelles questions techniques dans ce document, rendez-vous sur :

http://www.sun.com/service/contacting

Vos commentaires sont les bienvenus

Dans le souci d'améliorer notre documentation, nous vous invitons à nous faire parvenir vos commentaires et vos suggestions. Vous pouvez nous les transmettre à l'adresse suivante :

http://www.sun.com/hwdocs/feedback

N'oubliez pas de mentionner le titre et le numéro de référence du document dans votre commentaire :

Serveurs Sun Fire™ V20z et Sun Fire V40z — Guide de gestion des serveurs, référence 819-2919-15.

CHAPITRE 1

Introduction

Présentation

Les fonctions de gestion de serveurs sont primordiales pour la maintenance des serveurs capitaux pour la mission de l'entreprise. La notification avancée des problèmes ainsi que leur diagnostic rapide et leur correction sont des fonctions critiques dans un environnement dans lequel un petit nombre de serveurs supportent la plus grande partie de la charge de travail. Les serveurs Sun Fire™ V20z et Sun Fire V40z et leurs fonctions de gestion étendues réduisent les frais en diminuant les pannes et en éliminant potentiellement la gestion manuelle.

Ce document explique comment les gérer à distance.

Le serveur Sun Fire V20z est un serveur d'entreprise biprocesseur (2P) de une unité de rack (1U) à processeurs Opteron AMD. Le serveur Sun Fire V40z est aussi un serveur à processeurs Opteron AMD mais il mesure trois unités de rack (3U) et a quatre processeurs (4P).

Ces serveurs incluent un processeur de service (SP) intégré, une mémoire flash, une RAM, une interface Ethernet séparée et un logiciel de gestion de serveurs. Ils sont livrés équipés d'outils de gestion de serveurs supérieurs, clés d'un contrôle majeur et d'un coût total de possession minimum. Vous pouvez utiliser l'interface de ligne de commande, l'intégration SNMP avec des structures de parties tierces ou l'IPMI pour configurer et gérer la plate-forme avec le SP. Le SP dédié assure une indépendance totale vis-à-vis du système d'exploitation et une disponibilité maximale de la gestion du serveur.

Documentation pour les utilisateurs

Pour obtenir la documentation utilisateur la plus actuelle pour les serveurs Sun Fire V20z et Sun Fire V40z, veuillez visiter le site Web suivant :

http://www.sun.com/products-n-solutions/hardware/docs/Servers/Workgroup_Servers/Sun_Fire_V20z/index.html

Ce site contient les manuels de l'utilisateur, les notes de version et les guides individuels relatifs aux différentes CRU (*Customer-Replaceable Unit*, unité remplaçable par le client).

Pour savoir si le document disponible sur le site est plus récent que celui en votre possession, regardez les deux derniers chiffres (après le tiret) de la référence de ce document.

Remarque – Un document expliquant les différences existant entre les versions commercialisées des serveurs Sun Fire V20z et Sun Fire V40z est également disponible sur ce site Web. Voir le numéro de référence (PN) 817-7185.

Acronymes

Le TABLEAU 1-1 définit les acronymes qui figurent dans ce document.

TABLEAU 1-1 Acronymes

Acronyme	Explication
ACPI	*Advanced Configuration and Power Interface*
ARP	*Address Resolution Protocol,* protocole de résolution d'adresse
BMC	*Baseboard Management Controller,* contrôleur de gestion de carte de base
CRU	*Customer-Replaceable Unit*, unité remplaçable par le client
DPC	*Direct Platform Control*, contrôle de plate-forme direct
FRU	*Field-Replacement Unit*, unité remplaçable sur site
grub	*Grand Unified Bootloader*
IPMI	Interface de gestion de plate-forme intelligente
KCS	*Keyboard Controller Style*
KVM	*Keyboard, video and mouse*, clavier, vidéo et souris

TABLEAU 1-1 Acronymes *(suite)*

Acronyme	Explication
LAN	*Local Area Network*, réseau local
LILO	*Linux Loader*, chargeur Linux
LOM	*Lights Out Management*
MIB	*Management Information Base*, base d'informations de gestion
RMCP	*Remote Management Control Protocol*
SDR	*Sensor Data Record*
SEL	*System Event Log*, journal d'événements système
SNMP	Simple Network Management Protocol
SOL	Serial Over LAN
SP	Processeur de service
SSU	*System Setup Utility*
SunMC	*Sun Management Center*
UART	*Universal Asynchronous Receiver/Transmitter*
UDP	*User Datagram Protocol*
WAN	*Wide Area Network*, réseau étendu

Gestion des serveurs

Plusieurs options permettent de gérer à distance un serveur Sun Fire V20z ou Sun Fire V40z :

- Lights Out Management (LOM) via IPMItool ;
- le protocole SNMP.

Processeur de service

Les serveurs Sun Fire V20z et Sun Fire V40z sont dotés d'un processeur de service ou SP (de l'anglais *Service Processor*) dédié qui assure une indépendance totale vis-à-vis du système d'exploitation et une disponibilité maximale des fonctions de gestion de serveur. Ce chipset, appelé Service Processor (SP) est une puce PowerPC intégrée qui fournit les éléments suivants :

- le contrôle environnemental de la plate-forme (par ex. : températures, tensions, vitesse des ventilateurs et commutateurs du panneau) ;
- des messages d'alerte en cas de problème ;
- la commande à distance des opérations du serveur (initialisation, arrêt et redémarrage du système d'exploitation du serveur, mise sous puis hors tension du serveur, arrêt du processus d'initialisation du serveur dans le BIOS et mise à niveau du BIOS).

Remarque – Ce document fait référence à un Baseboard Management Controller (BMC, contrôleur de gestion de carte de base). C'est un contrôleur IPMI dédié. Le SP dont sont dotés ces serveurs est une CPU imbriquée générique contenant un logiciel d'émulation d'un BMC.

Le SP exécute une version imbriquée de Linux et toutes les fonctions de gestion de serveurs sont développées sous la forme d'applications Linux standard. Sa seule raison d'être est de supporter la gestion du serveur et, par conséquent, toutes les fonctionnalités du système d'exploitation ne sont pas disponibles dans le SP. De nombreuses applications courantes telles que `ftp` et `telnet` ne sont pas fournies puisqu'elles ne sont pas requises pour prendre en charge le jeu de fonctions de gestion de serveurs.

La FIGURE 1-1 illustre le panneau arrière du serveur Sun Fire V20z.

La FIGURE 1-2 illustre le panneau arrière du serveur Sun Fire V40z.

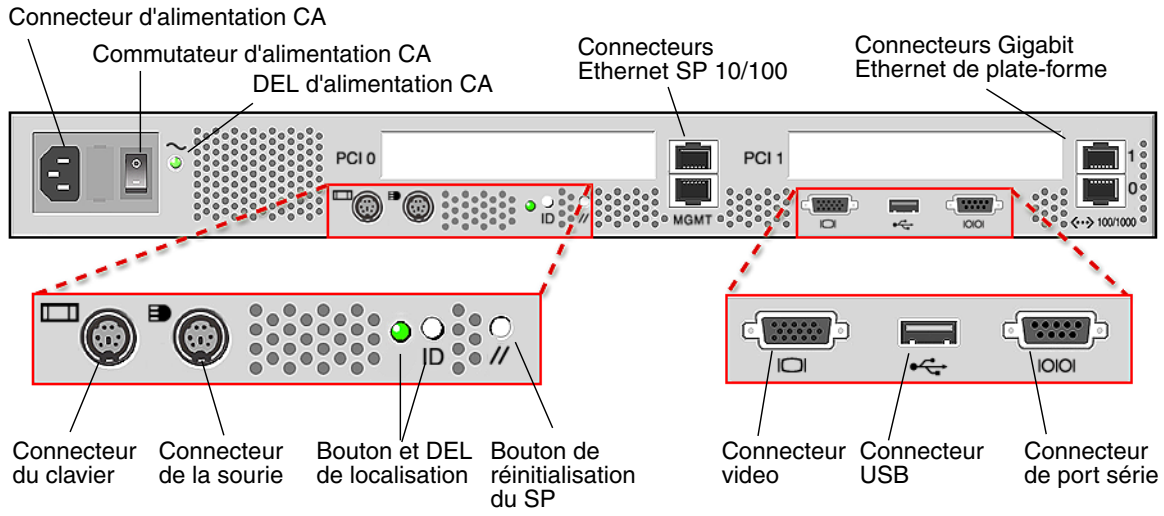


FIGURE 1-1 Panneau arrière du Sun Fire V20z

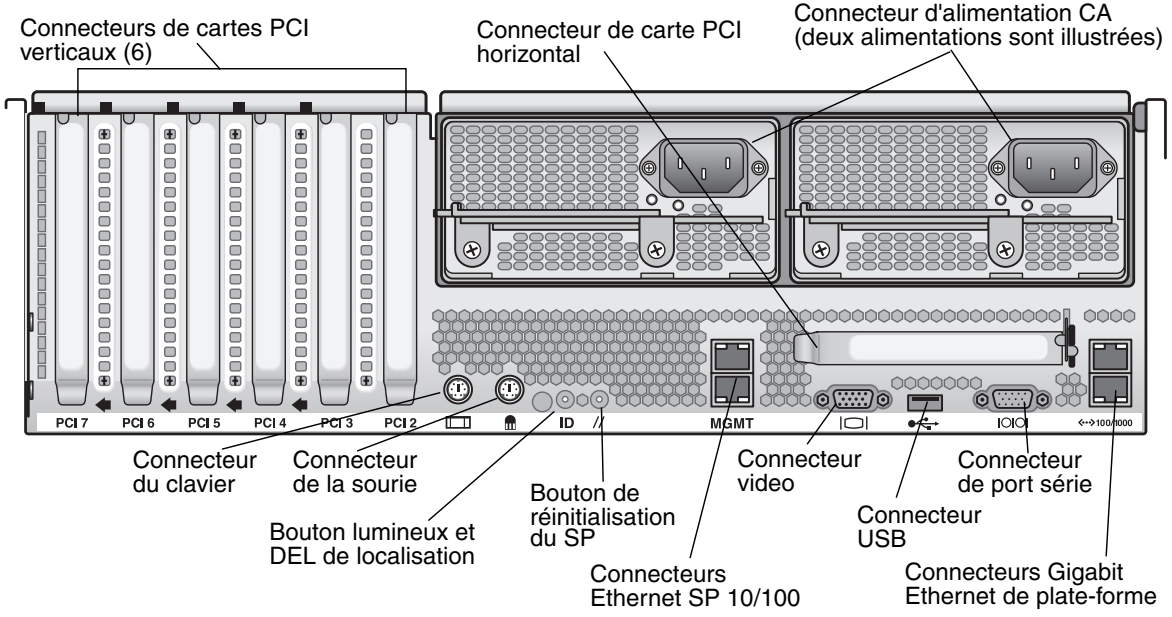


FIGURE 1-2 Panneau arrière du Sun Fire V40z

Interfaces de gestion de serveurs

Ces serveurs sont dotés de fonctions de gestion de serveurs locales et à distance par le biais du SP ; le SP prend en charge quatre interfaces de gestion de serveurs :

- IPMI en utilisant une interface KCS et un pilote de noyau IPMI (in-band) ;
- IPMI sur réseau local (LAN) (out-of-band) ;
- Intégration SNMP avec des consoles de gestion de tierces parties ;
- LOM de l'interface de ligne de commande (CLI).

Interface de ligne de commande

Les fonctions de gestion de serveur sont disponibles depuis la ligne de commande.

Consultez l'Annexe A pour la liste des commandes de gestion de serveur que vous pouvez utiliser avec ces serveurs. Vous y trouverez également pour chaque commande une description, le format de la commande, la liste des arguments ainsi que celles des codes de retour.

Fonctions SSH et de langage de script

Un administrateur système peut se connecter au SP en utilisant SSH et émettre des commandes ou, plus communément, écrire un script de shell qui appelle ces opérations à distance.

Les commandes de gestion de serveur vous permettent de gérer efficacement chaque section du serveur. De la ligne de commande, vous pouvez écrire des scripts pilotés par les données qui automatisent la configuration de plusieurs machines.
Par exemple, un système de gestion central peut imposer la mise sous tension et l'initialisation de plusieurs serveurs à un moment donné ou en présence d'une condition spécifique.

Pour plus d'informations sur les scripts, voir « Informations de gestion supplémentaires », page 103.

Intégration SNMP

La gestion SNMP fournit un accès distant via des entités conformes SNMP pour contrôler la maintenance et le statut du serveur. Le SP envoie des alertes SNMP à des fonctions de gestion externes lorsque cela est prévu.

Pour plus d'informations sur SNMP, voir « Gestion de serveurs SNMP », page 89.

Le schéma de la FIGURE 1-3 illustre les chemins de communication pour les différentes options de gestion de serveurs.

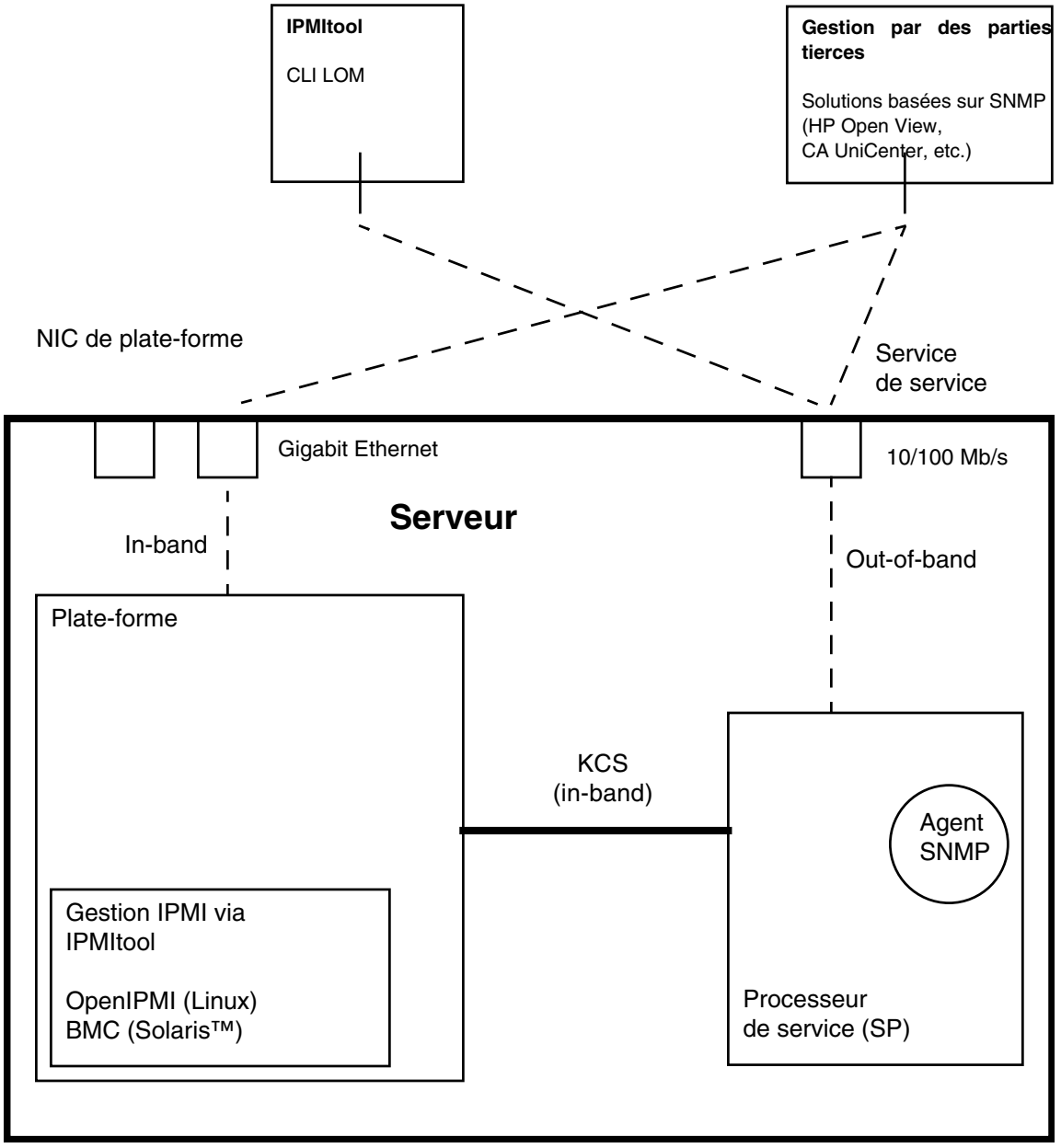


FIGURE 1-3 Schéma des options de gestion de serveurs

Panneau de l'opérateur

Vous pouvez utiliser le panneau de l'opérateur pour configurer les paramètres réseau pour le SP. Consultez la FIGURE 1-4 ou la FIGURE 1-5 pour connaître l'emplacement du panneau de l'opérateur sur votre serveur.

Remarque – Le SP passe par défaut sur la connexion réseau DHCP si le panneau de l'opérateur n'est pas engagé de façon interactive à la première mise sous tension.

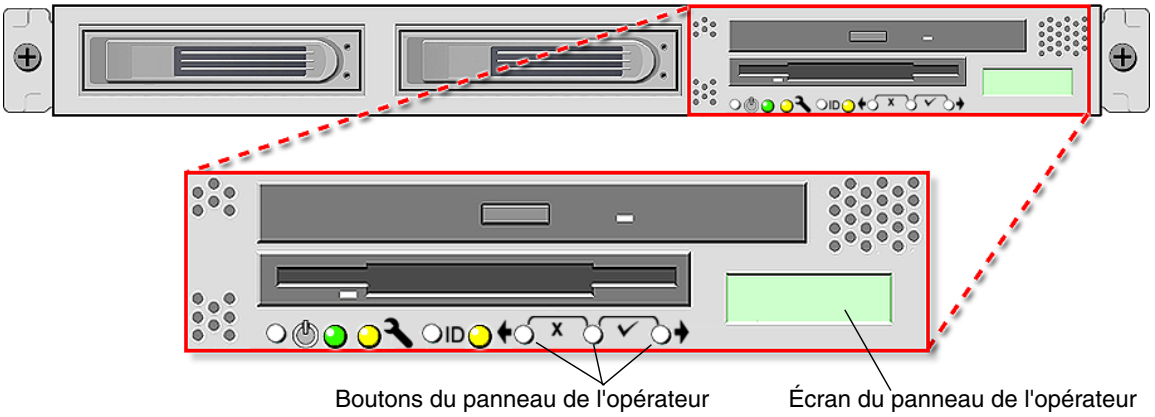


FIGURE 1-4 Panneau de l'opérateur et boutons du serveur Sun Fire V20z

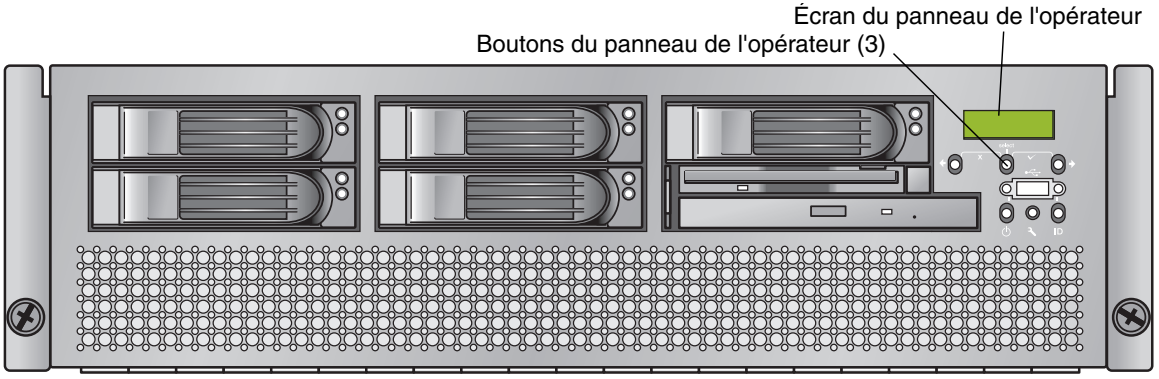


FIGURE 1-5 Panneau de l'opérateur et boutons du serveur Sun Fire V40z

Le panneau de l'opérateur affiche des informations sur l'écran LCD sur deux lignes ; vous répondez aux invites ou lancez des actions en utilisant les boutons suivants :

TABLEAU 1-2 Boutons du panneau de l'opérateur

Boutons	Fonction
	**Précédent** - Se déplace ou revient en arrière d'une étape dans les options de données d'un champ. Se déplace uniquement dans la ligne de texte du bas.
	**Sélection** - Se déplace en avant ou avance d'une étape dans les menus et les champs qui s'affichent dans la ligne supérieure et dans les valeurs des champs pour les octets qui s'affichent dans la ligne de texte du bas. Confirme et enregistre une option de données sélectionnée sur cet écran dans la ligne de texte du bas (pour confirmer les champs de sous-menu qui requièrent des octets, utilisez la combinaison de boutons Entrée).
	**Suivant** - Se déplace ou avance d'une étape dans les options de données d'un champ. Se déplace uniquement dans la ligne de texte du bas.
	**Entrée** - (**Sélection** plus **Suivant**, combinaison de sélection). Confirme et enregistre l'option de données sélectionnée dans les champs de sous-menu qui requièrent des octets, tels que l'adresse IP, le masque de réseau ou la passerelle.
	**Annuler** - (**Précédent** plus **Sélection**, combinaison X). Annule la confirmation précédente et revient à l'écran précédent.

Caractéristiques des écrans du panneau de l'opérateur

- La combinaison Entrée (Sélection plus Suivant) est indiquée par une coche. Cette combinaison confirme un choix de données dans les champs de sous-menu qui requièrent des octets tels que l'adresse IP. Vous devez appuyer simultanément sur les deux boutons et les relâcher simultanément (dans la plupart des champs, vous pouvez appuyer sur Sélection pour confirmer un choix de données).
- La combinaison Annuler (Précédent plus Sélection) est indiquée par un X. Cette combinaison annule une action, effectue une sauvegarde dans un menu et défait d'autres actions, selon le menu. Vous devez appuyer simultanément sur les deux boutons et les relâcher simultanément.
- Pour les valeurs numériques en octets, telles que l'adresse IP, vous pouvez appuyer sur le bouton Retour ou Suivant et le maintenir enfoncé pour activer la fonction de défilement automatique. Cela vous permettra de vous déplacer plus rapidement dans la plage numérique proposée.
- Un écran de menu ou de saisie de données qui reste affiché pendant plus de 30 secondes sans qu'aucune action ne soit effectuée est annulé et l'affichage revient à l'état inactif/arrière-plan.

- À chaque fois que vous confirmez une action, un retour d'informations s'affiche pour indiquer la réussite, l'échec ou le lancement de l'opération en question.

Pour la liste complète des options de menu du panneau de l'opérateur, voir « Panneau de l'opérateur » dans le *Serveurs Sun Fire V20z et Sun Fire V40z — Guide de l'utilisateur* (819-2914-15).

Groupes d'utilisateurs

Les administrateurs peuvent définir différents groupes d'utilisateurs, ou types, sur le serveur. Les fonctions des différents types d'utilisateurs sont définies dans le TABLEAU 1-3.

Par exemple, lorsque vous vous connectez au système pour la première fois en utilisant le compte de configuration, la première chose que vous devez faire est configurer le compte de gestionnaire initial de sorte à pouvoir gérer d'autres comptes d'utilisateur (pour plus d'informations, voir « Création du compte de gestionnaire initial », page 19).

TABLEAU 1-3 Types d'utilisateurs

Type d'utilisateur	Fonction
monitor	Accès en lecture seule aux données des captures et à l'affichage des journaux
admin	Toutes les fonctions à l'exception de la gestion des comptes d'utilisateur et des mises à niveau sur site du SP
manager	Toutes les fonctions à l'exception de la mise à niveau sur site du SP
service	Mise à niveau sur site du SP

Utilisateurs

Les utilisateurs du SP se divisent en deux catégories : une catégorie de superutilisateurs qui peuvent se connecter au SP via SSH ; une catégorie d'utilisateurs qui peuvent établir des sessions IPMI avec le SP.

Ces deux catégories d'utilisateurs sont gérées indépendamment :

- Les utilisateurs qui sont créés en utilisant l'interface IPMI ne peuvent pas accéder au SP via SSH.
- Ceux qui se connectent en utilisant SSH ne peuvent pas accéder au SP via l'interface IPMI.

Il est possible de configurer le SP pour que les utilisateurs des services d'annuaire (ADS/NFS) puissent se connecter au SP via SSH. Ces utilisateurs des services d'annuaire ne pourront toutefois pas se connecter au SP via l'interface IPMI.

Fichiers de mots de passe

Les mots de passe des utilisateurs locaux, non-IPMI, sont stockés dans un fichier de mots de passe shadow Linux qui renforce la sécurité du système. Le fichier qui contient les mots hachés ne peut pas être lu par les utilisateurs.

Les mots de passe des utilisateurs IPMI sont stockés séparément. Les utilisateurs ne peuvent pas lire le fichier des mots de passe IPMI, mais les mots de passe qui y sont stockés ne sont pas chiffrés à cause de limites dues aux algorithmes d'authentification d'IPMI.

Tâches de gestion de systèmes

Pour effectuer la plupart des tâches de gestion de systèmes, vous pouvez utiliser les outils de gestion de systèmes inclus avec votre serveur. Le TABLEAU 1-4 liste certaines tâches de gestion de systèmes communes, les outils à votre disposition pour les remplir et signale les sections de ce document ou d'autres ressources contenant des informations sur la réalisation de ces tâches.

TABLEAU 1-4 Tâches de gestion de systèmes

Tâche	SM Console	Panneau de l'opérateur	Commande de gestion de systèmes	SNMP	IPMI
Analyse des événements	Oui : Aide en ligne	Oui : minimum	Oui : document sur les commandes SM	Oui	Oui : document sur les commandes SM
Configuration automatique du SP	Oui	Oui :	Oui : document sur les commandes SM	Non	Non
Configuration des services d'annuaire	Oui :	Non	Oui : document sur les commandes SM	Non	Non
Configuration d'un système de fichiers externe	Oui :	Non	Oui : document sur les commandes SM	Non	Non
Configuration des paramètres réseau	Oui :	Oui :	Oui : document sur les commandes SM, aide en ligne	Non	Oui :
Configuration des fonctions d'écriture de scripts	Oui :	Non	Oui : document sur les commandes SM, aide en ligne	Non	Non
Configuration de la notification des événements SMTP	Oui :	Non	Oui : document sur les commandes SM	Non	
Configuration des paramètres de date et d'heure du SP	Oui :	Non	Oui : document sur les commandes SM	Non	
Configuration de SSL	Oui :	Non	Oui : document sur les commandes SM	Non	

TABLEAU 1-4 Tâches de gestion de systèmes *(suite)*

Tâche	SM Console	Panneau de l'opérateur	Commande de gestion de systèmes	SNMP	IPMI
Création du compte de gestionnaire initial	Oui :	Non	Oui : document sur les commandes SM	Non	S/O
Définition du nom par défaut du système dans le panneau de l'opérateur	Non	Oui :	Oui : document sur les commandes SM	Non	Non
Contrôle du statut du système	Oui : aide en ligne	Oui :	Oui : document sur les commandes SM	Oui :	Oui :
Mise sous et hors tension	Oui :\	Oui :	Oui : document sur les commandes SM		Oui
Suppression du logiciel			Oui : document sur les commandes SM	Non	
Exécution des tests de diagnostic	Oui : Guide de dépannage	Non	Oui : Guide de dépannage	Non	Non
Exécution de Troubleshooting Dump Utility		Oui :	Oui : document sur les commandes SM	Non	Non
Définition du nom d'hôte du SP	Oui :	Oui :	Oui : document sur les commandes SM	Non	Non
Configuration de NSV	Oui :	Non	Oui : document sur les commandes SM, aide en ligne	Non	
Démarrage et arrêt du SE de la plate-forme	Oui :	Oui :	Oui : document sur les commandes SM, aide en ligne	Non	Oui :
Mise à jour du logiciel	Oui :	Oui :	Oui : document sur les commandes SM	Non	Oui, SP seulement :
Mise à jour du logiciel du SP	Oui :	Oui :	Oui : document sur les commandes SM	Non	Oui :

Configuration initiale du SP

Cette procédure décrit les étapes à suivre pour la configuration initiale du SP.

Partie I : Assignation des paramètres réseau au SP

Cette section contient deux méthodes permettant de définir les paramètres réseau du SP :

- « Assignation des paramètres réseau SP en utilisant DHCP », page 14
- « Assignation des paramètres réseau à un SP statique », page 16

Remarque – Une autre solution consiste, si aucun serveur DHCP ou accès physique n'est disponible, à configurer le SP en utilisant IPMItool conjointement avec un pilote de noyau IPMI. Pour configurer votre serveur pour IPMI, suivez les procédures appropriées pour votre système d'exploitation dans « Partie III : Activation de l'accès IPMI sur le serveur », page 22, puis « Partie IV : Activation de l'accès LAN IPMI », page 25.

Assignation des paramètres réseau SP en utilisant DHCP

La procédure qui suit permet de configurer les paramètres réseau du SP en utilisant DHCP depuis le panneau de l'opérateur. Si votre réseau n'utilise pas DHCP ou si vous voulez assigner une adresse IP statique au SP, suivez les instructions de « Assignation des paramètres réseau à un SP statique », page 16.

Remarque – Cette procédure part du principe que vous avez câblé votre serveur et l'avez mis sous tension comme décrit dans le Guide d'installation des serveurs Sun Fire V20z et Sun Fire V40z. Au moins un des ports du SP du serveur doit être connecté à un LAN.

---

1. **Appuyez sur un bouton quelconque du panneau de l'opérateur sur le panneau frontal du serveur (voir** FIGURE 1-6**).**

   L'écran LCD affiche la première option de menu :

   ```
   Menu:
   Server Menu
   ```

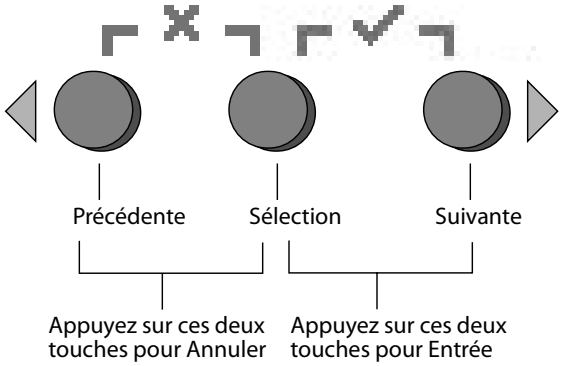


FIGURE 1-6 Boutons du panneau de l'opérateur

2. **Appuyez sur le bouton Suivante jusqu'à ce que vous atteigniez le menu SP :**

   ```
   Menu:
   SP menu
   ```

3. **Appuyez sur le bouton Suivante pour afficher les options du menu SP :**

   ```
   SP Menu:
   Set SP IP info?
   ```

4. **Appuyez sur le bouton de sélection.**

   Le message suivant s'affiche avec une réponse par défaut :

   ```
   SP use DHCP?
   Non
   ```

5. **Appuyez sur le bouton Suivante pour changer la réponse en** `Yes` **puis appuyez sur le bouton de sélection.**

6. **Appuyez sur le bouton de sélection à l'invite de confirmation.**

   ```
   SP use DHCP?
   Yes?
   ```

   Le serveur tente de contacter un serveur DHCP pour obtenir une adresse IP. Lorsque le serveur reçoit une réponse DHCP, l'écran LCD affiche les adresses IP de SP attribuées par DHCP. L'adresse du SP est configurée et le serveur est prêt à l'emploi.

Remarque – Selon les conditions de votre réseau, l'affichage de la nouvelle adresse IP allouée par le serveur DHCP sur l'écran LCD peut prendre jusqu'à dix secondes.

7. **Passez à « Partie II : Sécurisation du SP », page 19 pour les instructions à suivre pour la création d'un compte de gestionnaire initial.**

Remarque – Un message s'affiche vous invitant à effectuer une configuration automatique. Vous pouvez en effet, au lieu de configurer manuellement un SP, exécuter la configuration automatique qui réplique la configuration d'un SP sur un autre SP. Pour les instructions à suivre pour la configuration automatique, voir « Configuration automatique du SP (méthode optionnelle) », page 43.

Assignation des paramètres réseau à un SP statique

Depuis le panneau de l'opérateur, suivez les étapes ci-après pour configurer les paramètres réseau du SP en utilisant une adresse IP statique. Vous devez spécifier un masque de sous-réseau et une passerelle par défaut. Cet exemple utilise les paramètres d'exemple suivants :

Adresse IP : 10.10.30.5
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut : 10.10.30.254

1. **Appuyez sur un bouton quelconque du panneau de l'opérateur sur le panneau frontal du serveur (voir FIGURE 1-6).**

   L'écran LCD affiche la première option de menu :

   ```
   Menu:
   Server Menu
   ```

2. **Appuyez sur le bouton Suivante du panneau de l'opérateur jusqu'à ce que vous atteigniez le menu SP :**

   ```
   Menu:
   SP menu
   ```

3. **Appuyez sur le bouton Suivante du panneau de l'opérateur pour afficher les options du menu SP :**

   ```
   SP Menu:
   Set SP IP info?
   ```

4. **Appuyez sur le bouton de sélection du panneau de l'opérateur. Le message suivant s'affiche avec une réponse par défaut :**

   ```
   SP use DHCP?
   Non
   ```

5. **Appuyez sur le bouton de sélection du panneau de l'opérateur.**

   L'écran LCD affiche ce qui suit :

   ```
   Adresse IP du SP :
   0.0.0.0
   ```

6. **Le curseur étant dans le premier champ, augmentez ou diminuez la valeur en utilisant le bouton Précédente ou Suivante du panneau de l'opérateur.**

   La valeur contenue dans ce champ peut être comprise entre 0 et 255.

   ```
   Adresse IP du SP :
   10.0.0.0
   ```

7. **Une fois la valeur désirée atteinte, appuyez sur le bouton de sélection du panneau de l'opérateur pour amener le curseur au champ suivant.**

   ```
   Adresse IP du SP :
   10.0.0.0
   ```

8. **Répétez l'étape 6 et l'étape 7 pour chaque champ jusqu'à ce que l'adresse IP désirée s'affiche puis utilisez la combinaison de touches Entrée pour enregistrer l'adresse IP.**

   Le processus passe au prochain paramètre réseau, le masque de sous-réseau. L'écran LCD affiche ce qui suit :

   ```
   SP netmask:
   255.255.255.0
   ```

9. **Éditez le paramètre de masque de sous-réseau comme vous avez édité l'adresse IP. Lorsque vous avez terminé, utilisez la combinaison de touches Entrée pour enregistrer le masque de sous-réseau.**

   Le processus passe au prochain paramètre réseau, la passerelle par défaut. L'écran LCD affiche ce qui suit :

   ```
   Passerelle IP du SP :
   10.10.30.1
   ```

10. **Éditez le paramètre de la passerelle par défaut comme vous avez édité l'adresse IP et le masque de sous-réseau. Lorsque vous avez terminé, utilisez la combinaison de touches Entrée pour enregistrer la passerelle par défaut.**

    L'écran LCD affiche l'invite de confirmation suivante :

    ```
    Use new IP data:
    Yes?
    ```

11. **Appuyez sur le bouton de sélection du panneau de l'opérateur pour utiliser les nouvelles données ou utilisez la combinaison de touches Annuler pour ne pas en tenir compte.**

    L'adresse du SP est maintenant configurée et le serveur est prêt à l'emploi.

Remarque – Un message s'affiche vous invitant à effectuer une configuration automatique. Vous pouvez en effet, au lieu de configurer manuellement un SP, exécuter la configuration automatique qui réplique la configuration d'un SP sur un autre SP. Pour les instructions à suivre pour la configuration automatique, voir « Configuration automatique du SP (méthode optionnelle) », page 43.

---

12. **Continuez avec « Partie II : Sécurisation du SP », page 19.**

Partie II : Sécurisation du SP

Une fois que vous avez installé le serveur et configuré les paramètres réseau du SP, vous devez créer le compte de gestionnaire initial. Vous pourrez ensuite procéder à la configuration initiale du serveur et créer des comptes d'utilisateur supplémentaires. Seul l'administrateur qui effectue la configuration système initiale peut créer le compte de gestionnaire initial.

Attention – Le SP doit être sécurisé au moyen d'un nom d'utilisateur et d'un mot de passe quand le serveur est déployé pour la première fois. Ne pas sécuriser le SP peut exposer le serveur à une attaque de refus de service potentielle au travers de l'interface réseau du SP.

Création du compte de gestionnaire initial

Un compte de configuration est inclus avec tout serveur. Ce compte de configuration n'a pas de mot de passe. Lorsque vous vous connectez au SP pour la première fois en utilisant le compte de configuration, vous êtes invité à définir le compte de gestionnaire initial avec un mot de passe et une clé publique optionnelle.

Les noms d'utilisateurs et les mots de passe sont des chaînes composées de caractères alphanumériques, de traits de soulignements, de traits d'union ou de points.

- Les noms d'utilisateurs doivent être uniques et commencer par un caractère alphabétique.
- Les mots de passe peuvent contenir tout caractère imprimable et sont sensibles à la casse.
- Les noms d'utilisateur et les mots de passe ne peuvent pas dépasser 32 caractères et ne peuvent pas être des chaînes nulles ni vides.

Vous disposez de deux méthodes pour créer le compte de gestionnaire initial :

- Depuis une ligne de commande : voir « Création du compte initial depuis une ligne de commande », page 20.
- Depuis la console Server Management (SM) : voir « Création du compte initial depuis SM Console », page 20.

Création du compte initial depuis une ligne de commande

Connectez-vous au compte de configuration et créez le compte de gestionnaire initial en suivant la procédure ci-après :

1. **En utilisant un client SSHv1 ou SSHv2, connectez-vous à l'adresse IP du SP.**
2. **Authentifiez-vous comme l'utilisateur *setup* sans mot de passe.**

   # **ssh** *adresseipsp* **-l setup**

3. **Suivez les invites qui s'affichent pour créer le compte de gestionnaire initial.**

   Une fois le compte de gestionnaire initial créé, le compte de configuration est supprimé et vous êtes déconnecté du serveur. Vous pouvez ensuite vous connecter en utilisant le nouveau compte de gestionnaire initial, duquel vous pourrez créer d'autres comptes d'utilisateur.

Remarque – Si vous êtes invité à entrer un mot de passe, cela indique que le SP a déjà été sécurisé avec un compte. Si vous ne connaissez pas le nom de l'utilisateur de gestion ni son mot de passe, vous pouvez réinitialiser le SP depuis le panneau de l'opérateur en navigant jusqu'au menu `SP` et en sélectionnant l'option `Use defaults`. Vous remarquerez que tous les paramètres d'utilisateur et de réseau courants seront perdus et que le SP redémarrera.

Création du compte initial depuis SM Console

Pour plus d'informations sur les fonctions de SM, voir « Fonctions de la console Systems Management », page 48.

Pour créer le compte de gestionnaire depuis SM Console :

1. **Entrez le nom du SP ou son adresse IP en tant qu'URL ou adresse dans un navigateur, pour entrer dans SM Console.**

Remarque – Lorsque vous créez le compte de gestionnaire initial, vous êtes invité à accepter un accord de licence. Une fois que vous aurez créé le compte de gestionnaire initial cette invite n'apparaîtra plus.

---

2. **Dans l'écran Create Initial Manager-Level User ID, entrez un ID d'utilisateur pour ce compte.**
3. **Entrez un mot de passe pour le compte.**

4. **Ré-entrez le mot de passe pour confirmer.**

5. **Cliquez sur le bouton à cocher.**

6. **Utilisez SM Console pour sélectionner les options de configuration initiales.**

   Une fois l'utilisateur de niveau gestionnaire initial créé, l'écran Initial Configuration Checklist s'affiche dans SM Console. Cela vous permet de déterminer les options de votre choix pour la configuration initiale du SP.

   L'Initial Configuration Checklist est un tableau qui répertorie les options de menu de SM Console met les commandes que vous utilisez pour configurer chaque option. Ce tableau contient également des liens vers l'aide en ligne qui fournissent des instructions pour chaque option.

Remarque – Il s'affiche une fois l'utilisateur gestionnaire initial créé. Par conséquent, seul l'administrateur qui configure initialement le compte ou le réinitialise via le panneau de l'opérateur peut y accéder.

Remarque – L'adresse IP, le nom de l'utilisateur et le mot de passe que vous configurez sont représentés dans les exemples suivants comme *adripsp*, *utilisateursp* et *motpassesp*.

Partie III : Activation de l'accès IPMI sur le serveur

Cette section contient deux procédures : la première est relative à un serveur Linux et l'autre à un serveur x86 Solaris. Utilisez celle qui correspond à votre SE :

- « Activation de l'accès IPMI sur un serveur Linux (in-band) », page 22
- « Activation de l'accès IPMI sur un serveur x86 Solaris (in-band) », page 24

Activation de l'accès IPMI sur un serveur Linux (in-band)

1. **Connectez-vous au serveur et authentifiez-vous comme l'utilisateur *root*.**

2. **Installez le pilote de noyau Linux OpenIPMI à partir du CD Sun Fire V20z and Sun Fire V40z Servers Documentation and Support Files. Les pilotes se trouvent dans le répertoire du CD nommé** `/support/sysmgmt/`**.**

   Naviguez jusqu'à la version de SE installée sur votre serveur. Les options disponibles sont :

   - redhat/rhel3 pour Red Hat Enterprise Linux, version 3 (le mode 32-bits utilise le type d'architecture « i386 » ; le mode 64-bits le type d'architecture « x86_64 »)
   - suse/sles8 pour SUSE Enterprise Linux, version 8 (le mode 32-bits utilise le type d'architecture « i386 » ; le mode 64-bits le type d'architecture « x86_64 »)
   - suse/sles9 pour SUSE Enterprise Linux, version 9 (le mode 64-bits utilise le type d'architecture « x86_64 »)
   - suse/suse9 pour SUSE 9 Professional

3. **Assurez-vous que RPM kernel-source est déjà installé sur votre distribution en exécutant la commande suivante :**

   ```
   # rpm -qvi kernel-source
   ```

   Si cet utilitaire rapporte que le package kernel-source n'est pas installé, installez le RPM kernel-source courant pour la distribution de Linux installée.

   - Sur les distributions de SUSE, installez le RPM kernel-source en exécutant la commande suivante :

     ```
     # yast2
     ```

   - Sur les distributions RedHat, téléchargez le RPM kernel-source dans un répertoire temporaire (par exemple `/tmp`). Installez le package en exécutant la commande suivante :

     ```
     # rpm -ivh /tmp/kernel-source*.rpm
     ```

4. **Installez le RPM du pilote de noyau Linux d'OpenIPMI.**

   a. **Naviguez jusqu'à la version de SE installée sur votre serveur. Les options disponibles sont :**

      - redhat/rhel3 pour Red Hat Enterprise Linux, version 3 (le mode 32-bits utilise le type d'architecture « i386 » ; le mode 64-bits le type d'architecture « x86_64 »)
      - suse/sles8 pour Suse Enterprise Linux, version 8 (le mode 32-bits utilise le type d'architecture « i386 » ; le mode 64-bits le type d'architecture « x86_64 »)
      - suse/sles9 pour SUSE Enterprise Linux, version 9 (le mode 64-bits utilise le type d'architecture « x86_64 »)
      - suse/suse9 pour Suse 9 Professional

   b. **Installez le fichier du RPM d'OpenIPMI en exécutant la commande suivante :**

      # **rpm -ivh openipmi*.rpm**

Remarque – Le pilote du noyau sera compilé en utilisant le code kernel-source pendant l'installation.

---

5. **Installez IPMItool.**

   IPMItool est le client de gestion de serveur de l'interface de ligne de commande (CLI).

   - Si la distribution de Linux installée utilise l'architecture « i386 » 32 bits, exécutez la commande suivante :

     # **rpm -ivh ipmitool*.i386.rpm**

   - Si la distribution de Linux installée utilise l'architecture « x86_64 » 64 bits, exécutez la commande suivante :

     # **rpm -ivh ipmitool*.x86_64.rpm**

6. **Testez le pilote de périphérique du noyau IPMI et l'application cliente en exécutant la commande suivante :**

   # **ipmitool -I open chassis status**

   Une sortie indiquant une réussite ressemblera à la suivante :

```
"
System Power: on
Power Overload: false
Power Interlock: inactive
Main Power Fault: false
Power Control Fault: false
Power Restore Policy: unknown
Last Power Event:
Chassis Intrusion: inactive
Front-Panel Lockout: inactive
Drive Fault: false
Cooling/Fan Fault: false
"
```

Remarque – Lors du redémarrage suivant, il est possible que le pilote de noyau IPMI doive être rechargé avec la commande suivante :
modprobe ipmi_kcs_drv

Remarque – Si vous effectuez une mise à niveau de votre noyau de Linux, reportez-vous à « Mise à niveau du noyau de Linux », page 27.

Activation de l'accès IPMI sur un serveur x86 Solaris (in-band)

1. **Connectez-vous au serveur et authentifiez-vous comme l'utilisateur root.**
2. **Exécutez-la commande suivante pour installer le pilote de noyau Solaris x86 LIPMI et l'application de contrôle de gestion IPMItool.**

   Ces fichiers se trouvent sur le CD Documentation and Support Files dans le répertoire du CD nommé `support/sysmgmt/solaris9`.

   # **pkgadd -d ./**

   Confirmez l'installation de tous les packages quand vous y êtes invité.
3. **Redémarrez le serveur.**

Partie IV : Activation de l'accès LAN IPMI

Cette section contient trois procédures : deux de type in-band et une de type out-of-band. Utilisez celle qui correspond à votre SE :

- « Activation de l'accès LAN IPMI sur un serveur Linux (in-band) », page 25
- « Activation de l'accès LAN IPMI sur un serveur x86 Solaris (in-band) », page 26
- « Autre méthode permettant d'activer l'accès LAN IPMI (out-of-band) », page 26

Activation de l'accès LAN IPMI sur un serveur Linux (in-band)

1. **Si le serveur est mis hors tension, initialisez le SE local.**
2. **Connectez-vous au serveur et authentifiez-vous comme l'utilisateur *root*.**
3. **Chargez le pilote de périphérique de noyau OpenIPMI (tel qu'installé à l'étape 3 de « Activation de l'accès IPMI sur un serveur Linux (in-band) », page 22).**

   ```
   # modprobe ipmi_kcs_drv
   ```

4. **En utilisant les commandes suivantes dans IPMItool, configurez les paramètres réseau pour le SP.**

Remarque – Pour plus d'informations sur la syntaxe des commandes d'IPMItool, voir « Syntaxe », page 78.

```
# ipmitool -I open lan set 6 ipaddr adrip
# ipmitool -I open lan set 6 netmask masqueréseau
# ipmitool -I open lan set 6 defgw ipaddr adripwg
# ipmitool -I open lan set 6 password motpasseipmi
```

Activation de l'accès LAN IPMI sur un serveur x86 Solaris (in-band)

1. **Si le serveur est mis hors tension, initialisez le SE local.**
2. **Connectez-vous au serveur et authentifiez-vous comme l'utilisateur *root*.**
3. **En utilisant IPMItool, configurez les paramètres réseau pour le SP en utilisant les commandes suivantes.**

Remarque – Pour plus d'informations sur la syntaxe des commandes d'IPMItool, voir « Syntaxe », page 78.

```
# ipmitool -I lipmi lan set 6 ipaddr adrip
# ipmitool -I lipmi lan set 6 netmask masqueréseau
# ipmitool -I lipmi lan set 6 defgw ipaddr adripwg
# ipmitool -I lipmi lan set 6 password motpasseipmi
```

Autre méthode permettant d'activer l'accès LAN IPMI (out-of-band)

1. **En utilisant un client SSHv1 ou SSHv2, connectez-vous à l'adresse IP du SP.**
2. **Authentifiez-vous comme l'utilisateur de gestion qui vient d'être créé (voir « Partie II : Sécurisation du SP », page 19).**

   ```
   # ssh adripsp -l utilisateursp
   ```

3. **Activez l'accès LAN IPMI et attribuez un mot de passe lorsque vous y êtes invité.**

   ```
   # ipmi enable channel lan
   # exit
   ```

Remarque – Ce mot de passe sera indiqué par *motpasseipmi* dans les exemples suivants.

---

4. **Testez l'accès LAN IPMI en utilisant IPMItool.**

   ```
   # ipmitool -I lan -H adripsp -P motpasseipmi statut châssis
   ```

Mise à niveau du noyau de Linux

Mettre à niveau le noyau de Linux installé vers une version plus récente vous oblige à recompiler le pilote de périphérique du noyau IPMI.

1. **Installez le RPM kernel-source qui correspond à la version du package RPM binaire du noyau mis à jour.**
2. **Connectez-vous au serveur et authentifiez-vous comme l'utilisateur *root*.**
3. **Passez au répertoire suivant :**

   # **cd /usr/src/kernel-modules/openipmi**

4. **Recompilez le noyau en exécutant les commandes suivantes :**

   # **make clean**
   # **make**
   # **make install**

5. **Re-testez le pilote de périphérique du noyau IPMI et l'application cliente en exécutant la commande suivante :**

   # **ipmitool -I open chassis status**

   Une sortie indiquant une réussite ressemblera à la suivante :

```
"
System Power: on
Power Overload: false
Power Interlock: inactive
Main Power Fault: false
Power Control Fault: false
Power Restore Policy: unknown
Last Power Event:
Chassis Intrusion: inactive
Front-Panel Lockout: inactive
Drive Fault: false
Cooling/Fan Fault: false
"
```

Remarque – Lors du redémarrage suivant, il est possible que le pilote de noyau IPMI doive être rechargé avec la commande suivante :
modprobe ipmi_kcs_drv

Intégration au site

Lorsque vous déployez votre serveur, assurez-vous de déterminer la meilleure stratégie d'intégration pour votre environnement.

Ces serveurs incluent des connexions réseau pour le processeur de service, qui sont séparées des connexions réseau destinées à la plate-forme. Cela vous permet de configurer le serveur de sorte que le SP soit connecté à un réseau de gestion isolé et ne soit pas accessible depuis le réseau de production.

Raccordement de serveurs en guirlande

Vous pouvez connecter plusieurs serveurs selon différentes configurations en guirlande en utilisant des connecteurs SP pour former un LAN de gestion, comme indiqué à la FIGURE 1-7, la FIGURE 1-8 et la FIGURE 1-9. Les figures montrent également comment les serveurs sont connectés à des LAN externes en utilisant les connecteurs gigabit de la plate-forme.

Remarque – Sun Microsystems recommande d'utiliser des câbles cross-over d'au moins un mètre de long pour le raccordement en guirlande des serveurs.

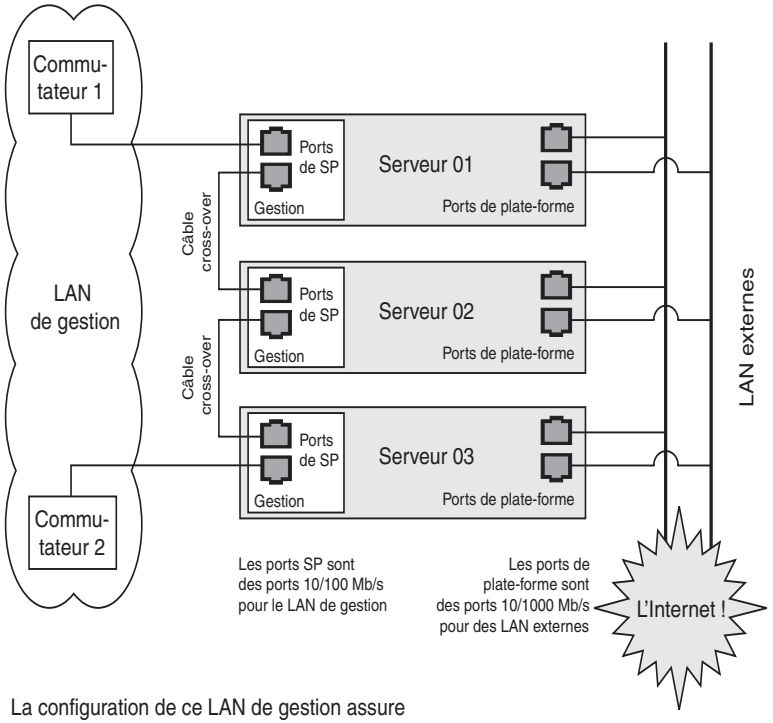
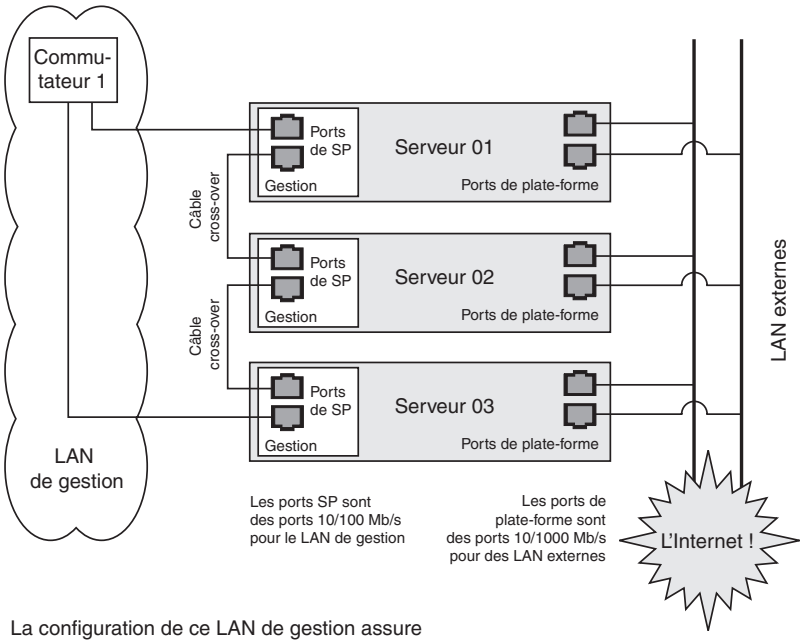


FIGURE 1-7 Architecture en guirlande avec redondance au niveau des commutateurs sur le LAN de gestion

Pour interconnecter les serveurs, vous devez utiliser un câble cross-over RJ-45. Les câbles peuvent être connectés au port supérieur ou inférieur du SP. Pour configurer les serveurs en guirlande, connectez le premier et le dernier serveurs de la chaîne à des commutateurs différents.

Dans la configuration illustrée à la FIGURE 1-7, deux commutateurs gérés à algorithme d'arbre maximal sont requis pour connecter de façon redondante à la fois le début et la fin de la chaîne. Si les commutateurs ne sont pas en mesure de gérer la détection de l'arbre maximal, connectez alors uniquement le début ou la fin de la chaîne mais pas ces deux éléments.



La configuration de ce LAN de gestion assure la redondance au niveau des ports de SP.

FIGURE 1-8 Architecture en guirlande avec redondance au niveau des ports sur le LAN de gestion

Pour interconnecter les serveurs, vous devez utiliser un câble cross-over RJ-45. Les câbles peuvent être connectés au port supérieur ou inférieur du SP. Pour configurer les serveurs en guirlande, connectez le premier et le dernier serveurs de la chaîne à des commutateurs différents.

Dans la configuration illustrée à la FIGURE 1-8, un commutateur géré à algorithme d'arbre maximal est requis pour connecter de façon redondante à la fois le début et la fin de la chaîne. Si le commutateur n'est pas en mesure de gérer la détection de l'arbre maximal, connectez alors uniquement le début ou la fin de la chaîne mais pas à ces deux éléments.

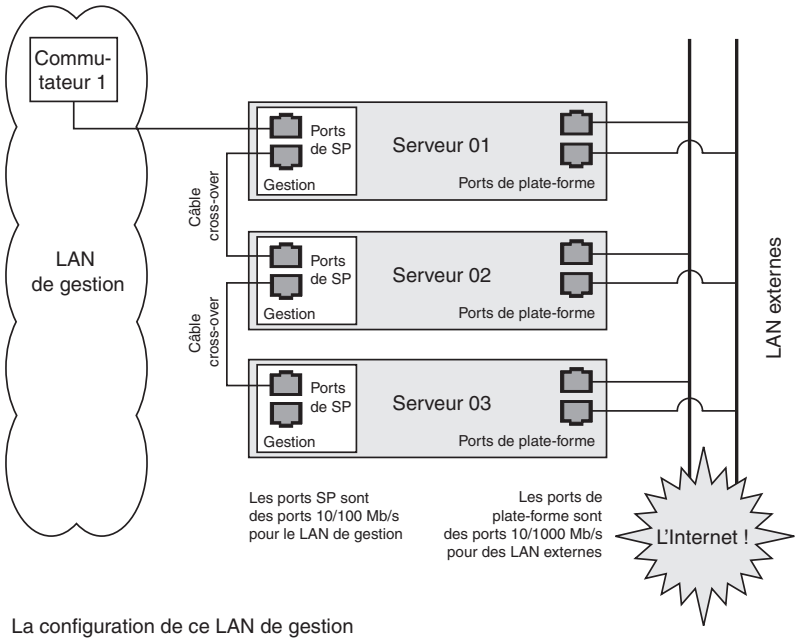


FIGURE 1-9 Architecture en guirlande sans redondance sur le LAN de gestion

Pour interconnecter les serveurs, vous devez utiliser un câble cross-over RJ-45. Les câbles peuvent être connectés au port supérieur ou inférieur du SP.

Dans la configuration illustrée à la FIGURE 1-9, aucune redondance n'est fournie sur le LAN de gestion.

Pilotes de plates-formes et applications

L'installation des pilotes de plates-formes et des applications fournit les fonctions suivantes :

- Elle permet la communication entre le SP et la plate-forme, ce qui permet un meilleur contrôle de la plate-forme. La plate-forme peut, par exemple, être arrêtée ou redémarrée correctement et non par force, au moyen de mises hors tension et réinitialisations.
- Elle permet aux déroutements SNMP de la plate-forme d'être transmis au travers du démon SNMP du SP.
- Elle permet au SP de contrôler l'intégrité du système d'exploitation de la plate-forme en cas de problèmes de plate-forme, et de tenter de gérer les erreurs de contrôle machine.
- Elle permet au SP de recueillir davantage de données VPD (*Vital Product Data*, données produit vitales) sur les composants du système.
- Elle permet au SP de recueillir des informations d'inventaire sur le logiciel de système d'exploitation.
- Elle permet de mettre à jour le BIOS de la plate-forme à partir du SP.

Si vous n'installez *pas* le logiciel de plate-forme Newisys, les fonctions suivantes ne seront *pas* disponibles depuis le SP :

- capacité d'arrêter et redémarrer la plate-forme progressivement ;
- capacité de recevoir des avis signalant les événement de contrôle machine corrigible et les erreurs ECC ;
- capacité d'obtenir le nom d'hôte de la plate-forme ;
- capacité de déterminer le statut courant du SE ;
- capacité de déterminer la version courante et l'inventaire des logiciels de la plate-forme ;
- capacité d'obtenir les VTD de la CPU et les informations d'inventaire ;
- capacité de déterminer si la plate-forme est en cours d'exécution, via la pulsation de la plate-forme ;
- capacité d'obtenir des informations SNMP côté plate-forme, si rattachée au serveur SNMP du SP ;capacité de définir l'adresse jnet de la plate-forme avec la commande `sp set jnet`.

Les fonctions ou caractéristiques ci-dessous sont disponibles sans installer les pilotes de la plate-forme. Le SP devra toutefois avoir été complètement initialisé pendant la dernière initialisation du BIOS :

- Les informations d'inventaire du BIOS sont disponibles via le SP.
- L'heure du SP est synchronisée sur la plate-forme.
- La gestion thermique optimisée est disponible via le SP.

Autres points importants sur les logiciels de la plate-forme

- Quand vous installez le système d'exploitation d'une plate-forme, vous avez la possibilité de configurer la prise en charge linguistique. Si vous choisissez une langue autre que l'anglais, assurez-vous d'installer aussi la version appropriée des pilotes de parties tierces.
- Quand vous installez le système d'exploitation d'une plate-forme, vous pouvez configurer l'état d'alimentation. Lorsque vous choisissez un état d'alimentation, désactivez Suspend et Hibernate.
- Il y a entre le SP et la plate-forme un réseau privé qui prend en charge les communications internes.
  - L'adresse locale de liaison 169.254.101.2 est attribuée au SP.
  - L'adresse locale de liaison 169.254.101.3 est attribuée à la plate-forme pour la communication sur ce réseau privé. Ces adresses sont attribuées physiquement et non pas générées de manière aléatoire, et sondées pour contrôler l'absence de conflits. Vous pouvez utiliser la commande `sp set jnet` pour changer ces adresses IP. Les pilotes de la plate-forme doivent être installés pour que la communication JNET fonctionne.

Mise à jour du logiciel

Remarque – Pour des informations complètes sur les options de menu disponibles via le panneau de l'opérateur, voir le *Serveurs Sun Fire V20z et Sun Fire V40z — Guide de l'utilisateur.*

Si vous essayez de mettre à jour le logiciel du SP en utilisant le panneau de l'opérateur lorsque l'adresse IP du SP n'a pas été définie, la mise à jour échoue. Assurez-vous que l'adresse IP a été définie avant de tenter une mise à jour. Pour plus d'informations, voir le *Serveurs Sun Fire V20z et Sun Fire V40z — Guide d'installation*.

Un nouveau volume de partage réseau (NSV) qui est installé sur votre réseau contient les packages du microprogramme. Vous pouvez rendre ces packages de microprogramme disponibles pour un SP de l'une ou l'autre des façons suivantes :

- La méthode recommandée est celle utilisant l'Update Server, une application Java qui transfert les packages du NSV au SP.
  - Vous pouvez mettre à jour plusieurs SP simultanément si vous utilisez l'application Update Server.
  - Vous devez utiliser l'application Update Server pour mettre à jour le package de base du SP.
- Une autre méthode consiste à utiliser le SP pour créer un montage NFS (Network File System, système de fichiers réseau) sur le NSV. Cela fait, le NSV et les packages qu'il contient apparaissent en local pour le SP et sont ainsi disponibles pour la mise à jour.

Remarque – Le dernier numéro de version du BIOS n'est jamais le même que le dernier numéro de version de NSV, tel que présenté dans les lignes de données d'exemple du fichier de configuration dans « Configuration et démarrage de l'application Update Server », page 37.

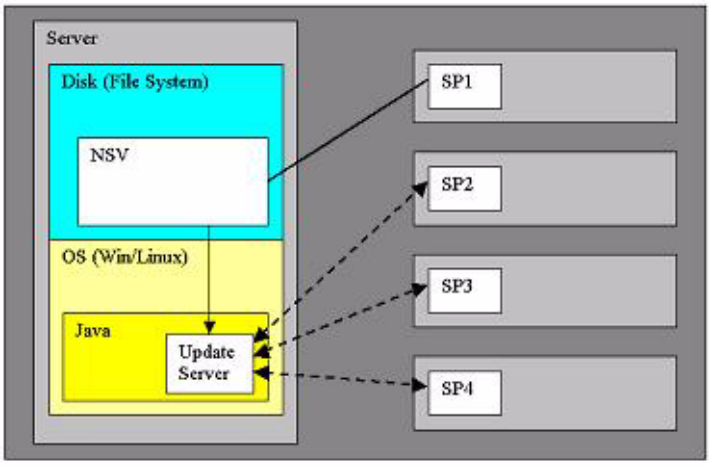


FIGURE 1-10 NSV sur un serveur accessible du réseau

Dans l'illustration ci-dessus, le NSV a été décompressé et enregistré sur un serveur accessible via le réseau par les SP qui ont besoin de packages à jour. SP1 a monté directement le NSV. SP2, SP3 et SP4 accèdent au NSV via l'Update Server.

Remarque – Dans cet exemple, SP1 ne peut pas mettre à jour le package de base du SP sans utiliser l'application Update Server.

Sélection et configuration du serveur de fichiers

Sélectionnez un serveur accessible via le réseau par le ou les SP.

Remarque – L'Update Server a besoin de Java, la version 1.4 minimum est requise. Si vous envisagez d'utiliser l'Update Server, ouvrez une fenêtre d'invite de commande ou de shell et saisissez **`java -version`** pour vérifier la version.

Pour installer le NSV, suivez les étapes ci-dessous.

1. **Téléchargez la dernière version ou procurez-vous le CD le plus récent du NSV.**
2. **Extrayez les fichiers et le NSV compressé dans un emplacement du serveur de fichiers sélectionné.**

Remarque – Lorsque vous décompressez un fichier compressé sur Linux, utilisez le commutateur **`-a`** (par exemple : **`unzip -a nomfichier.zip`**) pour forcer la conversion dans les fichiers de texte de la terminaison de fin de ligne appropriée au système d'exploitation cible.

Un nouveau fichier manifeste (`releaseVersion.xml`) est ajouté au répertoire racine du NSV. Pour plus de détails sur la structure du NSv, reportez-vous à « CD-ROM Network Share Volume (NSV) », page 120.

---

3. **Pour les systèmes basés sur Linux, assurez-vous que le répertoire NSV a été exporté.**
4. **Choisissez le mode de mise à jour : application Update Server ou montage NFS :**
   - Si vous envisagez d'utiliser l'application Update Server, allez à « Configuration et démarrage de l'application Update Server », page 37.
   - Si vous envisagez d'effectuer la mise à jour avec la méthode du montage NFS, connectez-vous au SP et montez le NSV.

     Par exemple, si l'adresse IP de la machine avec le nouveau NSV est 10.10.20.100 et que vous extrayez les fichiers NSV dans un répertoire nommé `newNSV`, vous exécuterez la commande suivante :

     ```
     sp add mount -r 10.10.20.100:/newNSV -l /mnt
     ```

     Le NSV sera ensuite disponible pour le SP en `/mnt/sw_images/`.

     Continuez avec « Identification des packages pour la mise à jour », page 38.

Configuration et démarrage de l'application Update Server

Le fichier de configuration d'Update Server vous permet d'exporter plusieurs packages avec plusieurs versions vers un ou plusieurs SP. Pour sélectionner les mise à jour appropriées, suivez les instructions ci-dessous.

1. **Naviguez vers** `NVS/serveur_mis_à_jour/`*Vx.xx* **(où** *Vx.xx* **est la version voulue) pour trouver le fichier de configuration.**

   Le fichier de configuration inclut des lignes de données d'exemple, indiquées ci-dessous.

```
SP_BASE         V2.0.0.38  /nsv/sw_images/sp/spbase/V2.0.0.38/install.image
SP_BASE         V2.0.0.40  /nsv/sw_images/sp/spbase/V2.0.0.40/install.image
SP_VALUE_ADD    V2.0.0.38  /nsv/sw_images/sp/spvalueadd/V2.0.0.38/install.image
SP_VALUE_ADD    V2.0.0.40  /nsv/sw_images/sp/spvalueadd/V2.0.0.40/install.image
BIOS-X250Alpha V1.27.9     /nsv/sw_images/platform/firmware/bios/V1.27.9/bios.sp
```

Remarque – Le dernier numéro de version du BIOS n'est jamais le même que le dernier numéro de version de NSV, comme indiqué dans l'exemple ci-dessus.

   Chaque ligne de données contient des trois valeurs séparées par des espaces :

   - Type du package : `SP-BASE`, `SP_VALUE_ADD`, `BIOS`

     Pour prendre en charge les mises à jour du BIOS pour plusieurs produits requérant chacun un microprogramme BIOS unique, le package du BIOS doit inclure l'ID du produit. L'ID du produit est la valeur qui est retournée par la commande `platform get product-id`. Il figure également dans le manifeste du logiciel du BIOS (`swimventory.xml`) qui est inclus dans un NSV. L'ID de produit actuel utilisé dans l'exemple ci-dessus est `x250 Alpha`. Lorsque vous l'incluez dans le type de package du NBIOS dans le fichier de configuration, vous devez ajouter un trait d'union entre BIOS et l'ID de produit et ne pas laisser d'espaces dans la chaîne d'ID de produit.

   - Version, dans le format de version standard : `V`*[major].[minor].[patch].[build].*
   - Chemin du fichier : chemin courant et nom de fichier d'un fichier de mise à jour.

2. **Dans le fichier de configuration, chaque ligne de données est précédée d'un signe `#`. Pour indiquer un fichier devant être mis à jour, ajoutez le numéro de version correct et supprimez le signe `#` au début des lignes de données.**

3. **Naviguez vers le dossier NSV qui contient l'application Update Server et démarrez le serveur via la ligne de commande :**

   java -jar updateServer.jar -c updateServer.config -p *<port>* **-l logfile.log**

   Le fichier `updateServer.jar` se trouve dans le dossier `update_server` du NSV.

   - Il est recommandé d'utiliser l'indicateur `-l` pour créer un fichier journal.
   - Seuls le début et la fin d'une transaction de mise à jour seront envoyés à la console.
   - Des informations détaillées sur le processus de mise à jour sont envoyées au fichier journal, qui peut être utile si vous devez isoler la cause de l'échec d'une mise à jour.
   - Par défaut, le serveur utilise le numéro de port 52708.
   - Si ce numéro de port est déjà utilisé, utilisez l'indicateur -p optionnel pour spécifier un autre port.
   - L'Update Server ne démarre pas si le fichier n'est pas trouvé dans le chemin spécifié. Sinon, le serveur est prêt à recevoir des requêtes de mise à jour de n'importe quel SP.
   - L'Update Server peut accepter simultanément plusieurs requêtes de mise à jour provenant de différents SP.

Identification des packages pour la mise à jour

1. **Pour déterminer les packages couramment installés sur un SP, exécutez la commande suivante depuis ce SP :**

   inventory get software

2. **Pour déterminer les packages disponibles depuis l'application Update Server en cours d'exécution, exécutez la commande suivante depuis le SP :**

   inventory get remote-software -i *<adresseip_serveur>* **-p** *<port_serveur>*

   Remarque – Certaines versions plus anciennes du SP n'acceptent pas les options `-i` ou `-p`. Ces versions plus anciennes n'acceptent que les arguments suivants : `[{-a|--all}], [{-D|--Delim}]` et `[{-H|--noheader}]`.

   ---

3. **Pour comparer les packages couramment installés avec ceux disponibles sur un NSV monté, exécutez la commande suivante depuis le SP :**

   inventory compare versions -f *<nomfichier_manifeste>*

4. **Pour comparer les packages couramment installés avec ceux disponibles sur un Update Server en cours d'exécution, exécutez la commande suivante depuis le SP :**

   `inventory compare versions -i` *<adresseip_serveur>* **`-p`** *<port_serveur>*

Remarque – Certaines versions plus anciennes du SP n'acceptent pas les options `-i` ou`-p`. Ces versions plus anciennes n'acceptent que les arguments suivants : `[{-a|--all}], [{-D|--Delim}] et [{-H|--noheader}]`.

Mise à jour du package de base du SP

Remarque – Vous pouvez utiliser l'application Update Server pour installer ce package, ou utiliser l'option SP Update Flash du menu SP du panneau de l'opérateur.

Le composant de base du SP inclut le composant SP Value-Add, qui est également mis à jour dans le cadre de ce processus.

Remarque – Compte tenu que le package Value-Add peut contenir toutes les mises à jour de fonctions dans une nouvelle version, contrôlez les *Release Notes* pour déterminer le package à mettre à jour.

---

1. **Connectez-vous au SP.**
2. **Exécutez la commande SP pour lancer le processus de mise à jour sur le SP :**

   `sp update flash all -i` *<adresse_ip_serveur>* **`-p`** *<port_serveur>* **`-r`** *<version>*

   - L'indicateur optionnel -p flag indique que le serveur est exécuté sur un port qui n'est pas celui par défaut. Cette commande interroge l'Update Server pour déterminer s'il est en cours d'exécution. Dans l'affirmative, la connexion prend fin lorsque le SP redémarre et le processus de mise à jour commence.
   - L'indicateur –r indique la version demandée du package distant. Si LATEST est spécifié, la dernière version disponible du package est demandée.

Remarque – Les versions plus anciennes du SP ne prennent pas en charge l'option -r. Si vous exécutez la commande `sp update flash all` avec une version plus ancienne du SP, l'Update Server va automatiquement mettre à jour votre logiciel à la version la plus récente.

---

3. **Contrôlez le processus de mise à jour sur le serveur. Des messages s'affichent au début et à la fin du processus (le fichier journal d'Update Server contient davantage de détails sur les processus de mise à jour). À la fin de la mise à jour, le SP redémarre avec la nouvelle version.**

Remarque – Si vous effectuez une mise à jour vers une nouvelle version du package SP Base ou Value-Add, mais n'installez pas la documentation associée dans le NSV, l'aide en ligne ne fonctionnera pas. Après avoir monté le système de fichiers, contrôlez la version du package SP Value-Add dans l'inventaire du logiciel. Assurez-vous que la dernière version de la documentation est installée dans le répertoire `/docs`.

Mise à jour du package SP Value-Add

Il est possible qu'une nouvelle version du composant SP Value-Add contienne toutes les nouvelles fonctions. Contrôlez les notes de version pour savoir si la mise à jour concerne le package SP Value-Add ou le package SP Base.

Remarque – Vous n'avez *pas* à effectuer cette mise à jour si vous avez déjà mis à jour le package SP Base.

---

1. **Connectez-vous au SP.**
2. **Exécutez la commande suivante :**

   `sp update flash applications -i` *<adresseip_serveur>* **`-p`** *<port_serveur>* **`-r`** *<version_package>*

Remarque – Si vous utilisez un montage NFS, exécutez la commande suivante : **`sp update flash applications -f`** *<nomfichier>*

Mise à jour du BIOS

Trois méthodes permettent de mettre à jour le BIOS, comme indiqué dans les procédures de cette section :

- l'utilisation de l'application Update Server,
- le montage du NSV,
- la copie directe de l'image du BIOS.

Utilisation de l'application Update Server pour la mise à jour du BIOS

1. **Suivez les étapes figurant dans « Configuration et démarrage de l'application Update Server », page 37 pour utiliser l'Update Server.**
2. **À l'invite du SP, entrez la commande suivante :**

   `platform set os state update-bios -i` *<adresseip_serveur>* **`-p`** *<port_serveur>* **`-r`** *<version_package>*

Montage du NSV pour la mise à jour du BIOS

1. **Connectez-vous au SP et montez le NSV.**

   Par exemple, si l'adresse IP de la machine avec le nouveau NSV est 10.10.20.100 et que vous extrayez les fichiers NSV dans un répertoire nommé `newNSV`, vous exécuterez la commande suivante :

   ```
   sp add mount -r 10.10.20.100:/newNSV
   ```

   Le NSV sera ensuite disponible pour le SP en `/mnt/sw_images/`.

2. **À l'invite du SP, entrez la commande suivante :**

   `platform set os state update-bios /mnt/sw_images/platform/firmware/bios/`*Vx.x.x.x***`/bios.sp`**

Copie de l'image du BIOS pour la mise à jour du BIOS

1. **Copiez l'image du BIOS directement de NSV au dossier `/tmp` sur le système de fichiers du SP.**
2. **À l'invite du SP, entrez la commande suivante :**

   ```
   platform set os state update-bios /tmp/bios.sp
   ```

Mise à jour des diagnostics

Les tests de diagnostic basés sur le SP sont stockés dans le NSV et référencés par le lien symbolique `/diags` dans le SP. Le logiciel du SP référencie une version par défaut des diagnostics. Cependant, si une nouvelle version est proposée et stockée sur le NSV, vous devez pointer sur cette nouvelle version pour l'utiliser.

1. **Connectez-vous au SP.**
2. **Montez le NSV en utilisant la commande** `sp add mount`**. Par exemple :**

   `sp add mount -r` *<CHEMIN_RÉSEAU>*

   Cette opération monte le répertoire spécifié par *CHEMIN_RÉSEAU* sur `/mnt`.
3. **Pour vérifier que le montage a réussi, tapez `ls /mnt/diags`. Par exemple :**

   `ls /mnt/diags V2.4.1.0`
4. **Utilisez la commande** `sp update diags` **pour établir une liaison logicielle de** `/diags` **au répertoire de diagnostics désiré. Par exemple :**

   `sp update diags -p /mnt/diags/V2.4.1.0`
5. **Pour vérifier ce nouveau lien logiciel, tapez `ls -l /diags`. Par exemple :**

   `ls -l /diags /diags -> /mnt/diags/V2.4.1.0`
6. **Pour vérifier si le sous-système de diagnostic est disponible, exécutez la commande suivante :**

   `diags`

   Cette opération liste toutes les sous-commandes de la commande `diags`.

Remarque – Pour la liste complète des modules de diagnostic et un exemple de sortie, reportez-vous au *Guide de l'utilisateur*.

Configuration automatique du SP (méthode optionnelle)

La configuration automatique réplique la majorité des fichiers de configuration d'un SP déjà configuré sur un autre SP, de sorte que les deux serveurs aient des configurations identiques à l'exception du nom de l'hôte et de l'adresse IP.

Par exemple, après avoir configuré un SP (en avoir défini les utilisateurs, les certificats, les montages, etc.), vous pouvez exécuter la configuration automatique sur chacun des autres SP pour que les paramètres soient identiques. De plus, si vous modifiez la configuration d'un SP, vous pouvez tous les mettre à jour en ré-exécutant sur chacun la configuration automatique (pour cette raison, définissez l'adresse IP du serveur de configuration automatique sur x.x.x.1.)

Pour la liste des fichiers qui sont copiés ou ne sont pas copiés pendant le processus de configuration automatique, voir « Fichiers copiés pendant le processus de configuration automatique », page 45.

Remarque – La configuration automatique ne fusionne pas les configurations mais écrase la configuration existante.

Remarque – La configuration automatique ne fonctionne pas sur des plates-formes serveurs différentes. C'est-à-dire que vous ne pouvez pas configurer un SP Sun Fire V40z en utilisant des paramètres définis sur un SP Sun Fire V20z.

Remarque – La configuration automatique ne fonctionne pas non plus sur des versions différentes du logiciel du SP. Les serveurs doivent exécuter la même version du logiciel du SP.

Vous pouvez démarrer la configuration automatique soit lorsque vous y êtes invité à la fin de la configuration de l'adresse IP du SP, soit en sélectionnant à tout moment l'option de menu SP sur le panneau de l'opérateur.

Pour procéder à la configuration automatique d'un SP, suivez les étapes ci-après :

1. **Sur le panneau de l'opérateur, appuyez sur le bouton Suivante ou Précédente jusqu'à ce que l'invite suivante s'affiche.**

   ```
   SP Autoconfigure?
   ```

2. **Appuyez sur le bouton de sélection.**

   L'invite suivante s'affiche :

   ```
   SP Auto Setup?
   No
   ```

3. **Appuyez sur le bouton Suivante ou Précédente pour changer la réponse en** `Yes`**.**

   Pour plus d'informations sur la configuration d'une adresse IP, voir le *Serveurs Sun Fire V20z et Sun Fire V40z — Guide d'installation*.

4. **Appuyez sur le bouton de sélection.**

   Le SP tente de localiser une adresse IP.

   - S'il y parvient, l'invite suivante s'affiche indiquant une adresse IP pour ce SP :

     ```
     Setup Server IP:
     x.x.x.1
     ```

     Où *x.x.x* correspond aux trois premiers octets de l'adresse IP du SP. Par exemple, si l'adresse est 10.10.30.19, l'adresse qui s'affiche dans l'invite est 10.10.30.1.

     Dans ce cas, appuyez sur le bouton de sélection du panneau de l'opérateur pour lancer la configuration automatique.

   - Si le SP ne localise pas l'adresse IP, le message suivant s'affiche :

     ```
     Unable to get
     SP IP address
     ```

     Dans ce cas, vous devez entrer manuellement une adresse IP avant d'appuyer sur le bouton de sélection du panneau de l'opérateur pour lancer la configuration automatique.

5. **Attendez que la fin de la configuration automatique, le SP redémarrera automatiquement.**

   Le message suivant s'affiche pendant l'exécution de la configuration automatique.

   ```
   SP AutoConfigure
   in progress
   ```

Remarque – Si la configuration automatique échoue, un message d'échec s'affiche. Appuyez sur un bouton quelconque pour l'effacer.

Fichiers copiés pendant le processus de configuration automatique

Le TABLEAU 1-5 liste les fichiers qui sont copiés pendant le processus de configuration automatique. Le TABLEAU 1-6 indique les fichiers qui ne sont pas copiés au cours de ce processus.

Le processus de configuration automatique effectue des contrôles de sécurité sur certains fichiers.

- Les fichiers `passwd` et `shadow` sont traités pour ne laisser passer que les comptes d'utilisateur qui peuvent être créés au travers de la commande `access`.
- Le compte *root*, activé ou non, n'est pas cloné.
- Le fichier `fstab` transfère uniquement les informations de point de montage relatives à `/mnt`.
- Seuls les fichiers de clé ssh des utilisateurs qui sont autorisés sur le système sont répliqués sur la cible. Les fichiers de clé des utilisateurs qui ont été supprimés de la cible sont supprimés.
- Sous la version 2.1.* du logiciel du SP, les fichiers `IPMIConfig.xml` et `SystemStruct.xml` ne sont copiés que si l'ID du produit et la révision de la carte sont identiques. Ces fichiers ne peuvent pas être transférés d'un serveur exécutant la version 2.1.* du logiciel du SP à un serveur exécutant la version 2.2.* ni vice-versa.

Tous les fichiers sont transférés entre les deux hôtes au travers d'une connexion de fiche SSL. Cela est vrai même si l'option `ssl_not_enforced` est activée.

TABLEAU 1-5 Fichiers copiés pendant le processus de configuration automatique

Fichier	But
`/pstore/passwd`	Liste des comptes d'utilisateur
`/pstore/group`	Liste des groupes d'utilisateurs
`/pstore/shadow`	Mots de passe des comptes d'utilisateur (utilisateurs locaux uniquement)
`/pstore/fstab`	Informations sur le système de fichiers `/mnt`
`/pstore/smb.creds`	Informations de type utilisateur/mot de passe pour le montage SMB
`/pstore/evcfg.xml`	Fichier de configuration du gestionnaire d'événements
`/pstore/seccfg.xml`	Fichier de configuration du gestionnaire de la sécurité
`/pstore/oppanelcfg.xml`	Fichier de configuration du panneau de l'opérateur
`/pstore/snmpd.conf.template`	Fichier de configuration SNMP
`/pstore/snmp_proxy_community.txt`	Fichier de configuration SNMP

TABLEAU 1-5 Fichiers copiés pendant le processus de configuration automatique *(suite)*

Fichier	But
`/pstore/resolv.conf`	Configuration du Directory Name Service
`/pstore/jnet_config`	Configuration réseau JNET
`/pstore/krb5.keytab`	Configuration de l'authentification Kerberos (pour l'authentification Windows)
`/pstore/ssl_not_enforced`	Désactive l'exigence d'une clé SSL pour la console de l'IG SM (***Remarque -*** *La console IG SM n'est pas disponible sur les serveurs Sun Fire V20z et Sun Fire V40z)*
`/pstore/user_ssl_server.key,.crt`	Clé SSL et certification pour la console de l'IG SM (**Remarque -** *La console IG SM n'est pas disponible sur les serveurs Sun Fire V20z et Sun Fire V40z)*
`/pstore/ssh_known_hosts`	Clés d'hôtes SSH (hôtes de confiance)
`/pstore/ssh_authorized_keys/*`	Clés d'utilisateurs SSH (utilisateurs de confiance)
`/pstore/IPMI/IPMIConfig.xml`	Configuration IPMI
`/pstore/IPMI/ipmiusers`	Liste des utilisateurs IPMI (***Remarque -*** *n'est pas copié par les serveurs ou les clients exécutant la version 2.1.* du logiciel du SP)*
`/pstore/SystemsStruct.xml`	Seuils de capteurs modifiés par l'utilisateur
`/dev/mtd/custom`	Section de la configuration personnalisée

TABLEAU 1-6 Fichiers copiés pendant le processus de configuration automatique

Fichier	But
/pstore/mc.conf	Configuration des contrôles de la machine
/pstore/hostname	Nom d'hôte du SP local
/pstore/ifcfg2-eth0	Adresse IP du SP local
/pstore/dimm.map	Configuration des DIMM de la plate-forme
/pstore/edstatefile	Journal d'événements du SP local
/pstore/emstatefile	Journal d'événements du SP local
/pstore/hwinventory	Liste d'inventaire du matériel
/pstore/inv_manifests/*	Liste d'inventaire des logiciels
/pstore/snmpd.conf	ID unique du moteur SNMP
/pstore/sp_uuid	ID unique du SP
/pstore/ssh/ssh_host*	Clés d'hôte SSH
/pstore/IPMI/sdrr	Référentiel des données des capteurs IPMI
/pstore/IPMI/SEL	Journal d'événements des capteurs IPMI

Détermination des adresse MAC réseau du SP et de la plate-forme

Utilisez les commandes suivantes si vous devez déterminer l'adresse MAC du SP ou de la plate-forme de votre serveur :

```
# ssh adresseipsp -l nomutilisateursp sp get mac
```

```
# ssh adresseipsp -l nomutilisateursp platform get mac
```

Fonctions de la console Systems Management

Il est possible de géré le serveur en utilisant les commandes de la CLI ou l'interface graphique Systems Management (SM) Console. Cette section présente les opérations réalisables avec l'interface SM Console.

Remarque – Pour plus d'informations sur les commandes de la CLI, reportez-vous aux annexes de ce guide.

Configuration des paramètres réseau

Les utilisateurs de niveau gestionnaire et administrateur peuvent utiliser SM Console pour configurer les paramètres réseau du SP pour définir la méthode d'attribution des adresses IP (statique ou DHCP) et d'autres paramètres réseau tels que le nom de l'hôte, l'adresse du serveur DNS et les domaines.

Remarque – Comme examiné dans la section précédente, vous pouvez aussi configurer les paramètres réseau depuis le panneau de l'opérateur, ou utiliser les commandes `sp ip`, qui sont expliquées dans l'aide en ligne.

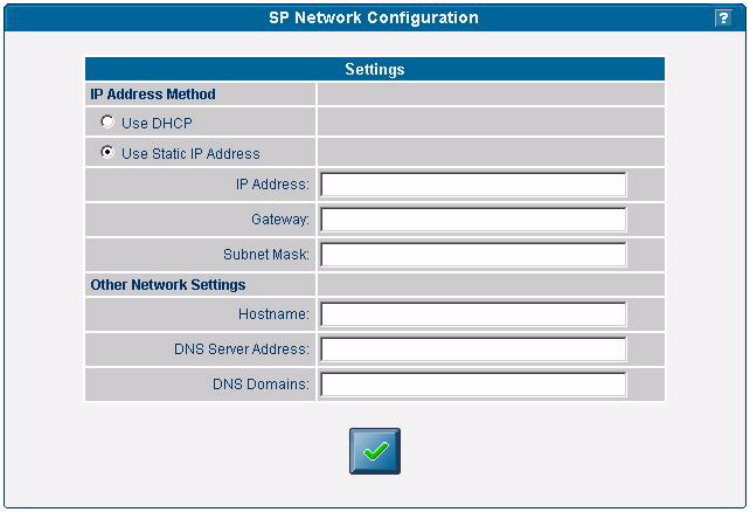


FIGURE 1-11 Configuration réseau

Pour configurer les paramètres réseau du SP depuis SM Console :

1. **Cliquez sur Configuration>SP Network dans la barre de menus.**
2. **Dans le tableau Settings, choisissez le bouton radio correspondant à la méthode d'attribution des adresses IP (DHCP ou Static IP Address) que vous voulez utiliser.**
3. **Si vous choisissez Static IP Address, tapez l'adresse IP, l'adresse de la passerelle et le masque de sous-réseau.**
4. **Identifiez d'autres paramètres réseau.**
   - le nom d'hôte du SP
   - une adresse IP unique de serveur DNS (s'il y en a un)
   - une liste aux éléments séparés par des espaces des domaines de recherche (le cas échéant)
5. **Cliquez sur le bouton à cocher pour enregistrer les paramètres.**

Remarque – Si vous choisissez DHCP, le SP recherche par diffusion un serveur DHCP pour obtenir une adresse IP dynamique. Les informations de l'adresse IP s'affichent mais il n'est pas possible de les éditer.

Démarrage et arrêt du SE de la plate-forme

es utilisateurs de niveaux gestionnaire et administrateur peuvent démarrer et arrêter le système d'exploitation de la plate-forme depuis SM Console. Choisissez Management>Platform Operations dans la barre de menus, puis choisissez l'une des options listées dans le tableau ci-dessous.

TABLEAU 1-7 Options d'arrêt et de redémarrage

Option	Description
Power On / Restart	L'option Power On/Restart démarre le système d'exploitation de la plate-forme.
	L'option Boot into BIOS Setup initialise la plate-forme et fait passer le BIOS en mode configuration. Vous pouvez ainsi modifier les paramètres du BIOS depuis la console de la plate-forme. Une fois cette option sélectionnée, vous devrez accéder à l'écran de configuration du BIOS pour changer les paramètres du BIOS. Pour plus de détails sur la configuration des paramètres du BIOS, reportez-vous au *Guide de l'utilisateur* de votre serveur. Pour l'accès à distance, connectez-vous via SM Console. Choisissez Troubleshooting>SP SSH Console. Exécutez ensuite la commande `platform console`.
	L'option Forced Restart saute la phase d'arrêt du système d'exploitation pendant le redémarrage du système. Elle peut entraîner la perte de données.
Shutdown / Power Off	L'option Shutdown/Power Off arrête le système d'exploitation de la plate-forme et met la machine hors tension.
	L'option Forced Power Off saute la phase d'arrêt du système d'exploitation. Elle peut entraîner la perte de données. Utilisez l'option Forced Power Off si vous devez imposer un arrêt.

Une fois que vous avez choisi une option et cliqué sur le bouton à cocher, l'opération est initialisée sur le serveur. Le texte d'aide affiche les messages relatifs au traitement et aux résultats. L'état courant est reflété dans le bouton System Status, ce qui vous permet de contrôler la progression.

Lorsque vous passez avec la souris sur le bouton Platform Operating System, l'un des états suivants s'affiche dans le panneau d'aide :

- Off
- On
- Communicating
- Diagnostics
- Sleeping
- BIOS booting
- BIOS setup
- OS booting
- OS shutting down

Remarque – Vous pouvez effectuer la gestion de l'état de la plate-forme depuis la ligne de commande avec les sous-commandes platform. Pour plus d'informations, reportez-vous à l'Annexe F de ce guide.

Si l'alimentation est déjà désactivée, l'option Shutdown/Power Off retourne un message indiquant que l'option n'a pas été exécutée à cause de l'état courant.

Configuration de la notification d'événements SMTP

Les utilisateurs de niveaux gestionnaire et administrateur peuvent configurer le système pour :

- Envoyer un e-mail pour les événements générés, via un serveur Simple Mail Transfer Protocol (SMTP).
- Acheminer un e-mail en fonction de la gravité des événements.
- Envoyer un e-mail contenant un objet et un contenu (format long) ou uniquement un objet (format court) pour prendre en charge des périphériques cibles tels que des téléphones, des pageurs, etc.

La notification SMTP assure une notification rapide des événements et une réponse rapide aux situations critiques. Vous pouvez utiliser SM Console ou les commandes `sp smtp` pour configurer la notification d'événements SMTP.

Suivez les étapes ci-après pour configurer les alertes SMTP automatiques via e-mail depuis SM Console :

1. **Cliquez sur Configuration>SMTP Event Notification dans la barre de menus.**
2. **Tapez le nom du serveur SMTP (au choix le nom d'hôte ou l'adresse IP du serveur SMTP auquel vous voulez que l'e-mail soit envoyé). Utilisez l'adresse IP à moins que DNS ne soit configuré sur le SP.**

3. **Pour chaque niveau de gravité, tapez une liste d'adresses e-mail séparées par des virgules. Ces adresses sont celles qui recevront un e-mail pour chaque niveau de gravité. Les niveaux de gravité sont les suivants :**
   - informationnel,
   - d'avertissement,
   - critique.

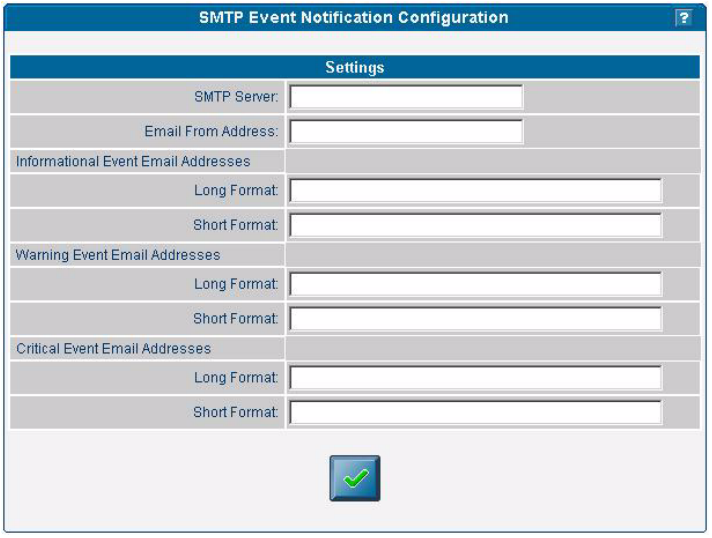


FIGURE 1-12 Notification d'événements SMTP

Remarque – Tapez des listes d'adresses distinctes pour les formats d'e-mail long et court. Mettez une virgule entre deux adresses e-mail consécutives. Tapez une liste distincte pour les adresses e-mail de pageurs qui requièrent le texte abrégé.

---

4. **Cliquez sur le bouton à cocher pour enregistrer les paramètres.**

Configuration des services d'annuaire

Configurez les options de services d'annuaire pour définir la façon dont sont stockées les informations de noms d'utilisateur et de mots de passe et celle dont on y accède.

TABLEAU 1-8 Options de services d'annuaire

Option	Description
NIS	Service d'information réseau : solution originaire d'UNIX pour service d'annuaire. Les fichiers locaux et un serveur NIS distant authentifient tous deux les utilisateurs.
ADS	Active Directory Service : service d'annuaire de Microsoft. Les fichiers locaux et un serveur ADS distant authentifient tous deux les utilisateurs.

Vous pouvez utiliser SM Console ou les sous-commandes `access` pour configurer les options de services d'annuaire. Pour plus d'informations, reportez-vous à l'Annexe B de ce guide.

Pour configurer les services d'annuaire depuis SM Console :

1. **Cliquez sur Access Control>Directory Services dans la barre de menu.**
2. **Si vous voulez utiliser uniquement l'authentification locale, sélectionnez le premier bouton radio du tableau Settings.**

   ou

   Si vous voulez utiliser les services d'annuaire, sélectionnez le bouton radio de la base de données de services d'annuaire à utiliser.

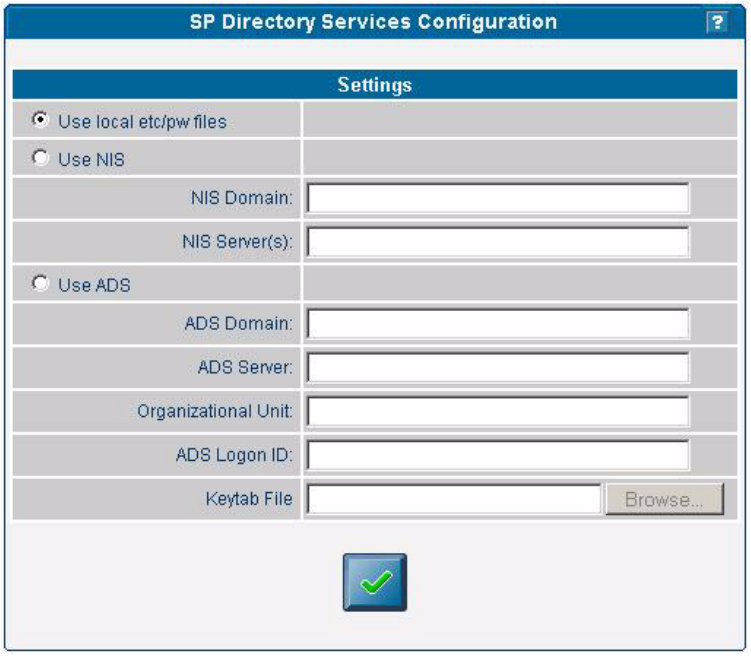


FIGURE 1-13 Configuration des services d'annuaire

3. **Tapez le nom du domaine pour l'option sélectionnée à l'étape 2.**
4. **Tapez le nom du serveur pour l'option sélectionnée à l'étape 2. (en cas de serveurs multiples, tapez une virgule entre deux noms de serveurs consécutifs).**
5. **Si vous aviez choisi ADS, tapez aussi l'unité organisationnelle, l'ID de connexion ADS et l'emplacement du fichier keytab (voir « Création des fichiers keytab pour ADS », page 56).**
6. **Cliquez sur le bouton à cocher pour enregistrer les paramètres.**

Remarque – Si vous utilisez ADS, l'horloge du processeur de service doit être synchronisée avec celle du serveur ADS. De même, le processeur de service et le serveur ADS doivent être à même de résoudre leurs noms d'hôtes respectifs en utilisant DNS.

Les utilisateurs à distance qui ont été authentifiés via les services d'annuaire ont accès au SP uniquement via un mappage de groupe qui mappe le groupe distant de l'utilisateur à un groupe administratif du SP.

Pour simplifier la configuration sur le SP, les utilisateurs de niveau gestionnaire peuvent mapper les groupes de service d'annuaire à des groupes prédéfinis. Lorsque vous mappez ces utilisateurs (membres de groupes de services d'annuaire) à un groupe administratif de SP , ceux-ci se voient automatiquement attribuer des droits d'accès appropriés.

Mappage de groupes de services d'annuaire

Le tableau Mappage de groupes de services d'annuaire identifie les mappages de groupes existants. Ce tableau indique aussi des options pour le mappage d'autres groupes de services d'annuaire à un groupe SP. Par exemple, si le groupe Directory Services 5 est mappé au gestionnaire, tous les membres de ce groupe se verront attribuer des privilèges de niveau gestionnaire sur le SP.

Pour mapper les groupes de services d'annuaire depuis SM Console :

1. **Cliquez sur Access Control>DS Group Mappings dans la barre de menu.**

   Le tableau des mappages de groupes courants s'affiche. Les groupes de services d'annuaire sont listés par ordre alphabétique.

FIGURE 1-14 Mappages des groupes de services d'annuaire

2. **Choisissez une des options suivantes :**
   - Sélectionnez le bouton radio correspondant au mappage que vous voulez créer (monitor, admin, manager).
   - Sélectionnez No Mapping pour désactiver l'accès au SP.
   - Entrez un nouveau groupe dans le champ de texte et sélectionnez une des options à bouton radio pour indiquer le groupe de SP requis pour cette nouvelle entrée.
   - Sélectionnez la case à cocher Verify de sorte qu'une erreur s'affiche si le nom d'un nouveau groupe ne figure pas dans le service d'annuaire.
3. **Cliquez sur le bouton à cocher.**

Création des fichiers keytab pour ADS

Pour utiliser ADS en tant que service d'annuaire sur le SP, vous devez créer un compte d'annuaire actif. La *bibliothèque du service d'attribution de noms* sur le SP utilise ce compte pour s'authentifier auprès de l'interface LDAP du serveur d'annuaire actif.

Exigences du serveur ADS

- Les Certificate Services et le High Encryption Pack doivent être installés sur le serveur ADS.
- L'administrateur Windows doit créer un compte Active Directory et un keytab (pour ce compte) que le ou les SP utiliseront pour mener des requêtes LDAP. Vous pouvez créer des fichiers keytab avec la commande `ktpass` qui se trouve dans le kit de ressources de Microsoft Windows 2000 :

```
ktpass -princ <connexion>@<domaine> -pass <motpasse> -mapuser
<connexion> -out <nomfichier sortie>
```

Remarque – Le fichier keytab créé avec cette commande peut être téléchargé sur le SP avec la commande `scp` ou être accédé depuis un système de fichiers exporté monté par le SP.
Pour plus de détails sur cette commande, reportez-vous à votre documentation Microsoft.

Exigences du SP ADS

- Vous devez configurer DNS.
  - Le nom canonique de chaque hôte doit être son nom d'hôte complet (domaine inclus).
  - L'adresse IP de chaque hôte soit permettre de retrouver le nom canonique.
- L'heure du SP ne peut pas être décalée de plus de cinq minutes de celle du serveur ADS (contrôleur du domaine). Au démarrage de la plate-forme, l'horloge du SP se synchronise sur celle de la plate-forme.
- Vous devez configurer correctement l'ADS. Depuis SM Console, tapez :
  - le domaine ADS,
  - le nom du serveur ADS,
  - l'unité organisationnelle sous laquelle le SP recherche des informations de groupe.
  - l'ID de connexion ADS (le nom du compte qui a été créé pour que le SP l'utilise),
  - le fichier keytab qui a été téléchargé et installé sur le SP.

Configuration de la date et de l'heure

Les utilisateurs de niveaux administrateur et gestionnaire peuvent configurer les paramètres de date et d'heure pour l'horloge du SP. Utilisez la commande `sp date` depuis la ligne de commande ou configure la date et l'heure depuis SM Console.

- L'horloge est automatiquement synchronisée lors de l'installation des pilotes de la plate-forme. Si la plate-forme est en cours d'exécution (et que les pilotes sont installés), l'heure de la plate-forme prime sur celle du SP.
- L'heure de la plate-forme doit être correctement réglée pour que ADS fonctionne.

Si vous configurez le SP avant de charger le système d'exploitation d ela plate-forme et voulez régler l'heure pour la synchroniser avec ADS et d'autres services du réseau, suivez la procédure ci-après.

Depuis SM Console :

1. **Cliquez sur Configuration>SP Date/Time dans la barre de menus.**
2. **Identifiez la date et l'heure sur l'horloge du SP.**

   L'heure courante du SP s'affiche dans le format `aaaa:mm:jj hh:mm:ss`. la FIGURE 1-15 illustre un exemple de ce format.

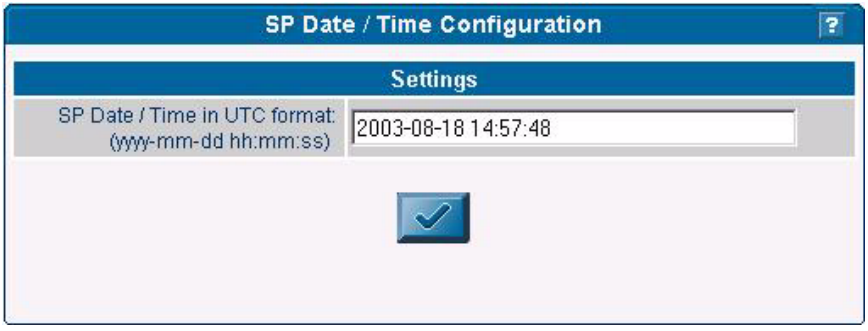


FIGURE 1-15 Configuration de la date et de l'heure

3. **Cliquez sur le bouton à cocher pour enregistrer les paramètres.**

Configuration de SSL

Configurez l'accès Web au SP avec au choix une méthode de communication chiffrée ou non-chiffrée.

Par défaut, tous les messages entre votre navigateur et le SP sont chiffrés selon Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). La version 0.9.6j est prise en charge.

1. **Permettez aux navigateurs de communiquer avec le SP au moyen de messages non-chiffrés par l'une des deux méthodes suivantes :**

   - Depuis la ligne de commande, utilisez la commande suivante :

     ```
     sp disable ssl-required
     ```

   - Depuis SM Console, sélectionnez les boutons radio Optional (disable) ou Required (enable) sur la page de configuration du certificat SSL comme décrit dans « Configuration du certificat SSL depuis SM Console », page 59.

     SSL étant désactivé, les requêtes HTTP sont servies directement sans être redirigées sur HTTPS. Les requêtes HTTPS continuent à être sécurisées.

Remarque – Si vous activez le protocole HTTPS, votre navigateur affichera un message d'avertissement qui indique qu'il ne peut pas vérifier la validité du certificat du serveur. Cet avertissement est donné à simple titre d'information et vous pouvez l'ignorer sans risque. Cet avertissement s'affiche car le certificat du serveur qui est envoyé avec le SP est auto-signé par Newisys, Inc. Pour télécharger un certificat qui soit signé par votre propre entreprise ou par une autorité de certification indépendante, sélectionnez User Supplied comme décrit dans « Configuration du certificat SSL depuis SM Console », page 59.

---

2. **Pour revenir au comportement par défaut, utilisez la commande suivante :**

   ```
   sp enable ssl-required
   ```

   Avec SSL activé, les requête HTTP sont automatiquement redirigées sur des requêtes HTTPS équivalentes pour maintenir la sécurité du site.

Configuration du certificat SSL depuis SM Console

Les utilisateurs de niveaux administrateur et gestionnaire peuvent activer ou désactiver le chiffrement SSL et peuvent définir le certificat SSL utilisé pour gérer la sécurité de la transmission.

Remarque – Vous pouvez aussi utiliser les commandes `sp ssl` pour configurer le certificat SSL. Pour plus de détails sur les commandes, reportez-vous à l'annexe H de ce document ou à l'aide en ligne de SM Console.

Suivez les étapes ci-après pour configurer le certificat SSL depuis SM Console :

1. **Cliquez sur Configuration>SSL Certificate dans la barre de menus.**
2. **Sélectionnez le bouton radio pour désigner l'accès SSL comme requis ou optionnel.**

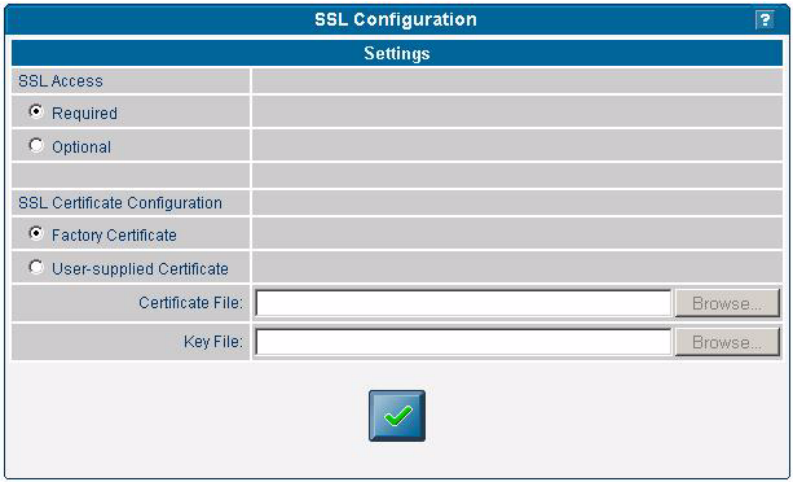


FIGURE 1-16 Configuration SSL

3. **Effectuez l'une des opérations suivantes selon votre choix : Required (requis) ou Optional (optionnel) :**
   - Si vous avez sélectionné Required, sélectionnez le bouton radio correspondant au type de configuration de certificat SSL que vous voulez utiliser : une gestion de la certification installée en usine ou maison.
   - Si vous avez sélectionné User-supplied :

   a. **Entrez le nom du fichier de certificat généré à installer avec Apache sur le SP ou cliquez sur le bouton Browse pour rechercher un fichier.**

   b. **Entrez le nom du fichier de clé généré à installer avec Apache sur le SP ou cliquez sur le bouton Browse pour rechercher un fichier.**

4. **Cliquez sur le bouton à cocher.**

Contrôle du statut du système

La fenêtre System Status affiche une image qui représente la disposition physique et le statut de l'ensemble des composants matériels et des capteurs. Vous pouvez utiliser cette fenêtre pour identifier les composants qui ont des problèmes ou les composants en panne à remplacer. Pour accéder à cette fenêtre, cliquez sur le bouton System Status depuis la barre d'outils dans SM Console.

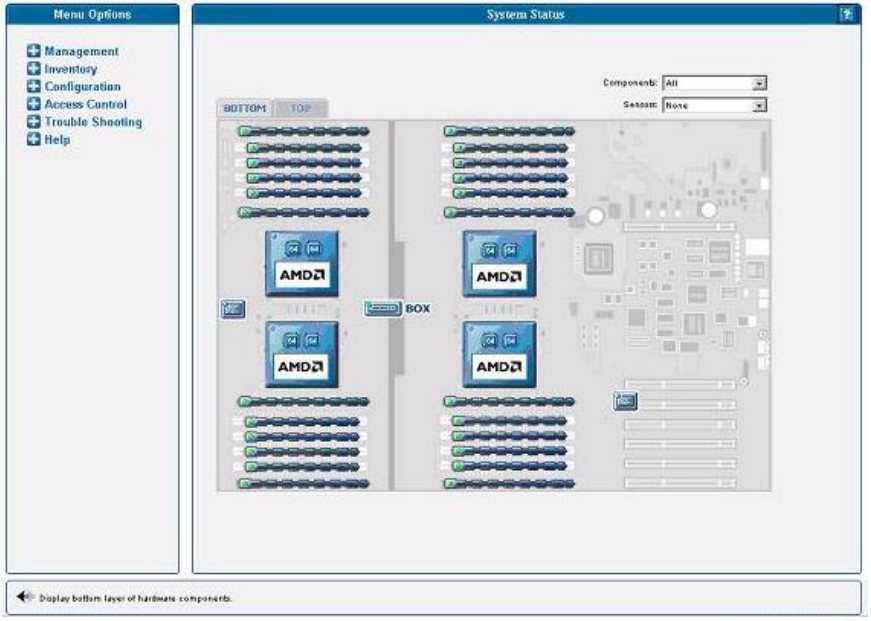


FIGURE 1-17 System Status, onglet Bottom, serveur Sun Fire V40z

Les images des composants représentent les composants matériels physiques et en incluent l'emplacement approximatif, la taille et le statut. La disposition du matériel d'un serveur Sun Fire V40z est représentée par deux couches (la FIGURE 1-17 est la vue de l'onglet Bottom par défaut d'un serveur Sun Fire V40z bicœur). Cliquez sur les onglets Bottom et Top dans le haut de l'image pour changer de vue.

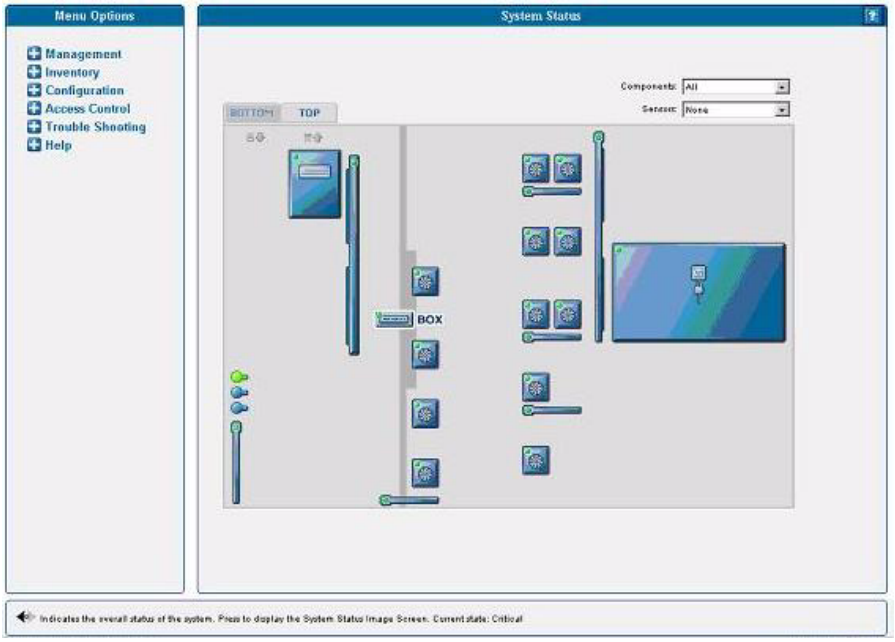


FIGURE 1-18 System Status, onglet Top, serveur Sun Fire V40z

Vous pouvez aussi afficher les détails d'un composant à des fins de dépannage. Pour ce faire, cliquez sur son image. Vous pouvez aussi utiliser les menus déroulants du coin supérieur droit de l'image pour localiser des types de composants spécifiques (unités de CD-ROM, CPU, unités de disque, ventilateurs, etc.) et des types de capteurs spécifiques (capteurs des ventilateurs et des alimentations, capteurs de température).

Les images des capteurs indiquent l'emplacement approximatif, la valeur courante et les seuils d'avertissement ou critique des capteurs et sondes du système. Les informations courantes sur le capteur (nom, type, valeur courante, seuils d'avertissement inférieur et supérieur, seuils critiques et statut) s'affichent dans un composant indicateur dans le coin supérieur droit de l'image.

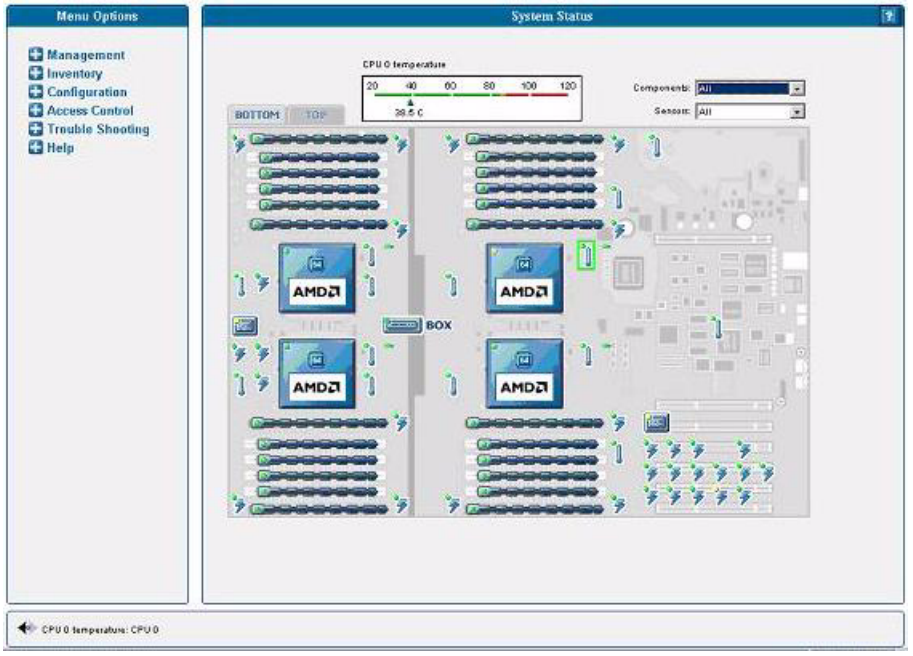


FIGURE 1-19 Capteurs de température affichées dans la couche du bas

Pour afficher les valeurs d'une sonde, cliquez sur son image. L'indicateur du capteur de température de CPU0 s'affiche dans la FIGURE 1-19, qui illustre la couche du bas.

FIGURE 1-20 Indicateur de la température de l'air ambiant, couche supérieure

L'indicateur du capteur de température de l'air ambiant s'affiche dans la FIGURE 1-20, qui illustre la couche supérieure.

Remarque – Pour des instructions supplémentaires et des détails sur les tâches de gestion, reportez-vous à l'aide en ligne de SM Console.

Événements système

Les administrateurs ayant des privilèges appropriés peuvent utiliser le tableau System Events de SM Console pour afficher des informations détaillées sur tous les événements actifs. Ils peuvent aussi effectuer diverses actions liées aux différents événements.

Chaque événement actif s'affiche sur une ligne propre du tableau, comme illustré dans la FIGURE 1-21 ci-dessous.

FIGURE 1-21 Table Événements système

Le TABLEAU 1-9 décrit les colonnes du tableau System Events.

TABLEAU 1-9 System Events, Tableau

Colonne	Description
Component	Nom unique du composant à l'origine de cet événement. Les composants peuvent être matériels ou logiciels.
Detail	Affiche les détails du composant.
ID	Contient un ID d'événement unique pour chaque événement vous permettant de suivre cet événement dans votre système de panne externe et d'interroger les fichiers journaux pour obtenir toutes les actions liées à l'événement.
All	Affiche la plus haut gravité jamais atteinte par cet événement : icônes informationnelle (verte), d'avertissement (jaune), critique (rouge). Cliquez sur l'icône pour afficher les détails pour l'événement.
Current	Affiche la gravité courante (icônes informationnelle (verte), d'avertissement (jaune), critique (rouge) et un message descriptif. Ces descriptions peuvent être longues (et décrire par exemple les températures nominale, d'avertissement, critique et courante d'un ventilateur), cas dans lequel elles s'afficheront dans le panneau d'aide.
Type	Identifie le type de l'événement. Pour la description des icônes représentant les différents types, reportez-vous au TABLEAU 1-10.
First	Liste la date et l'heure auxquelles l'événement a été généré initialement. Seule l'heure s'affiche dans le tableau ; le texte d'aide dans le bas de la fenêtre affiche l'intégralité de la date et de l'heure.
Last	Date et heure de la dernière génération de l'événement. Seule l'heure s'affiche dans le tableau ; le texte d'aide dans le bas de la fenêtre affiche l'intégralité de la date et de l'heure.
Count	Liste le nombre de fois où l'événement est survenu. Si un nouvel événement a le même composant et le même type d'événement d'un événement courant non-effacé, aucun nouvel événement n'est créé mais le nombre de l'événement courant est mis à jour dans la colonne Current.
Clear	Cliquer sur ce bouton efface l'événement. Vous devez effacer manuellement tous les événements. Tout événement effacé est supprimé du serveur et automatiquement effacé de tout autre écran SM Console System Events connecté. Seuls les utilisateurs de niveau administrateur ou gestionnaire peuvent effacer des événements.

Remarque – Vous pouvez aussi utiliser la commande `sp get events` pour obtenir des informations sur les événements. Pour plus d'informations sur cette commande, reportez-vous à l'annexe H de ce document ou à l'aide en ligne.

Icônes des types d'événements

SM Console affiche les icônes illustrées dans le Tableau 1-10 pour représenter des types d'événements spécifiques.

TABLEAU 1-10 Icônes des types d'événements

Type d'événement	Icône
Événements relatifs au BIOS	
Événements relatifs à la vitesse des ventilateurs	
Événements relatifs au contrôle machine	
Événements divers relatifs au système d'exploitation	
Événements relatifs à l'état de la plate-forme	
Événements relatifs à l'interrupteur	
Événements relatifs à la température	
Événement inconnu	
Événements relatifs à la tension	

Remarque – Pour le tableau des événements système et des suggestions de dépannage, reportez-vous au *Serveurs Sun Fire V20z et Sun Fire V40z - Guide des techniques de dépannage et de diagnostic* 819-2924-12.

CHAPITRE 2

Gestion de serveurs IPMI

Les fabricants de serveurs d'aujourd'hui sont sans cesse amenés à revoir la façon dont se gère chaque nouveau serveur. La conception matérielle et logicielle d'un serveur ne fonctionne pas nécessairement avec un autre serveur. Chaque fournisseur de serveurs fournit des fonctions de contrôle et de recueil de données de base mais ils ne sont pas deux à le faire de la même façon. Ces implémentations propriétaires ne font que compliquer les choses.

Interface de gestion de plate-forme intelligente

La standardisation de la gestion basée sur le serveur ou IPMI (*Intelligent Platform Management Interface*, Interface de gestion de plate-forme intelligente), constitue une solution intéressante. IPMI vous permet d'interconnecter la CPU et les périphériques gérés. Elle permet :

- une réplication aisée des fonctions de contrôle d'un serveur à l'autre,
- la prise en charge d'un nombre relativement important de périphériques de contrôle,
- un accès de niveau pilote courant aux instruments de gestion,
- des implémentations plus efficaces en terme de coûts,
- une évolutivité accrue des fonctions de gestion de serveurs.

IPMI est une interface de gestion de matériel standard de l'industrie, qui fournit une architecture définissant la façon dont des périphériques uniques peuvent tous communiquer avec la CPU de façon standard. Elle facilite la gestion du serveur côté plate-forme et les structures de gestion de serveurs à distance, en fournissant un jeu d'interfaces standard pour le contrôle et la gestion des serveurs.

Avec IPMI, le logiciel devient moins dépendant du matériel car l'intelligence de gestion réside dans la couche du microprogramme IPMI, ce qui crée un serveur géré de façon plus intelligente. La solution IPMI augmente l'évolutivité du serveur en distribuant l'intelligence de gestion plus près des périphériques gérés.

Contrôleur de gestion de carte de base

Pour pouvoir effectuer des fonctions de gestion de plate-forme autonomes, le processeur exécute un logiciel ou un microprogramme imbriqué. Ensemble, le processeur et son microprogramme de contrôle sont connus sous le nom de BMC *(Baseboard Management Controller)*, et constituent le noyau de la structure IPMI. Intégrer étroitement un BMC IPMI et le logiciel de gestion avec le microprogramme de la plate-forme fournit une solution de gestion complète.

Remarque – Une autre façon d'effectuer des interrogations et des actions IPMI sur le BMC consiste à utiliser l'utilitaire client IPMI `ipmitool`, qui est considérablement utilisé pendant le processus de test. Pour plus d'informations, voir « Lights Out Management (LOM) », page 78.

Le BMC est un processeur de service intégré à la conception de la carte mère, qui constitue une solution de gestion indépendante du processeur principal. Le serveur contrôlé communique avec le BMC au travers de l'une des trois interfaces définies, qui sont basées sur un ensemble de registres partagés entre la plate-forme et le BMC.

Remarque – Dans ces serveurs, le SP a un logiciel qui émule un BMC.

Le BMC est responsables des tâches/éléments suivants :

- gérer l'interface entre le logiciel de gestion de serveur et le matériel de gestion de la plate-forme,
- l'interface avec les capteurs du système, tels que ceux contrôlant la vitesse des ventilateurs et la tension,
- fournir un accès au journal d'événements du système,
- assurer un contrôle autonome du contrôle, de l'enregistrement des événements dans un journal et de la reprise,
- faire office de passerelle entre le logiciel de gestion et l'IPMB/ICMB,
- contrôler l'horloge de surveillance,
- faciliter les tâches de gestion à distance, même lorsque le matériel du serveur principal est dans un état non-opérationnel.

Le BMC fournit l'intelligence qui se cache derrière l'IPMI. Dans ces serveurs, le SP sert de BMC et fournit l'accès aux données et événements relatifs aux capteurs au travers des interfaces IPMI standard.

Facilité de gestion

IPMI définit un mécanisme de contrôle du serveur et de reprise qui est implémenté directement dans le matériel et le microprogramme. Les fonctions IPMI sont disponibles indépendamment des processeurs principaux, du BIOS et du système d'exploitation.

Les fonctions de contrôle, de journalisation et d'accès d'IPMI ajoutent un niveau intégré de gestion au matériel de la plate-forme. IPMI peut être utilisée conjointement avec le logiciel de gestion de serveurs s'exécutant sous le SE, ce qui offre un niveau de gestion amélioré.

IPMI fournit la base d'une gestion plus intelligente des serveurs en fournissant une méthodologie permettant de maintenir et d'améliorer la fiabilité, la disponibilité et l'entretien du matériel serveur coûteux.

Présentation fonctionnelle

La liste suivante détaille les principales caractéristiques d'IPMI dans les serveurs :

- Un SDDR (Sensor Data Record Repository, référentiel d'enregistrement des données des capteurs) est le conteneur dans lequel vous stockez les enregistrements SDR (Sensor Data Record, enregistrement des données des capteurs) et l'interface qui vous permet d'accéder à ces SDR.

  Le BMC est le propriétaire de tous les capteurs inclus dans le référentiel. Les fonctions SDRR sont les suivantes :

  - Un enregistrement de contrôleur de gestion unique,
  - Des capteurs analogiques basés sur des seuils pour la température, la tension, les ventilateurs et l'alimentation,
  - Des enregistrements de localisateur de périphérique pour les FRU, auxquels les enregistrements des capteurs physiques sont reliés (au travers de relations ID d'entité/instance),
  - Différents capteurs discrets et capteurs de type événement uniquement.
- Le System Event Log (SEL) est un fichier persistant de 16K maximum. Pour plus d'informations, voir « Journal d'événements système », page 72.
- L'horloge de surveillance (WDT) prend en charge toutes les utilisations de l'horloge, pas d'actions d'interruption de pré-temporisation et toutes les actions de temporisation (réinitialisation, mise hors tension et cycle d'alimentation). Pour plus d'informations, voir « Horloges de surveillance », page 77.
- Une FRU est de type lecture seule. Elle est étroitement intégrée aux fonctions de gestion d'inventaire du SP. Pour plus d'informations sur les commandes d'inventaire, voir l'annexe D de ce guide. Les données VPD qui sont disponibles par le biais de la commande d'inventaire le sont aussi depuis la FRU.

- Les actions de contrôle du châssis suivantes sont disponibles :
  - Mise hors tension
  - Mise sous tension
  - un cycle d'alimentation,
  - Réinitialisation matérielle
  - Arrêt logiciel
- Les alertes de filtrage d'événements et PET *(Platform Event Trap)* non-reconnues sont prises en charge. Pour plus d'informations, voir « Filtres d'événements », page 76.
- Les canaux SMS et LAN sont tous deux pris en charge. Voir « Conformité à IPMI et accès au canal LAN », page 70.
- Serial Over LAN (SOL) assure la redirection du port série sur le canal LAN. Voir « Serial Over LAN », page 122.

Conformité à IPMI et accès au canal LAN

Le serveur prend en charge IPMI avec les deux canaux SMS et LAN sur la version 2.2 et les versions ultérieures du logiciel du SP. Ces serveurs satisfont les standards de conformité d'IPMI version 2.

Le SMS est implémenté comme une interface KCS *(Keyboard Controller Style)*.

L'implémentation IPMI sur ces serveurs peut également prendre en charge l'accès par le canal LAN (pour plus de détails, voir la spécification IPMI v2). Par défaut, l'accès par le canal LAN est désactivé. Pour l'activer, utilisez la commande `ipmi enable channel` et indiquez l'ID du canal pour activer l'interface LAN, comme suit.

Remarque – L'ID est sensible à la casse et doit être indiqué en lettres minuscules.

```
# ssh adripsp -l utilisateursp ipmi enable channel {sms | lan}
```

Dans le cadre de cette commande, vous pouvez également spécifier le mot de passe de l'utilisateur par défaut *null*. L'utilisateur *null* peut ensuite utiliser IPMI sur l'interface LAN. Pour plus d'informations, voir « Noms d'utilisateur et mots de passe », page 71.

Pour plus d'informations sur l'activation et la désactivation du canal IPMI, voir l'Annexe E.

Noms d'utilisateur et mots de passe

L'accès de niveau opérateur et administrateur sur le canal LAN requiert un ID d'utilisateur et un mot de passe valides. Ces serveurs ne sont pas pré-configurés avec les comptes d'utilisateur activés. Lorsque vous activez au départ le canal LAN au moyen de la commande `ipmi enable channel`, il vous est demandé d'indiquer le mot de passe de l'utilisateur null. Voir « Conformité à IPMI et accès au canal LAN », page 70.

Remarque – Pour des raisons de sécurité, l'accès par le canal LAN est désactivé par défaut.

Remarque – Les identités d'utilisateur IPMI ne sont en aucune façon associées à des comptes d'utilisateur définis pour les fonctions de gestion de serveurs. Pour plus d'informations sur les comptes d'utilisateur de gestion de serveurs, voir « Configuration initiale du SP », page 14.

Prise en charge des options d'initialisation du serveur

IPMI vous permet de définir un certain nombre d'options d'initialisation qui seront interprétées par le BIOS. Le TABLEAU 2-1 contient des informations importantes sur les options d'initialisation du serveur et les paramètres pris en charge par le BIOS.

TABLEAU 2-1 Options d'initialisation

Paramètre	Numéro	Détails
`Set In Progress`	0	Ce paramètre est entièrement pris en charge à l'exception de la fonction d'annulation
`BMC boot flag valid bit clearing`	3	Entièrement pris en charge.
`Boot info ack`	4	Prises en charge du BIOS indiquant qu'il a géré les informations d'initialisation.
`Boot Flags`	5	• L'octet de données 1 est pris en charge pour le bit `boot flags valid`. • L'octet de données 2 (CMOS Clear) est pris en charge ; toutefois, quand ce bit est défini, tous les autres bits de cet octet sont ignorés. • Le verrouillage du clavier est entièrement pris en charge. • Le sélecteur du périphérique d'initialisation est pris en charge à l'exception de l'initialisation en BIOS Setup. • L'octet de données 3 est pris en charge pour `user password bypass`

Journal d'événements système

Le journal d'événements système (SEL, System Event Log) fait partie du BMC. Plusieurs types d'informations sont consignés dans le SEL, des messages administratifs à des messages indiquant des événements importants tels que le dépassement des seuils des capteurs.

La taille du journal est de 16 Mo, ce qui permet 1024 enregistrements.

Capteurs

Les capteurs génèrent des événements, recueillent des relevés et définissent des seuils. Le SDRR contient plusieurs types de capteurs.

Vous pouvez accéder à tous les capteurs par le biais du BMC. De nombreux capteurs représentent des capteurs physiques qui sont répartis sur la carte mère et contenus dans les FRU. Ces capteurs sont interrogés. Lorsqu'un seuil est dépassé, une entrée est ajoutée au SEL.

Pour plus d'informations sur les commandes des capteurs, voir l'annexe G de ce guide.

Détermination de la présence des capteurs

Pour déterminer la présence d'un capteur, exécutez la sous-commande `sensor get`.

Un capteur qui est hors ligne (ne rapporte rien) ou qui est physiquement absent du système est indiqué par l'état `unavailable` dans les données de réponse.

Seuils des capteurs

Pour récupérer les seuils des capteurs, exécutez la sous-commande `sensor get`.

Pour définir les seuils des capteurs, exécutez la sous-commande `sensor set`.

Si vous ne spécifiez aucun seuil, le résultat n'indique aucun changement et le code retourné est `success`.

Le TABLEAU 2-2 liste les codes de réalisation qui sont retournés par la sous-commande `set sensor`.

TABLEAU 2-2 Codes de réalisation

Code	Cause
`0x00 (succès)`	Les seuils des capteurs sont définis comme demandé.
`0xCD (commande non-admise)`	Les seuils des capteurs ne peuvent pas être modifiés.
`0xCC (requête incorrecte)`	Tenter de définir un seuil qui ne peut pas l'être ou de définir des seuils dans un ordre inapproprié (par exemple, si vous mettez le seuil critique supérieur sur une valeur inférieure à celle du seuil non-critique supérieur).
`0xC0 (nœud occupé)`	Les ressources de traitement sont temporairement indisponibles.

Capteurs de température

Les lectures des capteurs de température sont définies dans une plage de 0 ˚C à 150 ˚C, soit 151 ˚C de différence. Le déclenchement thermique pour température de mort de la CPU se produit à environ 140 ˚C.

Les capteurs de tension peuvent générer les événements SEL suivants :

- Upper Critical Moving Higher Assertion
- Upper Critical Moving Higher De-assertion
- Upper Non-critical Moving Higher Assertion
- Upper Non-critical Moving Higher De-assertion

Capteurs de mémoire pour DIMM

Chaque DIMM a son propre enregistrement, qui est uniquement utilisé pour enregistrer les événements IPMI.

Pour plus d'informations, voir « Analyse des événements » dans le *Serveurs Sun Fire V20z et Sun Fire V40z — Guide des techniques de dépannage et de diagnostic*, (819-2924-12).

Capteurs de tension

Toutes les lectures des capteurs de tension sont indiquées en volts (V).
Le changement de tension maximal mesuré est de 15 V (la plage des capteurs de tension va de 0 à 15 V). De nombreux capteurs de tension ont des maximum bien plus bas et des plages bien plus limitées. Les capteurs de tension peuvent générer les événements SEL suivants :

- Upper Critical Moving Higher Assertion
- Upper Critical Moving Higher De-assertion
- Lower Critical Moving Lower Assertion
- Lower Critical Moving Lower De-assertion

Capteurs des ventilateurs

Les valeurs rapportées pour tous les capteurs de vitesse des ventilateurs sont indiquées en tours par minute (tr/min). Les capteurs ont une limite supérieure de 15 000 tr/min.

Les capteurs des ventilateurs peuvent générer les événements SEL suivants :

- Lower Critical Moving Lower Assertion
- Lower Critical Moving Lower De-assertion

Capteurs des alimentations

Toutes les lectures des capteurs des alimentations sont indiquées en watts (W) et définies dans une plage qui va de 0 à 600 W.

- Les capteurs des alimentations ne génèrent pas d'événements SEL.
- Il n'y a pas de seuils pour ces capteurs.

Contrôleurs de gestion

Un capteur de contrôleur de gestion représente le BMC. Le contrôleur de gestion a les fonctions suivantes :

- **Initialisation globale.** L'agent `init` permet au contrôleur de générer des messages.
- **Fonctions de périphériques.** Ce périphérique effectue toutes les fonctions suivantes :
  - périphérique châssis,
  - récepteur d'événements IPMB,
  - périphérique d'inventaire des FRU,
  - périphérique SEL,
  - périphérique référentiel SDR,
  - périphérique capteur.

Capteurs variés

Les capteurs supplémentaires suivants sont également prises en charge :

- System Event
- Event Logging Disabled
- System Firmware Progress
- Watchdog

System Event

Le capteur événement système indique toute une variété d'événements du système. Aucune condition d'événement n'est cependant reflétée de la sous-commande `sensor get`.

PEF actions. Des actions en attente à l'encontre d'un filtre avec lequel une correspondance a été établie sont consignées si le capteur d'événement a été configuré pour le faire. Seules les assertions de conditions d'action PEF en attente sont consignées.

```
Sensor Type Code: 0x12 [System Event]
Sensor Specific Offset: 0x04 [PEF Action]
```

Time sync. Les événements de synchronisation surviennent par paires : le premier précède une synchronisation SEL et le second la suit.

```
Sensor Type Code: 0x12 [System Event]
Sensor Specific Offset: 0x05 [Time sync]
```

Event Logging Disabled

Le capteur `event logging disabled` indique certains événements relatifs à SEL. Ce capteur est représenté comme un enregistrement SDR de « type 2 ».

SEL Full. Lorsque SEL atteint le nombre « maximum-1 » d'enregistrements, un enregistrement est consigné et toutes les commandes `add SEL` successives retournent un code indiquant que la limite a été dépassée. Cet enregistrement devient le dernier enregistrement du SEL lorsque celui-ci est plein.

```
Sensor Type Code: 0x10
Sensor Specific Offset: 0x04 [Log Full]
```

SEL Clear. Un enregistrement est écrit dans le SEL à chaque fois que la commande `Clear SEL` est exécutée. Cela ne se produit que sur la commande `Clear SEL` ; pas si vous supprimez la dernière entrée SEL avec la commande `Delete SEL Entry`.

```
Sensor Type Code: 0x10
Sensor Specific Offset: 0x02 [Log AreaReset/Cleared]
```

System Firmware Progress

Le capteur de progression du microprogramme du système est un capteur de type événement uniquement. L'entrée BIOS Boot Success SEL peut être consignée pour ce capteur lorsque le BIOS s'est initialisé avec succès et à tenté de rendre le contrôle SE ou si le BIOS a été initialisé et que vous êtes entré dans un écran de BIOS Setup.

```
Sensor Type Code: 0x0F
Sensor Specific Offset: 0x02 [Firmware Progress]
Event Data 2: 0x13 [Starting operating system boot process]
```

Watchdog

Le capteur `Watchdog 2` est utilisée pour consigner les événements d'expiration de l'horloge de surveillance. Ces événements ne sont générés que pour les horloges dont le bit « do not log » n'est pas défini. Un événement d'expiration d'horloge est consigné lorsqu'une horloge de watchdog expire.

```
Sensor Type Code: 0x23
Sensor Specific Offset: * all supported actions
```

Filtres d'événements

Remarque – Pour assurer un arrêt progressif, les pilotes de plate-forme appropriés doivent être installés sur le serveur.

Platform Event Filtering (PEF) fournit une gestion stratégique qui permet au BMC d'agir en présence d'événements particuliers. Les actions prises en charge par le biais de PEF sont les suivantes :

- Mise hors tension
- un cycle d'alimentation
- une réinitialisation
- l'envoi d'une alerte

Le TABLEAU 2-3 liste les filtres d'événements qui sont activés par défaut.

TABLEAU 2-3 Filtres d'événements activés par défaut

Correspondance	Action
`ambienttemp asserts upper critical threshold`	Mise hors tension
`cpu0.dietemp asserts upper critical threshold`	Mise hors tension progressive
`cpu1.dietemp asserts upper critical threshold`	Mise hors tension progressive

TABLEAU 2-3 Filtres d'événements activés par défaut *(suite)*

Correspondance	Action
`cpu2.dietemp asserts upper critical threshold` ***Remarque -*** *Ce filtre est ignoré sur les systèmes à deux CPU.*	Mise hors tension progressive
`cpu3.dietemp asserts upper critical threshold` ***Remarque -*** *Ce filtre est ignoré sur les systèmes à deux CPU.*	Mise hors tension progressive

Horloges de surveillance

Une horloge de surveillance permet l'exécution d'une action sélectionnée à l'expiration de l'horloge.

Pour les actions d'horloge, les interruptions de pré-temporisation ne sont pas prises en charge actuellement. Les actions suivantes sont prises en charge :

- la réinitialisation du système
- la mise hors tension du système
- un cycle d'alimentation du serveur

Alertes

Lorsque vous utilisez les alertes LAN PET (Platform-Event-Trap), le nombre des destinataires des alertes est limité à 16 (une destination non-volatile, quinze destinations volatiles). Le nombre des stratégies d'alerte est limité à 32.

Remarque – Les accusés de réception des alertes LAN PET et les chaînes d'alerte ne sont pas pris en charge.

Détermination du jeu de stratégies d'alerte

En cas de correspondance avec les filtres d'événements, les opérations suivantes se produisent :

- Toutes les actions qui ne sont pas des alertes sont balayées pour les filtres ;
- L'action associée à tous les fichiers ayant la priorité la plus élevée est prise ;
- Toutes les actions d'alerte sont balayées pour les filtres ;
- Le jeu de stratégies d'alerte ayant la priorité la plus élevée (sur la base du nombre de stratégies numérique le plus bas) est choisi.

Vous pouvez configurer les stratégies de sorte que, si l'alerte précédente a réussi, aucune alarme ne soit envoyée en tant que résultat de l'exécution de la stratégie d'alerte.

Lights Out Management (LOM)

Sur ces serveurs, la gestion Lights Out Management s'effectue par le biais d'IPMItool, utilitaire permettant de contrôler les périphériques compatibles IPMI.

Description

IPMItool est une interface de ligne de commande (CLI) avec les serveurs simple qui prend en charge la spécification Intelligent Platform Management Interface (IPMI) v1.5. Il permet de :

- Lire les SDR et imprimer les valeurs des capteurs ;
- Afficher le contenu du journal d'événements système (SEL) ;
- Imprimer des informations sur les FRU ;
- Lire et définir les paramètres de configuration du LAN ;
- Contrôler l'alimentation du châssis.

Écrit à l'origine pour exploiter les interfaces IPMI-sur-LAN, IPMItool est également en mesure d'utiliser une interface système, telle que fournie par un pilote de périphérique de noyau tel qu'OpenIPMI.

Informations supplémentaires

- Pour des informations à jour sur IPMItool, visitez :

  `http://ipmitool.sourceforge.net/`

- Pour plus d'informations sur la spécification IPMI, visitez :

  `http://www.intel.com/design/servers/ipmi/spec.htm`

- Pour plus d'informations sur le projet OpenIPMI (le pilote de noyau IPMI MontaVista), visitez :

  `http://openipmi.sourceforge.net/`

Syntaxe

La syntaxe utilisée par IPMItool est la suivante :

`ipmitool` `[`**`-ghcvV`**`]` **`-I lan -H`** *adresse* `[`**`-P`** *motdepasse*`]` *expression*

`ipmitool` `[`**`-ghcvV`**`]` **`-I open`** *expression*

Options

Le TABLEAU 2-4 indique les options disponibles pour IPMItool.

TABLEAU 2-4 Options d'IPMItool

Option	Description
-h	Fournit de l'aide sur l'utilisation de base depuis la ligne de commande.
-c	Rend la sortie adaptée à l'analyse, lorsque cela est possible, en séparant les champs par des virgules au lieu d'utiliser des espaces.
-g	Tente de rendre la communication IPMI-sur-LAN plus stable.
-V	Affiche les informations relatives à la version.
-v	Augmente la quantité de la sortie de texte. Cette option peut être spécifiée plusieurs fois pour augmenter le niveau de la sortie de débogage. Si elle est donnée trois fois, vous recevez des hexdumps de tous les paquets entrants et sortants.
-I *interface*	Sélectionnez l'interface IPMI à utiliser. Les interfaces possibles sont les suivantes : LAN ou open interface.
-H *adresse*	Affiche l'adresse du serveur distant, peut être une adresse IP ou un nom d'hôte. Cette option est requise pour la connexion de l'interface LAN.
-P *motdepasse*	Affiche le mot de passe du serveur distant ; ce mot de passe est limité à un maximum de 16 caractères. Le mot de passe est optionnel pour l'interface LAN ; si aucun mot de passe n'est fourni, la session n'est pas authentifiée.

Expressions

Le TABLEAU 2-5 indique les expressions et les paramètres disponibles pour IPMItool.

Remarque – Pour chacune de ces expressions, la commande de début est toujours **`ipmitool`** suivie de l'expression et du ou des paramètres.

Remarque – La commande sol n'est pas prise en charge sur ces serveurs, mais vous pouvez activer une fonction série-sur-LAN. Voir « Serial Over LAN », page 122.

TABLEAU 2-5 Expressions et paramètres d'IPMItool *(1 de 4)*

Expression	Paramètre	Sous-paramètre	Description et exemples

help			Peut être utilisé pour obtenir de l'aide de ligne de commande sur les commandes d'IPMItool. Peut aussi être placé à la fin des commandes pour obtenir de l'aide sur l'utilisation des options.
			
			EXEMPLES :
			`ipmitool -I open help`
			`Commands: chassis, fru, lan, sdr, sel`
			
			`ipmitool -I open chassis help`
			`Chassis Commands: status, power, identify, policy, restart_cause`
			
			`ipmitool -I open chassis power help`
			`Chassis Power Commands: status, on, off, cycle, reset, diag, soft`

raw	*netfn*	*cmd données*	Vous permet d'exécuter des commandes IPMI brutes (par exemple, d'interroger le compteur POH).
			
			EXEMPLE :
			`ipmitool -I open raw 0x0 0x1`
			
			`RAW REQ (netfn=0x0 cmd=0x1 data_len=0)`
			`RAW RSP (3 bytes)`
			`60 00 00`

TABLEAU 2-5 Expressions et paramètres d'IPMItool *(2 de 4) (suite)*

Expression	Paramètre	Sous-paramètre	Description et exemples

chaninfo	*canal*		Affiche des informations sur le canal sélectionné. Si aucun canal n'est spécifié, la commande affiche des informations sur le canal en cours d'utilisation.
			
			EXEMPLES :
			`ipmitool -I open chaninfo`
			`Channel 0xf info:`
			`  Channel Medium Type: System Interface`
			`  Channel Protocol Type: KCS`
			`  Session Support: session-less`
			`  Active Session Count: 0`
			`  Protocol Vendor ID: 7154`
			
			`ipmitool -I open chaninfo 7`
			`Channel 0x7 info:`
			`  Channel Medium Type: 802.3 LAN`
			`  Channel Protocol Type: IPMB-1.0`
			`  Session Support: multi-session`
			`  Active Session Count: 1`
			`  Protocol Vendor ID: 7154`
			`  Alerting: enabled`
			`  Per-message Auth: enabled`
			`  User Level Auth: enabled`
			`  Access Mode: always available`

userinfo	*canal*
	Remarque - Les canaux 6 et 7 ne sont pas pris en charge sur les serveurs Sun Fire V20z.
			Affiche des informations sur les informations de l'utilisateur configuré sur un canal LAN spécifique.
			
			EXEMPLE :
			`ipmitool -I open userinfo 6`
			`Maximum User IDs      : 4`
			`Enabled User IDs      : 1`
			`Fixed Name User IDs  : 1`
			`Access Available      : call-in / callback`
			`Link Authentication  : disabled`
			`IPMI Messaging        : enabled`

chassis	status		Retourne des informations sur le statut de plus haut niveau du châssis du serveur et du sous-système d'alimentation principal.
	identify	*intervalle*	Contrôle le voyant identification du panneau frontal. La valeur par défaut est 15 secondes. Entrez « 0 » pour le désactiver.
	restart_cause		Interroge le châssis au sujet de la cause du dernier redémarrage du serveur.

TABLEAU 2-5 Expressions et paramètres d'IPMItool *(3 de 4) (suite)*

Expression	Paramètre	Sous-paramètre	Description et exemples
power			Effectue une commande de contrôle du châssis pour visualiser et changer l'état de l'alimentation.
	status		Affiche le statut courant de l'alimentation du châssis.
	on		Met sous tension le châssis.
	off		Met le châssis hors tension, à l'état *soft off* (état S4/S5). REMARQUE - Cette commande ne lance pas d'arrêt progressif du système d'exploitation avant de mettre le serveur hors tension.
	cycle		Fournit un intervalle de mise hors tension d'au moins une seconde. Aucune action ne devrait se produire si l'alimentation du châssis est à l'état S4/S5, mais il est recommandé de contrôler d'abord l'état de l'alimentation avant de donner une commande de cycle d'alimentation si l'alimentation du serveur est activée ou dans un état de veille inférieur à l'état S4/S5.
	reset		Effectue une réinitialisation matérielle.
lan	print	*canal*	Imprime la configuration courante pour le canal indiqué.
	set	*canal paramètre*	Définit le paramètre indiqué pour le canal indiqué.
		ipaddr *x.x.x.x*	Définit l'adresse IP pour ce canal.
		netmask *x.x.x.x*	Définit le masque de réseau pour ce canal.
		macaddr *xx:xx:xx:xx:xx:xx*	Définit l'adresse MAC pour ce canal.
		defgw ipaddr *x.x.x.x*	Définit l'adresse IP de la passerelle par défaut.
		defgw macaddr *xx:xx:xx:xx:xx:xx*	Définit l'adresse MAC de la passerelle par défaut.
		bakgw ipaddr *x.x.x.x*	Définit l'adresse IP de la passerelle de réserve.
		bakgw macaddr *xx:xx:xx:xx:xx:xx*	Définit l'adresse MAC de la passerelle de réserve.
		password *passe*	Définit le mot de passe de l'utilisateur null.
		user	Active le mode d'accès de l'utilisateur.
		access [on | off]	Définit le mode d'accès du canal LAN.

TABLEAU 2-5 Expressions et paramètres d'IPMItool *(4 de 4) (suite)*

Expression	Paramètre	Sous-paramètre	Description et exemples
		ipsrc *source*	Définit la source de l'adresse IP. Vous pouvez indiquer comme source les éléments suivants : none = pas spécifiée static = adresse IP statique configurée manuellement dhcp = adresse obtenue par le BMC en exécutant DHCP bios = adresse chargée par le BIOS ou le logiciel du système
		arp respond [on | off]	Définit les réponses ARP générées par le BMC.
		arp generate [on | off]	Définit les ARP gratuites générées par le BMC.
		arp interval [seconds] s	Définit l'intervalle pour les ARP gratuites générées par le BMC.
		auth *niveau*,... *type*,...	Cette commande définit les authtypes valides pour un niveau auth donné. Ce niveau peut être : `callback`, `user`, `operator`, `admin` Les types peuvent être : `none`, `md2`, `md5`
fru	print		Lit les données de l'inventaire des CRU et en extrait des informations telles que le numéro de série, le numéro de référence, les étiquettes et les chaînes décrivant le châssis, la carte ou le produit.
sdr	list		Lit les SDR et en extrait les informations des capteurs puis interroge chaque capteur et en imprime le nom, la lecture et le statut.
sel	info		Interroge le BMC pour obtenir des informations sur le SEL et son contenu.
	clear		Efface le contenu du SEL. La commande `clear` est irréversible.
	list		Liste le contenu du SEL.

Pilote de périphérique du noyau Linux IPMI

L'application IPMItool utilise un pilote de noyau OpenIPMI MontaVista qui figure sur le CD Documentation and Support Files des serveurs Sun Fire V20z et Sun Fire V40z. Ce pilote a été modifié pour utiliser une adresse matérielle de base différente et un enregistrement d'E/S de périphérique modifié.

Ce pilote doit être compilé et installé à partir du CD Documentation and Support Files.

Les modules suivants du noyau doivent être chargés pour qu'IPMItool fonctionne :

1. `ipmi_msghandler`

   Le gestionnaire de messages des messages entrants et sortants pour les interfaces IPMI.

2. `ipmi_kcs_drv`

   Pilote d'interface KCS IPMI Keyboard Controller Style (KCS) pour le gestionnaire de messages.

3. `ipmi_devintf`

   Interface de périphérique de caractères Linux pour le gestionnaire de messages.

Pour forcer IPMItool à utiliser l'interface de périphérique, vous pouvez spécifier cet élément sur la ligne de commande :

```
# ipmitool -I open [option...]
```

Installation et compilation du pilote

Pour installer et compiler ce pilote de périphérique de noyau, voir « Configuration initiale du SP », page 14.

Interface LAN pour le BMC

Remarque – Dans ces serveurs, le SP a un logiciel qui émule un BMC.

L'interface LAN d'IPMItool communique avec le BMC via une connexion LAN Ethernet en utilisant le protocole UDP (User Datagram Protocol) sous IPv4. Les datagrammes UDP sont formatés pour contenir des messages de requête/réponse IPMI avec des en-têtes de session IPMI et des en-têtes RMCP *(Remote Management Control Protocol)*.

RMCP est un protocole requête-réponse s'effectuant par le biais de datagrammes UDP sur le port 623. IPMI-sur-LAN utilise la version 1 de RMCP pour prendre en charge la gestion à la fois avant d'installer le SE sur le serveur ou si le serveur n'a pas de SE d'installé.

L'interface LAN est une connexion multisession authentifiée ; les messages fournis au BMC peuvent (et doivent) être authentifiés avec un protocole de type défi/réponse avec soit un mot de passe/ une clé direct soit un algorithme message-digest MD5. IPMItool tente une connexion avec un niveau de privilège d'administrateur car cela est requis pour effectuer les fonctions liées à l'alimentation du châssis.

Avec l'option `-I`, vous pouvez indiquer à IPMItool d'utiliser l'interface LAN :

ipmitool -I lan [*option***...]** *adresse motdepasse*

Pour utiliser l'interface LAN avec IPMItool, vous devez fournir un nom d'hôte sur la ligne de commande.

Le champ du mot de passe est optionnel, si vous n'indiquez pas de mot de passe sur la ligne de commande, IPMItool tente une connexion sans authentification. Si vous indiquez un mot de passe, il utilise l'authentification MD5 si elle est prise en charge par le BMC et, sinon, un mot de passe/une clé direct.

Fichiers

Le fichier `/dev/ipmi0` est un fichier de périphérique de caractères utilisé par le pilote de noyau OpenIPMI.

Exemples

Si vous voulez commander à distance l'alimentation d'un serveur compatible IPMI-sur-LAN, vous pouvez utiliser les commandes suivantes :

ipmitool -I lan -H *adripsp* **-P** *motpassesp* **chassis power on**

Le résultat obtenu en retour est :

```
Chassis Power Control: Up/On
```

ipmitool -I lan -H *adripsp* **-P** *motpassesp* **chassis power status**

Le résultat obtenu en retour est :

```
Chassis Power is on
```

Affichage du journal d'événements système IPMI

Pour afficher le journal d'événements système ou SEL, utilisez IPMItool.

La commande out-of-band est la suivante :

```
# ipmitool -I lan -H adripsp -P motpasseipmi sel list
```

La commande in-band (en utilisant OpenIPMI sur un serveur Linux ou LIPMI sur un serveur Solaris) est la suivante :

```
# ipmitool -I open sel list
```

Remarque – Pour que les messages du journal soient plus détaillés, vous pouvez exécuter la commande suivante :

```
# ssh -l utilisateursp adripsp sp get events
```

Effacement du journal d'événements système IPMI

Vous pouvez utiliser des commandes pour effacer le contenu du SEL IPMI.

Selon votre SE, utilisez l'une ou l'autre des commandes suivantes :

- Pour Linux : **`ipmitool -I open sel clear`**
- Pour Solaris : **`ipmitool -I lipmi sel clear`**

Dépannage d'IPMI

Le TABLEAU 2-6 décrit certains problèmes pouvant survenir avec IPMI et indique des solutions.

TABLEAU 2-6 Dépannage d'IPMI

Problème	Solution
Vous ne parvenez pas à connecter le contrôleur de gestion en utilisant IPMItool sur LAN.	Vérifiez la connexion réseau avec le contrôleur de gestion et son adresse IP, et contrôlez si le canal est activé en utilisant la commande `ipmi get channels`.
Vous ne parvenez pas à vous authentifier auprès du contrôleur de gestion en utilisant IPMItool sur LAN.	Vérifiez si vous utilisez bien le mot de passe qui a été attribué lors de l'activation de l'accès LAN IPMI depuis l'invite de shell du contrôleur de gestion.
Vous avez oublié le mot de passe de l'accès IPMI sur LAN.	1. Vous pouvez redéfinir le paramètre IPMI, redéfinir le SDRR et purger le SEL depuis le shell du contrôleur de gestion en exécutant la commande suivante : # **ssh** *adripsp* **-l** *utilisateursp* **ipmi reset -a** 2. Réactivez maintenant l'accès IPMI sur LAN avec les commandes suivantes : # **ssh** *adripsp* **-l** *utilisateursp* # **ipmi enable channel lan** # **exit**
IPMItool échoue lorsque l'interface « open » est utilisée.	Vérifiez que le module de noyau de Linux `ipmi_kcs_drv` est chargé en exécutant la commande `lsmod`.

CHAPITRE 3

Gestion de serveurs SNMP

Vous pouvez gérer votre serveur en utilisant le protocole SNMP (*Simple Network Management Protocol)*.

Simple Network Management Protocol

SNMP est un protocole de gestion réseau pratiquement exclusivement utilisé dans les réseaux TCP/IP. SNMP fournit un moyen de contrôler et commander les périphériques du réseau, ainsi que de gérer les configurations, le recueil de statistiques, les performances et la sécurité sur un réseau.

La gestion basée sur SNMP permet d'utiliser des solutions de tierces parties telles que des produits comme HP OpenView et CA Unicenter.

Le composant de base d'une solution SNMP est la MIB (*Management Information Base*, base d'informations de gestion). La MIB figure sur le CD Network Share Volume des serveurs Sun Fire V20z et Sun Fire V40z.

Cette configuration est avantageuse quand, par exemple, un cluster de machines sert le contenu Web et que la plate-forme est connectée à Internet, mais que le SP est protégé et n'est accessible que sur un réseau interne.

Intégration SNMP

SNMP est une technologie de gestion réseau ouverte qui permet la gestion de réseaux et d'entités connectées à un réseau. L'architecture SNMP est basée sur un ensemble de stations de gestion réseau et de nœuds gérés.

Les stations de gestion réseau exécutent des applications de gestion, qui contrôlent et commandent les nœuds gérés. Les nœuds gérés sont des périphériques tels que des hôtes, des passerelles et autres, qui sont dotés d'agents de gestion en charge de l'exécution des fonctions de gestion demandées par les stations de gestion.

SNMP est utilisé pour la communication des informations de gestion entre les stations de gestion et les agents. En d'autres mots, SNMP est le protocole par lequel l'agent et la station de gestion communiquent.

Le contrôle d'état au travers de SNMP à tout niveau significatif de détail se fait principalement en demandant les informations appropriées du côté de la station de gestion. Les nœuds gérés peuvent également fournir des informations de statut non-sollicitées sous la forme de déroutements, ce qui guidera probablement l'interrogation au niveau de la station de gestion.

La communication d'informations entre les entités de gestion dans un réseau se fait par l'échange de messages SNMP, qui prennent la forme à la fois de requêtes (get/set) de la station de gestion et de messages non-sollicités (déroutements) indiqués par l'agent.

Votre serveur inclut des agents SNMP qui permettent le contrôle out-of-band du statut et de la maintenance. L'agent SNMP s'exécute sur le SP et, par conséquent, toute la gestion basée sur SNMP du serveur devrait se faire par le biais du SP.

L'agent SNMP des serveurs assure les fonctions suivantes :

- la gestion des événements
- la gestion de l'inventaire
- le contrôle de l'état des capteurs et du système
- le contrôle de la configuration du SP

La MIB SNMP

La MIB est un fichier de texte qui décrit les données SNMP comme des objets gérés. Ces serveurs fournissent des MIB SNMP qui vous permettent de gérer et de contrôler votre serveur en utilisant tout système de gestion réseau compatible SNMP tel que HP OpenView Network Node Manager (NNM), Tivoli, CA Unicenter, IBM Director, etc. Les données de la MIB décrivent les informations gérées, reflètent les statuts courant et récent du serveur et fournissent des statistiques sur le serveur.

Arborescence de la MIB des serveurs Sun Fire V20z et Sun Fire V40z

La FIGURE 3-1 illustre l'arborescence MIB.

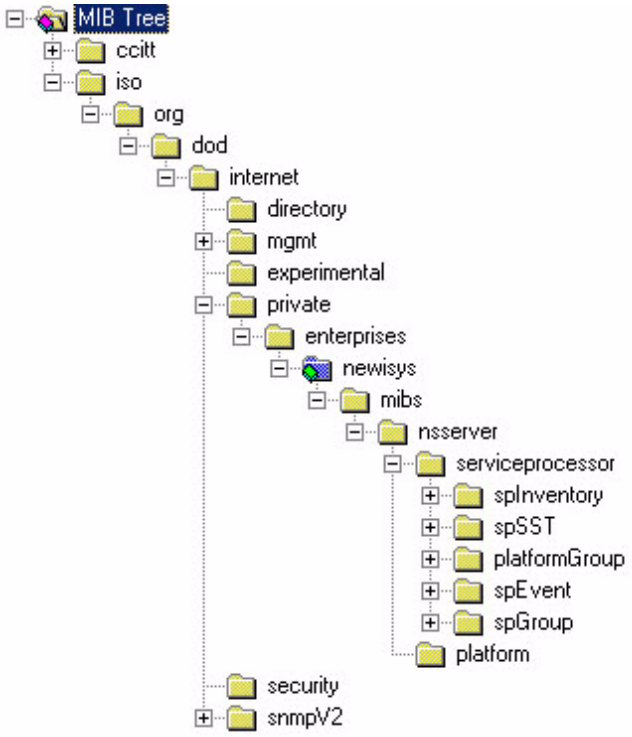


FIGURE 3-1 Arborescence MIB

Intégration des MIB avec des consoles de tierces parties

Vous utilisez les MIB des serveurs pour intégrer la gestion et le contrôle du serveur dans les consoles de gestion SNMP. La branche de la MIB est une MIB d'entreprise privée, localisée à l'identificateur d'objet (OID) 1.3.6.1.2.1.9237. Le port SNMP standard 161 est utilisé par l'agent SNMP sur le SP.

Configuration de SNMP sur le serveur

Remarque – Plusieurs services sont fournis par l'agent SNMP du serveur. Selon les besoins de votre entreprise et la configuration de votre environnement de gestion et réseau courant, certains de ces services peuvent vous intéresser.

Certains éléments de configuration et conditions sont requis à la fois sur le SP et la plate-forme pour activer et utiliser chacun de ces services :

- l'agent SNMP sur le SP
- l'application de retransmission proxy/l'agent proxy [RFC 2271]
- l'agent X [RFC 2741]

Les clients peuvent choisir de gérer un serveur out-of-band (OOB) par le biais du SP. Avec la gestion OOB, le SP est la cible de la requête SNMP. L'agent SNMP du SP est configuré pour assurer une fonction de requêtes proxy de sorte que les requêtes d'OID qui ne sont pas liées au SP sont transmises, de manière transparente, au SE de la plate-forme.

Configuration de la gestion out-of-band

La FIGURE 3-2 illustre l'architecture SNMP et les voies de communication entre le SP et la plate-forme.

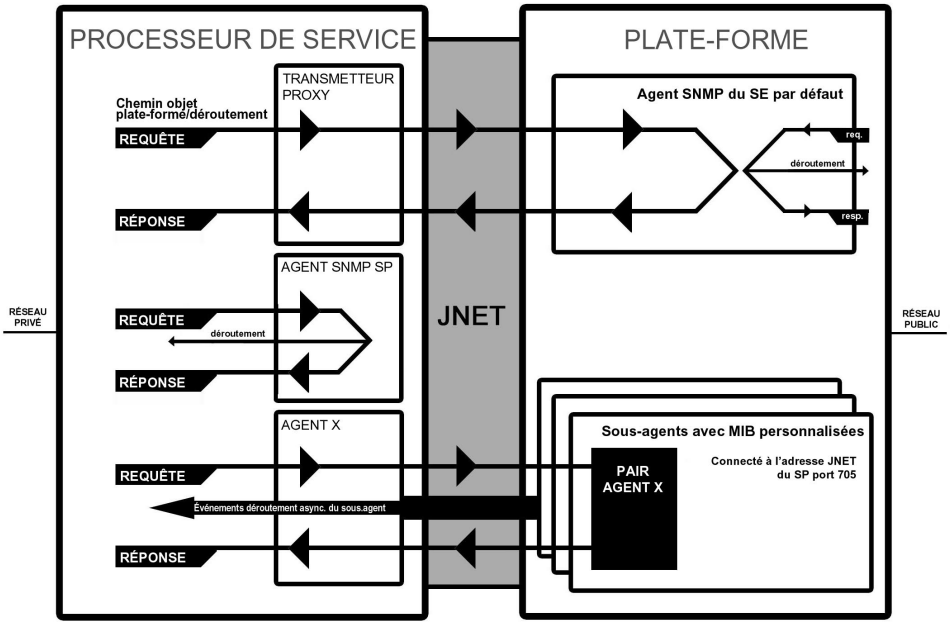


FIGURE 3-2 Architecture SNMP et communications

Agent SNMP du processeur de service

L'agent SNMP qui s'exécute sur le SP facilite la gestion et le contrôle du serveur. L'agent SNMP peut être utilisé pour demander divers types d'informations relatives au SP. Reportez-vous à la FIGURE 3-1 pour la liste des MIB ; au TABLEAU 3-3 pour leur description détaillée.

Aucune configuration n'est requise pour utiliser cette fonction à l'exception de l'intégration des MIB du serveur avec la station de gestion de votre choix.

Reportez-vous à la procédure permettant d'utiliser l'agent SNMP sur le SP, comme expliqué dans « Intégration des MIB avec des consoles de tierces parties », page 92.

Remarque – L'agent SNMP de ces serveurs prend en charge SNMP v1/v2c. Pour des raisons de sécurité, il n'y a pas d'attributs définissables dans cet agent.

Agent proxy

Le SP agit comme un agent proxy SNMP intermédiaire pour la plate-forme. Les requêtes faites depuis une station de gestion à l'agent SNMP du SP sont interceptées par l'agent proxy du SP et transmises à la plate-forme ; l'agent proxy du SP contacte la plate-forme pour récupérer les informations demandées. L'agent proxy reçoit ensuite les données de la plate-forme et renvoie la requête à la station de gestion. La station de gestion ignore totalement que la requête est passée par un proxy. Le SP et la plate-forme communiquent sur un réseau privé interne.

Pour activer cette fonction, vous devez d'abord exécuter un agent SNMP sur le système d'exploitation de votre plate-forme (consultez le vendeur de votre SE pour vous procurer cet agent). Cette opération active de façon transparente la gestion au niveau de la plate-forme au travers du SP. Interroger des MIB autres que celle du serveur (par exemple, la MIB des ressources de l'hôte) et la MIB système MIBII du SP permet d'obtenir des informations de la plate-forme en transmettant par un proxy la requête à l'agent SNMP de la plate-forme.

Assurez-vous que le SP peut identifier les noms des communautés de lecture seule et écriture seule qui sont configurés pour l'agent SNMP de votre plate-forme. Voir « Définition du nom de la communauté », page 94.

Définition du nom de la communauté

L'agent SNMP du SP agit comme un proxy pour l'agent SNMP s'exécutant sur la plate-forme (voir « Configuration de SNMP sur le serveur », page 92). Pour utiliser correctement le proxy, vous devez utiliser la chaîne de communauté. La chaîne de communauté nécessaire pour cette opération est la valeur définie lorsque vous avez configuré la plate-forme pour SNMP.

Si vous trouvez que vos requêtes SNMP ne sont pas transmises par le proxy aux agents SNMP de la plate-forme, vérifiez si la chaîne de communauté définie sur le SP correspond à celle qui l'est sur la plate-forme. La chaîne de communauté du proxy du SP peut être modifiée pour correspondre à la chaîne de communauté de la plate-forme en utilisant la commande suivante :

```
# sp set snmp proxy community
```

Il n'y a pas de restrictions au niveau de la longueur des chaînes de communauté ; les noms courants sont *private* et *public*. Le nom par défaut est *public*.

Pour plus d'informations, voir « Sous-commande sp set snmp proxy community », page 288.

Agent X

Un sous-agent utilisant le protocole Agent X SNMP sur la plate-forme peut se connecter à l'agent SNMP du SP (au travers d'un port spécial) et transmettre les réponses aux requêtes ou les déroutements non-sollicités au travers du SP. Cela permet au trafic de gestion du serveur de rester protégé du réseau de production connecté à la plate-forme, si requis.

Pour activer correctement cette fonction, vous devez identifier la paire adresse IP / numéro de port associée au SP (telle que vue de la plate-forme). Le port Agent X est fixé à 705 (TCP). Toutefois, l'adresse IP du réseau privé est configurable et est, par défaut, 169.254.101.2.

Reportez-vous à la documentation de votre application pour les instructions de configuration des sous-agents.

Remarque – Vous pouvez utiliser la sous-commande `sp get jnet` sur le SP pour récupérer l'adresse IP JNET du SP. Pour plus d'informations, voir « Sous-commandes du SP relatives à l'adresse JNET », page 247.

Utilisation d'un navigateur de MIB de tierce partie

L'exemple suivant illustre l'intégration des MIB du serveur dans un gestionnaire de nœuds SNMP.

1. **Dans le menu Manager Preferences, choisissez Load/Unload MIBS : SNMP**
2. **Localisez et sélectionnez le fichier** `SP-MasterAgent-MIB.mib`**.**
3. **Cliquez sur Load.**
4. **Spécifiez le répertoire dans lequel les MIB du serveur sont placées et cliquez sur Open.**
5. **Répétez les opérations de l'étape 2 à l'étape 4 pour charger d'autres MIBS (par exemple,** `SP-SST-MIB.mib`**,** `SP-INVENTORY-MIB.mib`**,** `SP-EVENT-MIB.mib`**,** `SP-PLATFORM-MIB.mib`**,** `SP-GROUP-MIB.mib`**, etc.).**
6. **Sortez du menu Manager Preferences.**
7. **Ouvrez un navigateur de MIB SNMP.**

   L'arborescence standard de SNMP s'affiche dans le navigateur de MIB.
8. **Localisez la branche Newisys sous private.enterprises.**

   Pour un exemple d'arborescence de MIB, voir la FIGURE 3-1.

Définition des options de journalisation

Vous pouvez aussi intégrer facilement les déroutements générés par le SP et définir les options de journalisation. L'exemple suivant illustre les étapes à suivre quand HP OpenView NNM est utilisé :

1. **Chargez** `SP-EVENT-MIB.mib` **comme indiqué dans la procédure précédente.**
2. **Choisissez Options>EventConfiguration**
3. **Sélectionnez le module spEvent dans la liste Enterprises.**
4. **Double-cliquez sur un événement dans la liste Events for Enterprise spEvent.**
5. **Sélectionnez l'onglet Event Message.**
6. **Sélectionnez Log and Display dans la boîte de dialogue Category et choisissez une catégorie dans la liste correspondante ou créez votre propre catégorie d'événements.**
7. **Sélectionnez la gravité de l'événement dans la liste Severity.**
8. **Entrez un message ou `$*` pour afficher toutes les informations du champ Event Log Message.**
9. **Cliquez sur OK.**

Déroutements SNMP

Les déroutements SNMP sont des notifications de gestion réseau d'un événement se produisant au niveau d'un nœud géré du réseau. Ces événements peuvent identifier les problèmes du réseau, les machines en ou hors service, etc. Ces serveurs utilisent des déroutements pour signaler des conditions liées à la maintenance du serveur, y compris des conditions critiques liées à des composants physiques, le retour à un état normal de ces composants et d'autres situations liées à l'état du logiciel en cours d'exécution sur le SP (par exemple, les paramètres réseau reconfigurés).

Les déroutements sont définis dans les fichiers MIB et sont générés, reçus et traités par une station de gestion SNMP. Les données des déroutements SNMP sont identifiées de façon unique par la MIB. Chaque déroutement SNMP contient des informations qui identifient le nom du serveur, l'adresse IP et d'autres données pertinentes sur l'événement.

Au sein de la MIB des événements du serveur, chaque déroutement a les variables et les liaisons d'événement suivantes ; voir le TABLEAU 3-1.

TABLEAU 3-1 Déroutements d'événement du serveur

Événement	Description
EventID	Identifie de façon unique l'événement sur le SP d'où il vient.
EventSource	Indique le module source qui a généré l'événement.
EventComponent	Indique l'ID du composant auquel l'événement fait référence.
EventDescription	Message de l'événement reçu de sa source.
EventTimeStampInitial	Heure à laquelle cet ID d'événement a été généré à l'origine.
EventTimeStampLast	Heure la plus récente à laquelle cet ID d'événement a été généré.

Configuration des destinations des déroutements SNMP

Bien que les déroutements SNMP soient générés pour des événements qui se produisent sur le SP, vous devez configurer l'endroit où ces déroutements doivent être envoyés. Il n'y a pas de destination par défaut pour les déroutements. Vous pouvez utiliser les sous-commandes de gestion du serveur (voir le TABLEAU 3-2) sur le SP pour configurer les destinations SNMP.

Pour plus d'informations sur ces sous-commandes, voir l'Annexe H.

TABLEAU 3-2 Sous-commandes pour la configuration des destinations SNMP

Sous-commande	Description
`sp get snmp-destinations`	Affiche les adresses IP de toutes les destinations SNMP disponibles et les noms des hôtes auxquels le SP enverra les déroutements.
`sp add snmp-destination`	Ajoute une nouvelle destination SNMP à raison d'une adresse IP ou d'un nom d'hôte à la fois.
`sp delete snmp-destination`	Supprime une destination SNMP existante à raison d'une adresse IP ou d'un nom d'hôte à la fois.

Configuration des destinations SNMP

Les utilisateurs administratifs et de niveau gestionnaire peuvent définir les destinations SNMP auxquelles des événements SNMP (alertes) seront envoyés en utilisant cette option. Tous les utilisateurs peuvent afficher les destinations courantes (en utilisant l'accès en lecture seule).

Le nombre des destinations que vous créez est limité par la mémoire.

Vous pouvez configurer des destinations SNMP en utilisant les sous-commandes `sp snmp`. Pour plus d'informations sur ces sous-commandes, voir l'Annexe H.

Détails de la MIB du serveur

SNMP utilise des identificateurs d'objet ou OID *(Object Identifier)* pour fournir des variables de nom sous lesquelles les objets sont regroupés pour qu'il soit plus facile d'y faire référence. Ces serveurs fournissent des agents pour les MIB indiquées dans le TABLEAU 3-3.

TABLEAU 3-3 MIB SNMP

MIB	OID	Description
SP-MasterAgent-MIB .mib	.1.3.6.1.4.1.9237	Crée le tronc principal de l'arborescence de la MIB du serveur. Toutes les autres MIB du SP partent de ce tronc. Doit être chargé en premier lors de l'intégration avec une structure de partie tierce.
SP-INVENTORY-MIB .mib	.1.3.6.1.4.1.9237.2.1.1.1 .1.3.6.1.4.1.9237.2.1.1.1.2 .1.3.6.1.4.1.9237.2.1.1.1.3	Est utilisé pour demander les informations d'inventaire pour tous les composants matériels et logiciels des serveurs Sun Fire V20z et Sun Fire V40z. **Hardware Inventory Table** : contient l'inventaire des composants matériels. **Software Inventory Table** : contient l'inventaire des composants logiciels.
SP-SST-MIB.mib	.1.3.6.1.4.1.9237.2.1.1.4	Définit les objets pour le tableau System State Table dans le SP. Contient tous les relevés des capteurs, indique le nom du capteur, sa valeur courante, la valeur maximale autorisée, le type de mesure, l'échelle et l'intervalle de balayage.

TABLEAU 3-3 MIB SNMP *(suite)*

MIB	OID	Description
SP-PLATFORM-MIB.mib	.1.3.6.1.4.1.9237.2.1.1.5	Définit les objets pour le SNMP de la plate-forme, qui incluent l'état du SE, l'état de la plate-forme et la table IP de la plate-forme.
SP-EVENT-MIB.mib	.1.3.6.1.4.1.9237.2.1.1.6	Identifie les OID associés à tous les déroutements SNMP ayant pour origine le SP.
SP-GROUP-MIB.mib	.1.3.6.1.4.1.9237.2.1.1.7	Définit les objets pour le SP, dont le nom de l'hôte, le DNS, un nœud de redémarrage, un nœud devant contenir le dernier code POST du port 80, un arbre clone et une table IP.

Les événements listés dans le TABLEAU 3-4 sont envoyés à la destination SNMP par `SP-EVENT-MIB.mib`.

TABLEAU 3-4 Événements du SP *(1 de 2)*

ID du déroutement d'entreprise	Événement
1	`spGenericEventInformational`
2	`spGenericEventWarning`
3	`spGenericEventCritical`
4	`spTemperatureEventInformational`
5	`spTemperatureEventWarning`
6	`spTemperatureEventCritical`
7	`spVoltageEventInformational`
8	`spVoltageEventWarning`
9	`spVoltageEventCritical`
10	`spFanEventInformational`
11	`spFanEventWarning`
12	`spFanEventCritical`
13	`spPlatformMachineCheckEventInformational`
14	`spPlatformMachineCheckEventWarning`
15	`spPlatformMachineCheckEventCritical`
16	`spPlatformStateChangeEventInformational`
17	`spPlatformStateChangeEventWarning`
18	`spPlatformStateChangeEventCritical`
19	`spPlatformBIOSEventInformational`

TABLEAU 3-4 Événements du SP *(2 de 2) (suite)*

ID du déroutement d'entreprise	Événement
20	spPlatformBIOSEventWarning
21	spPlatformBIOSEventCritical
22	spGenericEventInformational
23	spGenericEventWarning
24	spGenericEventCritical
25	spTemperatureEventInformational
26	spTemperatureEventWarning
27	spTemperatureEventCritical
28	spVoltageEventInformational
29	spVoltageEventWarning
30	spVoltageEventCritical
31	spFanEventInformational
32	spFanEventWarning
33	spFanEventCritical
37	spPlatformStateChangeEventInformational
38	spPlatformStateChangeEventWarning
39	spPlatformStateChangeEventCritical
40	spPlatformBIOSEventInformational
41	spPlatformBIOSEventWarning
42	spPlatformBIOSEventCritical

Dépannage SNMP

Le TABLEAU 3-5 décrit un problème pouvant survenir avec SNMP et indique une solution.

TABLEAU 3-5 Dépannage SNMP

Problème	Solution
Les requêtes SNMP faites au SP expirent.	Le SE de la plate-forme a besoin à la fois du RPM de la suite de pilotes RPM et d'un démon SNMP actif partageant la chaîne de communauté du SP.

CHAPITRE 4

Informations de gestion supplémentaires

Configuration des fonctions d'écriture de scripts

Un administrateur système peut se connecter au SP en utilisant SSH et émettre des commandes ou, plus communément, écrire un script de shell qui appelle ces opérations à distance.

Remarque – Vous devez créer un compte de gestionnaire initial valide avant d'utiliser SSH. Le SP inclut un compte de configuration qui peut être utilisé pour configurer un compte de gestionnaire initial. Cet utilisateur gestionnaire initial peut créer des utilisateurs supplémentaires.

Pour plus d'informations sur le compte de gestionnaire initial, voir « Partie II : Sécurisation du SP », page 19.

Le SP inclut une suite de commandes qui permettent la gestion et le contrôle du serveur, à laquelle il est fait référence comme aux commandes de gestion du serveur. De la ligne de commande, par exemple, vous pouvez écrire des scripts pilotés par les données qui automatisent la configuration de plusieurs machines.

Le CD Network Share Volume des serveurs Sun Fire V20z et Sun Fire V40z contient des exemples de scripts pour la mise en route, auxquels vous pourrez accéder après avoir extrait les fichiers du CD. Pour plus d'informations sur l'emplacement des scripts, voir « CD-ROM Network Share Volume (NSV) », page 120.

Utilisation des scripts de shell

Un administrateur peut apporter des changements de configuration à un SP donné en utilisant SSH pour se connecter et exécuter des commandes. Pour un environnement à plusieurs systèmes dans lequel les configurations de tous les SP doivent être synchronisées, vous pouvez automatiser les changements de configuration.

En tant qu'administrateur Unix/Linux ou Windows, vous pouvez utiliser SSH, des relations d'hôte de confiance ou l'authentification à clé publique, et des scripts de shell Unix/Linux pour automatiser les tâches qui doivent être effectuées sur plusieurs SP.

1. **Configurez votre système pour l'écriture de scripts.**

   Les solutions d'écriture de scripts à distance pour serveurs dépendent de SSH pour l'authentification et le chiffrement des données. Si vous n'avez pas SSH, vous pouvez en obtenir une implémentation gratuite, OpenSSH, sur `www.openssh.org`. Le SP permet uniquement l'utilisation de SSH v2. Voir « Scripts à distance utilisant SSH », page 105.

2. **Créez une relation d'hôte de confiance ou ajoutez une clé publique pour l'authentification SSH.**

   Pour pouvoir utiliser SSH dans un environnement utilisant des scripts sans être invité à entrer un mot de passe à l'exécution de chaque commande, vous pouvez établir une relation d'hôte de confiance entre la machine de laquelle les commandes sont envoyées et le SP sur lequel les commandes sont exécutées (ceci exige la création préalable d'un utilisateur de niveau gestionnaire sur le SP). Voir « Création de relations d'hôte de confiance », page 107.

   Vous pouvez aussi ajouter une clé publique pour l'authentification SSH, ce qui vous permettra de vous connecter via SSH et d'exécuter des commandes à distance sans être invité à entrer un mot de passe. Voir « Ajout de clés publiques », page 107.

3. **Configurez votre client pour l'écriture de scripts.**

   Vous devez configurer la machine cliente sur laquelle vous exécuterez des scripts. Étant donné que Windows ne prend au départ pas en charge la fonction de relation d'hôte de confiance du SP, l'utilisation de scripts depuis un client Windows exige que vous installiez un jeu d'outils Unix/Linux-sur-Windows prenant en charge SSH. Voir « Configuration d'un client Windows pour l'utilisation de scripts », page 109.

4. **Créez vos scripts.**

Scripts à distance utilisant SSH

L'écriture de scripts à distance vers le SP s'effectue en utilisant un programme appelé SSH. Par exemple, si vous étiez un utilisateur sur la machine UNIX **client.company.com** et que le nom du SP était **sp.company.com**, vous pourriez exécuter une commande sur le SP depuis le client UNIX en utilisant le format suivant :

```
# ssh sp.company.com commande
```

Étant donné que le serveur SSH doit authentifier l'utilisateur distant, soit ce dernier doit entrer un mot de passe, soit il doit y avoir une relation d'hôte de confiance, soit la clé publique de l'utilisateur distant doit être installée sur le SP.

Si des relations d'hôte de confiance sont utilisées pour un accès sans mot de passe, le SP doit avoir un utilisateur local du même nom que l'utilisateur distant (ou l'utilisateur distant doit être membre d'un groupe de service d'annuaire qui est mappé vers un groupe administratif local du SP).

Vous pouvez aussi ajouter votre fichier de clé publique au lieu de créer une relation d'hôte de confiance pour être authentifié via SSH. Voir « Ajout de clés publiques », page 107.

Dans le cadre d'une configuration autorisant l'accès sans mot de passe, le démon SSH qui est sur le SP autorise l'utilisateur distant à accéder à **sp.company.com** sans mot de passe, que ce soit pour se connecter ou pour émettre des commandes ssh à distance depuis la ligne de commande ou un script.

Configuration de plusieurs systèmes pour l'utilisation de scripts

Il y a deux façons de configurer plusieurs SP pour l'emploi de scripts :

- Exécutez la procédure pour configurer la machine cliente sur laquelle vous exécuterez des scripts pour chaque SP. Voir « Configuration d'un client Windows pour l'utilisation de scripts », page 109.
- Établissez une relation de confiance ou ajoutez votre fichier de clé publique sur une première machine puis utilisez la fonction de configuration automatique pour répliquer la configuration sur chacune des autres machines. Voir « Création de relations d'hôte de confiance », page 107 et « Ajout de clés publiques », page 107.

Génération de clés d'hôte

Pour établir une relation d'hôte de confiance, vous devez configurer une clé d'hôte qui est utilisée pour authentifier un hôte auprès d'un autre. L'installation SSH de l'hôte devrait générer les clés d'hôte. Si ce n'est pas le cas, suivez ces étapes pour générer une paire de clés d'hôte :

1. **Entrez la commande suivante :**

   ```
   # ssh-keygen -q -t rsa -f rsa_key -C '' -N ''
   ```

2. **Déplacez** `rsa_key` **dans** `/etc/ssh/ssh_host_rsa_key`**.**

3. **Déplacez** `rsa_key.pub` **dans** `/etc/ssh/ssh_host_rsa_key.pub`**.**

4. **Assurez-vous que seul l'utilisateur *root* a des permissions de lecture ou d'écriture dans** `/etc/ssh/ssh_host_rsa_key`**.**

   Le fichier `ssh_host_rsa_key.pub` est le fichier que vous transférez au SP.

   Remarque – Seuls les types de clé de la version 2 du protocole et les tailles de clé de 1024 bits (la clé par défaut générée par `ssh-keygen`) sont pris en charge.

   ---

5. **Copiez la clé publique de l'hôte (le fichier** `ssh_host_rsa_key.pub`**) sur le SP en utilisant** `scp` **(copie sécurisée) ou en copiant la clé de l'hôte sur un système de fichiers externe qui a été monté sur le SP.**

   Remarque – Utilisez `scp` pour copier les fichiers dans le répertoire `/tmp` ou dans votre répertoire personnel. Les commandes `sp` installeront ensuite le fichier spécifié sur le ligne de commande.

   ---

6. **Passez ensuite à « Création de relations d'hôte de confiance », page 107 où vous trouverez les instructions à suivre pour créer des clés publiques pouvant être utilisées pour un accès sans mot de passe.**

Création de relations d'hôte de confiance

Ajouter une relation d'hôte de confiance est l'une des méthodes permettant un accès sans mot de passe et permet par conséquent l'utilisation de scripts de type un à plusieurs. Une fois une relation d'équivalence d'hôte créée avec un client, les utilisateurs de ce client peuvent exécuter à distance des commandes sur le SP sans être invités à entrer de mot de passe, du moment que l'une des conditions suivantes est remplie :

- Le nom de connexion de l'utilisateur sur le client est identique à celui de l'utilisateur local sur le SP.
- La connexion de l'utilisateur sur le client appartient à un groupe de services d'annuaire qui est mappé vers un groupe administratif du SP (dans ce cas, la commande SSH exécute aussi un utilisateur auxiliaire bien connu sur le SP : *rmonitor*, *radmin* ou *rmanager*).

Remarque – La prise en charge est disponible uniquement pour les types de clés de la version 2 du protocole SSH (RSA ou DSA). Si DNS est activé sur le SP, la machine cliente doit être spécifiée par son nom DNS, pas par une adresse IP.

Les utilisateurs du niveau gestionnaire peuvent créer une relation d'hôte de confiance pour l'hôte spécifié depuis la ligne de commande en utilisant la commande `access add trust` :

access add trust {-c | --client} *HOST* **{-k | --keyfile} **
FICHIER CLÉ PUBLIQUE

Ajout de clés publiques

Ajouter la clé publique d'un utilisateur est une autre méthode permettant un accès sans mot de passe et permet par conséquent l'utilisation de scripts de type un à plusieurs. Une fois une clé publique installée sur le SP pour un utilisateur spécifique, cet utilisateur peut exécuter à distance des commandes sur le SP sans être invité à entrer de mot de passe, si cet utilisateur a installé la clé privée associée sur le client.

Remarque – La prise en charge est disponible uniquement pour les types de clés de la version 2 du protocole SSH (RSA ou DSA).

Seuls les utilisateurs locaux peuvent ajouter des clés publiques. Les utilisateurs qui obtiennent une autorisation à partir des mappages de groupes des services d'annuaire ne sont pas autorisés à ajouter des clés publiques.

Les utilisateurs locaux de niveau administratif ou de niveau gestionnaire peuvent ajouter des clés publiques en utilisant la commande `access add public key`:

```
# access add public key -l FICHIER_CLÉ_PUBLIQUE [-u user]
```

Le fichier de clé publique est votre clé RSA ou DSA. Un maximum de 10 utilisateurs peuvent installer des clés publiques ; une seule clé est autorisée par utilisateur.

Les utilisateurs de niveau administratif peuvent ajouter leur clé publique propre. Les utilisateurs de niveau gestionnaire peuvent ajouter une clé publique pour tout utilisateur local. Si l'*utilisateur* n'est pas spécifié dans la commande, l'utilisateur courant est celui par défaut.

Remarque – La longueur de clé maximale prise en charge est de 4 096 bits.

Génération d'une paire de clés d'hôte

Pour établir une relation d'hôte de confiance, vous devez configurer une clé d'hôte qui est utilisée pour authentifier un hôte auprès d'un autre. Suivez ces étapes pour générer une paire de clés d'hôte en copiant la clé publique sur le SP auquel vous voulez pouvoir accéder sans mot de passe :

1. **Exécutez la commande suivante :**

   ```
   # ssh-keygen -t rsa -N
   ```

2. **Acceptez les valeurs par défaut, en effectuant l'installation dans le répertoire suivant :**

   `$HOME/.ssh/id_rsa`

   Les fichiers suivants sont créés :

   ```
   $HOME/.ssh/id_rsa
   $HOME/.ssh/id_rsa.pub
   ```

Configuration d'un client Windows pour l'utilisation de scripts

Pour configurer la machine cliente sur laquelle vous exécuterez des scripts :

1. **Créez un utilisateur de niveau gestionnaire à la fois sur la machine cliente et sur le SP.**

   Vous pouvez créer un utilisateur de n'importe quel nom du moment que le nom en question existe sur les deux machines.

2. **Définissez un nom d'hôte pour le SP.**
3. **Définissez un nom d'hôte pour la machine cliente.**
4. **Vérifiez que le SP et la machine cliente peuvent tous deux résoudre mutuellement leurs adresses.**

Installation du jeu d'outils Cygwin

Étant donné que Windows ne prend au départ pas en charge la fonction de relation d'hôte de confiance sur le SP, l'utilisation de scripts depuis un client Windows exige que vous installiez un jeu d'outils Unix/Linux-sur-Windows prenant en charge SSH.

Pour installer le jeu d'outils Cygwin

1. **Naviguez vers** `www.cygwin.com`**.**
2. **Pour lancer le programme d'installation, cliquez sur l'un des nombreux liens « Install Cygwin now! ».**
3. **Enregistrez le programme** `setup.exe` **dans un dossier local :**

   Choisissez Save dans la boîte de dialogue Download.

4. **Ouvrez le dossier et exécutez le programme** `setup.exe`**.**
5. **Suivez les invites de l'assistant d'installation.**

   Les options suivantes sont recommandées :

   - Download Source: Install from Internet
   - Root Install Directory: File type - Unix
   - Internet Connection: Direct Connection

6. **Choisissez un site de téléchargement miroir.**
7. **Dans la boîte de dialogue Select Packages, ouvrez Net Category et contrôlez les éléments OpenSSH et OpenSSL.**
8. **Complétez l'installation.**

Activation de l'accès SSH en utilisant les hôtes de confiance

Suivez ces étapes pour ajouter des utilisateurs au fichier `local /etc/password` pour tenter un accès de type hôte de confiance au processeur de service :

1. **Activez l'accès pour les clients en lançant un shell Bash.**
   - Si vous voulez que tous les comptes du réseau soient ajoutés, exécutez **`mkpasswd >> /etc/passwd`**.
   - Si vous voulez que seuls les comptes locaux soient ajoutés, exécutez **`mkpasswd -l >> /etc/passwd`**.
2. **Créez ou modifiez le fichier** `/etc/ssh_config` **pour vous assurer qu'il contient l'entrée suivante :**

   ```
   Host *
   HostbasedAuthentication yes
   ```
3. **Configurez les clés de votre hôte en exécutant la commande suivante :**

   # **`ssh-host-config`**
4. **En tant qu'utilisateur de niveau gestionnaire sur le client, exécutez les commandes suivantes pour établir une relation d'hôte de confiance (*gestionnaire1* est utilisé dans l'exemple à cette étape) :**

   a. **Copiez la clé du client dans** `/tmp` **sur le SP.**

      # **`scp /etc/ssh_host_dsa_key.pub`** *gestionnaire1*`@sp.test.com:/tmp`

   b. **Authentifiez-vous pour la commande** `scp` **en entrant le mot de passe correspondant à votre nom d'utilisateur de niveau gestionnaire.**

   c. **Ajoutez la clé du client au jeu des hôtes de confiance de ce SP.**

      # **`ssh`** *gestionnaire1*`@sp.test.com access add trust -c client.test.com\ -k /tmp/ssh_host_dsa_key.pub`

   d. **Authentifiez-vous pour la commande SSH.**

   À ce stade, tout utilisateur ayant le même nom de connexion dans à la fois `sp.test.com` et `client.test.com` aura accès sans mot de passe au compte du même nom sur `sp.test.com`.

Génération d'une paire de clés d'hôte sous Windows

Pour configurer votre paire de clés d'hôte :

1. **Lancez un client SSH.**

   Sous Windows, lancez un shell Cygwin Bash. L'utilisation de scripts depuis un client Windows exige que vous installiez un jeu d'outils Unix/Linux-sur-Windows prenant en charge SSH. Voir « Configuration d'un client Windows pour l'utilisation de scripts », page 109.

2. **Exécutez ssh-host-config pour créer les deux paires de clés DSA et RSA :**

   ```
   /etc/ssh_host_dsa_key
   /etc/ssh_host_dsa_key.pub
   /etc/ssh_host_rsa_key
   /etc/ssh_host_rsa_key.pub
   ```

   Les paires de clés d'hôte sont créées dans `/etc` pour les machines Windows et dans `/etc/ssh` sur les machines Unix/Linux.

Activation de l'accès SSH en utilisant des clés publiques

Suivez ces étapes pour installer des clés publiques pour permettre l'accès SSH.

1. **Configurez vos clés d'hôte. Voir « Génération d'une paire de clés d'hôte », page 108.**

2. **Installez votre clé publique en utilisant la commande** `access add public key`**.**

3. **Exécutez la commande suivante sur la machine cliente :**

   # **ssh -t rsa -N**

   Cette commande génère `~/.ssh/id_dsa` et `~/.ssh/id_dsa.pub`.

4. **Exécutez la commande suivante sur la machine cliente :**

   # **scp ~/.ssh/id_rsa.pub** *IP_SP*:**/tmp**

   Entrez votre mot de passe lorsque vous y êtes invité.

5. **Exécutez la commande suivante sur la machine cliente :**

   # **ssh** *IP_SP* **access add public key -k /tmp/id_rsa.pub**

   Entrez votre mot de passe lorsque vous y êtes invité.

6. **Exécutez la commande suivante :**

   # **ssh** *IP_SP* **rm -f /tmp/id_rsa.pub**

   À cs stade, l'accès vous est autorisé sans mot de passe.

Directives pour l'écriture de scripts de commande pour la gestion du serveur

Cette section contient des directives de base relatives à la gestion des systèmes au moyen de scripts pour une exécution à distance sur un ou plusieurs SP.

- **Scripts de shell :** vous devez avoir l'habitude des scripts de shell standard. Voir « Utilisation des scripts de shell », page 104.
- **SSH :** vous devez couramment utiliser un client SSH (Secure Shell) pour exécuter les scripts de commande automatisés. Voir « Scripts à distance utilisant SSH », page 105.
- **Authentification :** pour éviter d'être invité à entrer un mot de passe à chaque fois que vous exécutez un script sur un SP, téléchargez vers chaque SP une clé publique ou une clé d'hôte de confiance SP. Voir « Création de relations d'hôte de confiance », page 107 et « Ajout de clés publiques », page 107.
- **Niveaux d'autorisation :** les changements au niveau de l'accès (par exemple l'ajout d'utilisateur ou le téléchargement de clés) nécessite en général un accès de niveau gestionnaire tandis que la plupart des autres tâches de gestion peuvent être effectuées par un utilisateur de niveau gestionnaire.
- **Codes retournés :** chaque sous-commande retourne un ou plusieurs codes de retour à la fin de l'opération.
- **Argument nowait :** la plupart des commandes s'exécutent relativement rapidement et sont par conséquent effectuées de façon synchronisée. Pour certaines opérations plus longues (par exemple redémarrage de la plate-forme), une option `--nowait` est fournie pour qu'un script puisse lancer l'opération sans attendre le retour.
- **Argument quiet :** les opérations de suppression et de mise à jour (par exemple `access delete user`, `sp delete event`) acceptent les cibles multiples. Pour vous assurer qu'un certain ensemble de cibles est supprimé d'un ensemble de SP, vous pouvez utiliser l'argument `--quiet` pour supprimer les erreurs si l'une des cibles est introuvable ou pour supprimer des messages d'avertissement interactifs depuis la commande de la plate-forme.

Sortie des commandes

La liste suivante définit une sortie générale courante :

- Les commandes qui retournent `0` sans chaîne de retour de succès. Certaines exceptions sont des commandes qui retournent aussi des informations capitales.
- La sortie du tableau, les avertissements interactifs et d'autres messages qui ne sont pas des erreurs sont dirigés dans la sortie standard.
- Pour les commandes qui retournent des erreurs, les codes de retour et une chaîne d'erreur de description s'affichent.

Voici les caractéristiques courantes de la sortie sous forme de tableau d'une commande `get` :

- Les titres de colonnes sont fournis par défaut pour les sorties comportant plus de une colonne.
- Une sortie à une seule colonne ne comporte pas de titre.
- Pour supprimer les titres, utilisez l'argument `-H`.
- Les données de chaque colonne sont alignés à gauche avec au moins un espace entre les colonnes. Les données numériques sont alignées à droite.
- L'argument `-D` vous permet de spécifier un caractère de délimitation lors de l'écriture du script. Cela est très utile lors de l'analyse des champs contenant des espaces vierges.
- Si toutes les lignes ont le même nombre et type de valeurs de données, chaque ligne est imprimée sous la forme d'une ligne distincte de sorte qu'il est facile d'analyser les données. Par exemple, exécuter `access get users -g monitor` retourne la liste des utilisateurs du moniteur avec chaque utilisateur faisant l'objet d'une ligne séparée.
- Les commandes qui retournent plusieurs colonnes (par exemple `inventory get hardware`) peuvent avoir un ensemble minimum de colonnes par défaut de défini et un argument `--verbose` permettant d'afficher toutes les colonnes. Certaines commandes incluent des arguments qui vous permettent de sélectionner des colonnes spécifiques pour la sortie.

Autres conseils pour des résultats optimaux

- Rendez externe l'ensemble des adresses IP du SP dans un fichier qui sera partagé par tous vos scripts.
- Envisagez d'utiliser un script pour créer un compte de gestionnaire initial et téléchargez sa clé publique vers vos SP.
- Testez manuellement la sortie et les codes de retour de chaque commande en utilisant SSH pour vous connecter au SP et exécuter les commandes une à une.
- Testez vos scripts sur une machine de stadification avant de les appliquer au reste des machines.
- Pour configurer tous vos SP de façon identique, envisagez de configurer un unique SP puis d'utiliser la commande `sp load settings` pour synchroniser cette configuration sur le reste des machines.

Remarque – Si le script est exécuté depuis le SP, le nombre des commandes est limité (il ne s'agit pas d'un environnement Bash complet).

Redirection de la console sur une connexion série

Rediriger l'interaction avec la console sur le port série est une autre méthode permettant à l'utilisateur de contrôler le serveur.

Le BIOS redirige la sortie de la console sur le port série par défaut (9600, 8N1, pas de handshake).

Cette section explique la configuration de ces options pour les serveurs Linux et Solaris.

Serveur basé sur Linux

Attention – Rediriger la console sur une connexion série est une procédure réservée aux seuls utilisateurs avancés de Linux.

Vous pouvez entraver sérieusement le fonctionnement du serveur ou rendre le serveur indémarrable si vous introduisez un problème dans les fichiers de configuration.

Ces configurations ont pour but de configurer le chargeur de démarrage pour rediriger sa sortie, passer au noyau les paramètres appropriés et configurer une session d'utilisateur sur le port série.

Le BIOS redirige la sortie de la console sur le port série par défaut (9600, 8N1, pas de handshake) jusqu'à ce qu'un programme chargeur de démarrage soit exécuté depuis l'unité de disque dur. Le chargeur de démarrage doit être configuré pour prendre en charge la console série en plus de la console KVM constituée par le clavier, l'écran et la souris.

Deux chargeurs de démarrage courants sont `grub` et Linux Loader (LILO).

Attention – N'éditez pas directement la section de l'image de travail de vos fichiers de configuration.

Copiez la section de l'image de travail et collez-la dans le fichier de configuration. Apportez les changements à cette section copiée.

grub

Si vous utilisez `grub`, trois étapes permettent d'activer la redirection de la console sur la connexion série ; ces étapes nécessitent toutes l'édition du fichier de configuration `grub` :

- Si vous utilisez Red Hat Linux, le fichier grub est `/etc/grub.conf`.
- Si vous utilisez SUSE Linux, le fichier grub est `/boot/grub/menu.1st`.

Remarque – Sur les systèmes Red Hat Linux, le fichier `/etc/grub.conf` peut être un lien symbolique vers le fichier `/boot/grub/grub.conf`.

---

1. Passez les paramètres de console appropriés au noyau.
2. Configurez le système de menu de grub pour que la redirection s'effectue sur la console appropriée.
3. Supprimez les éventuelles images de démarrage pouvant empêcher l'affichage adéquat de la console série

Pour plus d'informations sur les paramètres, voir le fichier `kernel-parameters.txt` dans la documentation du noyau.

Pour plus d'informations sur `grub`, exécutez la commande `info grub`.

Remarque – Si les touches fléchées ne fonctionnent pas au travers de votre concentrateur série à distance, vous pouvez utiliser les combinaisons de touches <CTRL+P> et <CTRL+N> pour mettre en surbrillance les entrées précédente et suivante, respectivement. Appuyez sur Entrée puis initialisez cette entrée.

Le paramètre `console=ttyS0` indique au système d'envoyer d'abord des données au port série. Le paramètre `console=tty0` indique au système d'envoyer ensuite les données au KVM.

Dans votre fichier de configuration grub, une section d'image de travail doit avoir une entrée pour l'initialisation de l'image du noyau. L'entrée de noyau de stock ressemble à la suivante :

`kernel /vmlinuz-`*`révision_noyau`* `ro root=/dev/sda5`

Où *révision_noyau* est simplement la version du noyau que vous utilisez.

1. **Changez l'entrée du noyau de stock de votre image de façon à inclure les paramètres de noyau de la console, comme ci-après :**

   ```
   kernel /vmlinuz-révision_noyau ro root=/dev/sda5
   console=ttyS0,9600 console=tty0
   ```

Remarque – Ces options devraient toutes figurer sur une ligne sans retour à la ligne.

---

2. **Ajoutez les deux lignes suivantes en haut de votre fichier de configuration grub :**

   ```
   serial --unit=0 --speed=9600
   terminal serial console
   ```

   Ajouter ces deux lignes au début du fichier configure votre port série ou votre KVM comme votre console `grub` ce qui vous permet de sélectionner à distance ou localement une image d'initialisation dans le menu `grub`.

3. **Mettez en commentaires ou supprimez la ligne suivante de votre fichier de configuration grub :**

   ```
   splashimage=(hd0,1)/boot/grub/splash.xpm.gz
   ```

   Supprimer la ligne `splashimage` autorise une compatibilité majeure pendant la connexion série ; lorsque cette ligne est supprimée, l'image de démarrage n'empêche pas l'affichage du menu `grub` approprié.

LILO

Remarque – Lorsque vous activez l'option du BIOS « Console Redirection After POST » et que LILO est utilisé en tant que chargeur de démarrage, le système risque de s'arrêter brusquement en affichant un « L » à l'écran.

Ce problème survient car il n'y a pas suffisamnent de mémoire inférieure disponible pour charger le fichier d'initialisation de deuxième stade que LILO utilise. Si vous désactivez l'option « Console Redirection After POST » dans le BIOS, le système s'initialisera normalement. Voir « Activation et désactivation de la redirection de la console du BIOS », page 119.

Si vous avez besoin de l'option « Console Redirection after POST », utilisez `grub` ou effectuez une mise à niveau vers une version plus récente de LILO. La version courante de LILO est la 22.5.9 ; pour accéder aux pages de LILO, visitez `http://lilo.go.dyndns.org/` et cliquez sur le lien.

Avant de procéder à la mise à niveau, nous vous recommandons de vérifier auprès du vendeur de votre SE si la version mise à jour de LILO est prise en charge.

Transmission des paramètres appropriés au noyau

LILO utilise la fonction `append` dans une section d'image pour transmettre au noyau les paramètres appropriés pour utiliser la console série.

1. **Dans le fichier** `/etc/lilo.conf` **de votre serveur Sun Fire V20z ou V40z, entrez les consoles dans l'instruction** `append` **:**

   ```
   append="console=ttyS0,9600 console=tty0"
   ```

2. **Après avoir modifié le fichier** `/etc/lilo.conf`**, exécutez** `lilo` **depuis la ligne de commande pour activer le changement.**

   Pour plus d'informations sur LILO; exécutez les commandes `man lilo` ou `man lilo.conf`.

getty

Vous pouvez exécuter un service appelé `getty` pour activer la connexion sur l'interface série.

Pour activer `getty`, ajoutez la ligne suivante à la liste `gettys` du fichier `/etc/inittab` :

```
7:12345:respawn:/sbin/agetty 9600 ttyS0
```

Remarque – L'endroit où vous ajoutez cette ligne dans la liste n'a pas d'importance.

Remarque – Assurez-vous que le premier numéro est unique dans le fichier `inittab`.

La liste de `gettys` ressemble actuellement à la suivante :

```
# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6
```

securetty

Pour ajouter le périphérique de console série `/dev/ttyS0` au fichier /etc/securetty, exécutez la commande suivante :

```
# echo ttyS0 >> /etc/securetty
```

Serveur basé sur Solaris

Attention – Rediriger la console sur une connexion série est une procédure réservée aux seuls utilisateurs avancés de Solaris.

Vous pouvez entraver sérieusement le fonctionnement du serveur ou rendre le serveur indémarrable si vous introduisez un problème dans le fichier `bootenv.rc`.

Remarque – Le paramètre de périphérique de sortie par défaut est `screen` et celui du périphérique d'entrée `keyboard`.

Pour changer les paramètres

Pour activer la redirection de la console sur une connexion série sur un serveur Solaris :

- **Dans une fenêtre de terminal, exécutez la commande `eeprom` pour changer les paramètres pour les périphériques de sortie et d'entrée, comme indiqué ici.**

```
eeprom output-device=ttya
eeprom input-device=ttya
```

Pour vérifier les paramètres

Pour vérifier si les changements ont été effectués :

1. **Dans une fenêtre de terminal, exécutez la commande `eeprom` sans argument.**

   Le contenu du fichier `bootenv.rc` s'affiche dans la fenêtre de terminal.

2. **Localisez les lignes suivantes et vérifiez si les valeurs correctes sont affichées.**

```
output-device=ttya
input-device=ttya
```

Pour rétablir les paramètres par défaut

Pour rétablir les paramètres par défaut du système :

- **Pour rétablir les paramètres par défaut pour les périphériques d'entrée et de sortie, exécutez la commande** `eeprom` **avec les arguments suivants.**

```
eeprom output-device=screen
eeprom input-device=keyboard
```

Activation et désactivation de la redirection de la console du BIOS

Remarque – La redirection de la console est activée par défaut dans le BIOS.

Si les paramètres par défaut ont été modifiés dans le BIOS, la procédure suivante permet de changer les paramètres de redirection de la console.

1. **Démarrez ou redémarrez le serveur.**
2. **À l'invite, appuyez sur la touche <F2> pour entrer dans l'utilitaire BIOS Setup.**
3. **Sélectionnez le menu Advanced dans les sélections de catégories dans la partie supérieure.**
4. **Sélectionnez Console Redirection.**

Remarque – Notez tous les paramètres du menu tels qu'ils sont requis pour configurer l'accès à distance à la console et la fonction SOL (Serial-Over-LAN).

   - Pour désactiver la redirection de la console sur la connexion série, sélectionnez Disabled depuis l'option Com Port Address.
   - Pour changer la vitesse de transmission en bauds, sélectionnez le débit de bits de votre choix pour l'option Baud Rate.
   - Pour désactiver Continue C.R. after POST, faites basculer le paramètre sur OFF.
5. **Enregistrez les changements apportés aux paramètres du BIOS.**
6. **Appuyez sur <F10> pour quitter la configuration du BIOS.**

Pour que les nouveaux paramètres soient appliqués, vous devez redémarrer le serveur.

CD-ROM Network Share Volume (NSV)

Une structure NSV figure sur le CD Network Share Volume des serveurs Sun Fire V20z et Sun Fire V40z.

Bien que le SP fonctionne normalement sans accès à un système de fichiers externe, un système de fichiers est requis pour activer plusieurs fonctions, dont les fichiers journaux d'événements, les mises à jour du logiciel, les diagnostics et l'utilitaire de vidage de dépannage. Vous pouvez configurer le NSV pour qu'il soit partagé par plusieurs SP. Les utilisateurs de niveau administratif et gestionnaire peuvent configurer le système de fichiers externe tandis que les utilisateurs normaux peuvent uniquement afficher la configuration courante.

Les composants logiciels suivants sont inclus avec le serveur :

- BIOS de la plate-forme
- le logiciel de base du SP
- le logiciel à valeur ajoutée du SP
- le fichier de mise à jour pour le téléchargement des packages du Java Runtime Environment (JRE)
- le logiciel NVS, diagnostics inclus
- le logiciel de la plate-forme
- les pilotes de plate-forme de la carte mère

Tous ces packages sont fournis avec le NSV et sont installés sur le serveur de fichiers lorsque le système de fichiers externe est installé et configuré.

Pour plus d'informations sur l'extraction et l'installation du logiciel NVS, voir le *Serveurs Sun Fire V20z et Sun Fire V40z — Guide d'installation*.

Structure de NVS

Le TABLEAU 4-1 liste les packages compressés qui sont inclus sur le CD-ROM Network Share Volume des serveurs Sun Fire V20z et Sun Fire V40z.

TABLEAU 4-1 Packages compressés du CD-ROM NVS

Nom du fichier	Contenu du fichier
`nsv_V2_2_0_x.zip`	Diagnostics du SP et de la plate-forme avec une prise en charge pour le logiciel SP
`nsv-redhat_V2_2_0_x.zip`	Pilotes pour le SE Red Hat Linux
`nsv-solaris_V2_2_0_x.zip`	Pilotes pour le SE Solaris 9 et le SE Solaris 10
`nsv-suse_V2_2_0_x.zip`	Pilotes pour le SE SUSE Linux

Une fois extraits, les packages compressés du TABLEAU 4-1 remplissent les répertoires suivants sur le NSV :

```
/mnt/nsv/
diags
logs
scripts
snmp
update_server
sw_images (ce dossier apparaît une fois que vous avez extrait l'un des fichiers .zip spécifiques des SE)
```

TABLEAU 4-2 Fichiers extraits sur NVS

Nom du fichier	Description
`diags`	Emplacement hors ligne des diagnostics du serveur.
`logs`	Emplacement hors ligne des fichiers journaux du SP.
`scripts`	Exemples de scripts qui peuvent être utilisés pour écrire des scripts pour les commandes.
`snmp`	MIB SNMP. Voir le Chapitre 3 pour plus de détails.
`update_server`	Application permettant de mettre à jour le logiciel du SP et le BIOS. Voir le Chapitre 1 pour plus de détails.
`sw_images`	Contient une hiérarchie de répertoires de composants de la plate-forme et du SP, incluant des sous-répertoires pour chaque version.

Serial Over LAN

La fonction SOL (Serial Over LAN) permet aux serveurs de rediriger de façon transparente le flux de caractères série provenant de l'UART de la carte de base vers et depuis le système client distant sur le LAN. Cette fonction présente les avantages suivants par rapport à une interface série :

- Elle élimine le besoin d'un concentrateur série ;
- Elle réduit la quantité de câbles ;
- Elle permet la gestion à distance des serveurs sans écran, clavier ni souris (serveurs sans écran).

SOL requiert une connexion LAN correctement configurée et une console depuis laquelle établir une session `ssh`.

Dans un environnement Linux, vous pouvez utiliser un shell tel que `csh` ou `ksh` comme console. Cette console fonctionne bien dans un environnement utilisant des scripts dans lequel vous pouvez vouloir contrôler de nombreux serveurs.

Activation ou désactivation de la fonction SOL sur le serveur

---

Remarque – Quand la fonction SOL est activée, vous ne pouvez pas accéder au serveur par le biais du port série DB9 externe (COM A).

Remarque – La variable *utilisateursp* est le compte d'utilisateur créé lors de la sécurisation du SP. La variable *adripsp* est l'adresse IP attribuée au SP.

Pour plus d'informations, voir « Configuration initiale du SP », page 14.

Vous pouvez activer ou désactiver la fonction SOL par le biais du SP.

Activation de la fonction SOL

Pour activer la fonction, exécutez la commande suivante :

```
# ssh -l utilisateursp adripsp platform set console -s sp -e -S 9600
```

Remarque – Vérifiez si la valeur de la vitesse de transmission en bauds transmise à l'argument `-S` correspond à la vitesse qui a été spécifiée pour la fonction de redirection série du BIOS et à la vitesse utilisée pour votre chargeur de démarrage et la configuration du SE.

La vitesse de transmission en bauds par défaut dans les paramètres du BIOS est 9 600.

Désactivation de la fonction SOL

Pour désactiver la fonction, exécutez la commande suivante :

```
# ssh -l utilisateursp adripsp platform set console -s platform
```

Lancement d'une session SOL

Pour lancer une session SOL, exécutez la commande suivante :

```
# ssh adripsp -l utilisateursp platform console
```

Arrêt d'une session SOL

Pour arrêter une session SOL :

1. **Appuyez sur Ctrl-e.**
2. **Appuyez sur la touche « c ».**
3. **Appuyez sur la touche du point « . ».**

Vous pouvez aussi mettre fin à une session SOL en arrêtant la session `ssh` :

1. **Appuyez sur Entrée.**
1. **Appuyez sur la touche du tilde « ~ ».**
2. **Appuyez sur la touche du point « . ».**

Séquences d'échappement pour le terminal de console distant

Si vous accédez au serveur en utilisant un terminal de console distant, il est possible que vous deviez utiliser les séquences d'échappement figurant dans le TABLEAU 4-3. Si l'une des touches de fonction courantes ne fonctionne pas correctement, utilisez la séquence d'échappement qui la suit dans le tableau.

Vous aurez très certainement à utiliser les séquences d'échappement si vous utilisez un SE Linux ou Solaris.

TABLEAU 4-3 Touches spéciales pour le terminal de console distant

Touche de fonction	Séquence d'échappement
ORIGINE	<ÉCHAP> h
FIN	<ÉCHAP> k
TOUCHE D'INSERTION	<ÉCHAP> +
TOUCHE DE SUPPRESSION	<ÉCHAP> -
PAGE PRÉCÉDENTE	<ÉCHAP> ?
PAGE SUIVANTE	<ÉCHAP> /
ALT	<ÉCHAP>^A
CTRL	<ÉCHAP>^C
F1	<ÉCHAP> 1
F2	<ÉCHAP> 2
F3	<ÉCHAP> 3
F4	<ÉCHAP> 4
F5	<ÉCHAP> 5
F6	<ÉCHAP> 6
F7	<ÉCHAP> 7
F8	<ÉCHAP> 8
F9	<ÉCHAP> 9
F10	<ÉCHAP> 0
F11	<ÉCHAP> !
F12	<ÉCHAP> @

ANNEXE **A**

Récapitulatif des commandes de gestion de serveurs

Le SP inclut une suite de commandes qui permettent la gestion et le contrôle du serveur, à laquelle il est fait référence comme aux commandes de gestion de serveurs.

Remarque – Cette annexe présente l'ensemble des groupes de commandes de gestion de serveurs disponibles sur le SP. Pour la description détaillée des sous-commandes, des arguments et des codes de retour de chaque type de commandes, reportez-vous aux annexes de ce guide, comme indiqué dans le TABLEAU A-1.

Utilisation du protocole `ssh`

Vous devez utiliser `ssh` pour exécuter ces commandes sur le SP. Il y a deux manières d'effectuer cela :

- utiliser le shell interactif sur le SP ;
- faire précéder chaque commande d'un morceau de texte défini ou préface.

Shell interactif du SP

Pour utiliser le shell interactif :

- **Connectez-vous et authentifiez-vous sur le shell interactif en exécutant la commande suivante :**

  # **`ssh -l`** *adripsp utilisateursp*

Texte de préface

- **Faites précéder chaque commande du texte suivant :**

  # **`ssh -l`** *adripsp utilisateursp*

Commandes

Les commandes de gestion de serveurs acceptent des arguments, effectuent une ou plusieurs actions et affichent le résultat ou du texte sur le périphérique de sortie standard. Les commandes sont regroupés par fonction, chaque commande possède de nombreuses sous-commandes prenant en charge les fonctions du regroupement en question.

Remarque – Chaque sous-commande (à l'exception de `help`) retourne un ou plusieurs codes de retour à la fin de l'opération. Pour un récapitulatif, voir « Codes de retour », page 129.

Le TABLEAU A-1 liste les groupes de commandes de gestion de serveurs.

TABLEAU A-1 Commandes de gestion de serveurs

Groupe de commandes	Description
access	Permet à l'utilisateur autorisé de gérer et de contrôler les fonctions de contrôle d'accès et de sécurité du SP, telles que les utilisateurs, les groupes, SSL, etc. **Voir l'Annexe B « Commandes d'accès ».**
diags	Gère les tests de diagnostic qui sont inclus avec votre serveur. **Voir l'Annexe C « Commandes de diagnostic ».**
Inventaire	Permet à l'utilisateur autorisé de contrôler les informations d'inventaire du matériel et des logiciels. **Voir l'Annexe D « Commandes d'inventaire ».**
ipmi	Gère les fonctions IPMI. **Voir l'Annexe E « Commandes IPMI ».**
Plate-forme	Permet à l'utilisateur autorisé de gérer et de contrôler les activités de la plate-forme, telle que le redémarrage du système d'exploitation de la plate-forme, le recueil du statut du système, etc. **Voir l'Annexe F « Commandes de la plate-forme ».**

TABLEAU A-1 Commandes de gestion de serveurs *(suite)*

Groupe de commandes	Description
sensor	Rapporte ou définit la valeur d'un capteur ou d'un dispositif de contrôle environnemental. **Voir l'Annexe G « Commandes relatives aux capteurs ».**
sp	Permet à l'utilisateur autorisé de gérer et de contrôler les configurations du SP, telles que l'interconnexion en réseau, le système de fichiers externe, SNMP, SMTP, SSL, les journaux d'événements, etc. **Voir l'Annexe H « Commandes du processeur de service ».**
help	Retourne le texte suivant : `Available Commands: platform, access, sp, sensor, inventory, ipmi. Each of these commands includes a help option (--help).`

Codes de retour

Chaque sous-commande retourne un ou plusieurs des codes de retour suivants à la fin de l'opération. Reportez-vous aux annexes suivantes de ce guide de l'utilisateur pour connaître les différentes sous-commandes et les codes de retour correspondants.

Le TABLEAU A-2 liste les codes de retour pour les commandes de gestion de serveurs.

TABLEAU A-2 Codes de retour *(1 de 2)*

Code de retour	ID	Description
NWSE_Success	0	La commande a réussi.
NWSE_InvalidUsage	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
NWSE_RPCTimeout	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
NWSE_RPCNotConnected	3	Connexion au serveur RPC impossible.
NWSE_InvalidArgument	4	Un ou plusieurs arguments étaient incorrects ou invalides.
NWSE_NotFound	5	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
NWSE_NoPermission	6	Pas autorisé à effectuer cette opération.
NWSE_MissingArgument	7	Argument(s) manquant(s).
NWSE_NoMemory	8	Mémoire insuffisante.
NWSE_Busy	9	Périphérique ou ressource occupé.
NWSE_NotImplemented	10	Fonction pas implémentée.
NWSE_RPCConnected	11	Client RPC déjà connecté.
NWSE_RPCConnRefused	12	Connexion RPC refusée.
NWSE_NoRouteToHost	13	Pas de route vers l'hôte (réseau hors service).
NWSE_HostDown	14	Hôte hors service.
NWSE_UnknownError	15	Erreur de type divers pas capturée par d'autres erreurs.
NWSE_GatewayOffNet	16	L'adresse de la passerelle n'est pas sur le réseau.
NWSE_NetMaskIncorrect	17	Un masque de réseau inapproprié a été spécifié.

TABLEAU A-2 Codes de retour *(2 de 2) (suite)*

Code de retour	ID	Description
NWSE_FileError	18	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.
NWSE_Exist	19	Entité (utilisateur, service ou autre) déjà présente.
NWSE_NotRecognized	20	Requête non-comprise.
NWSE_NotMounted	21	Le système de fichiers n'est pas monté.
NWSE_InvalidOpForState	22	Opération incorrecte pour l'état courant.
NWSE_TimedOut	23	Opération arrivée à échéance.
NWSE_ServiceNotAvailable	24	Le service demandé n'est pas disponible.
NWSE_DeviceError	25	Impossible de lire ou d'écrire sur le périphérique.
NWSE_LimitExceeded	26	Limite dépassée.

ANNEXE **B**

Commandes d'accès

La commande `access` valide les pouvoirs d'un utilisateur ou contrôle les services d'autorisation. Elle vous permettra d'obtenir des informations sur les groupes d'utilisateurs, d'ajouter un utilisateur à un groupe ou de l'en supprimer et de spécifier un mappage entre les groupes administratifs définis sur le site et ceux employés pour autoriser des actions sur le processeur de service.

Remarque – Le TABLEAU B-1 liste les groupes de sous-commandes de la commande `access`. Chaque sous-commande retourne un code de retour à la fin de l'opération.

TABLEAU B-1 Groupes de sous-commandes d'accès

Groupe de sous-commandes	Description
`access config-sharing`	Contrôle le partage de la configuration pour procéder à la configuration automatique.
`access groups`	Retourne le groupe d'autorisations pour un utilisateur spécifique ou une liste de groupes définis.
`access map`	Mappe, annule un mappage et retourne la liste des noms des groupes spécifiés du site (le groupe du service d'annuaire) mappés vers l'un des groupes administratifs standard.
`access public key`	Gère les clés publiques et les utilisateurs des clés publiques.
`access services`	Active, désactive ou définit un mécanisme de services d'annuaire qui détermine l'appartenance d'un utilisateur à un groupe.
`access trust`	Crée une relation de confiance basée sur l'hôte pour l'hôte spécifié.
`access user`	Gère les utilisateurs locaux ou un groupe d'utilisateurs.

Sous-commandes d'accès relatives à config-sharing

Les sous-commandes du TABLEAU B-2 contrôlent la fonction de partage de configuration. Cette fonction est requise pour la configuration automatique.

TABLEAU B-2 `Sous-commandes d'accès relatives à config-sharing`

Sous-commande	Description
`access enable config-sharing`	Autorise le SP à être une source de paramètres de configuration pour d'autres SP.
`access diable config-sharing`	Empêche le SP d'être une source de paramètres de configuration pour d'autres SP.
`access get config-sharing`	Retourne la valeur du paramètre de partage de configuration.

Sous-commande access enable config-sharing

Description : Cette commande est exécutée sur le SP. Elle permet à un SP d'être une source de paramètres de configuration pour d'autres SP. Une fois le paramètre de partage de configuration activé sur un SP, tout autre SP ayant un accès réseau au premier serveur peut répliquer les paramètres de configuration du premier serveur.

Format

```
access enable config-sharing
```

Codes de retour

Le TABLEAU B-3 liste les codes de retour pour cette sous-commande.

TABLEAU B-3 Codes de retour de la sous-commande `access enable config-sharing`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

Sous-commande access disable config-sharing

Description : Cette commande est exécutée sur le SP. Elle empêche un SP d'être une source de paramètres de configuration pour d'autres SP.

Format

```
access disable config-sharing
```

Codes de retour

Le TABLEAU B-4 liste les codes de retour pour cette sous-commande.

TABLEAU B-4 Codes de retour de la sous-commande `access disable config-sharing`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.

Sous-commande access get config-sharing

Description : Cette commande retourne la valeur du paramètre de partage de configuration.

Format

```
access get config-sharing
```

Valeurs

Le TABLEAU B-5 liste les valeurs pour cette sous-commande.

TABLEAU B-5 Valeurs de la sous-commande `access get config-sharing`

Valeur	Description
`Enabled`	Autorise le partage des paramètres de configuration. Le SP est une source de paramètres de configuration pour d'autres SP.
`Disabled`	Empêche le partage des paramètres de configuration. Le SP ne peut pas devenir une source de paramètres de configuration pour d'autres SP.

Codes de retour

Le TABLEAU B-6 liste les codes de retour pour cette sous-commande.

TABLEAU B-6 Codes de retour pour la sous-commande `access get config-sharing`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

Sous-commandes d'accès relatives aux groupes

Les sous-commandes du TABLEAU B-7 retournent le groupe d'autorisations pour un utilisateur spécifique ou une liste de groupes définis.

TABLEAU B-7 `Sous commandes de groupes d'accès`

Sous-commande	Description
`access get group`	Retourne le groupe d'autorisations pour l'utilisateur spécifié.
`access get groups`	Retourne la liste des groupes définis, groupes standard inclus.

Sous-commande access get group

Description : Retourne le groupe d'autorisations pour l'utilisateur spécifié.

Format

```
access get group
```

Codes de retour

Le TABLEAU B-8 liste les codes de retour pour cette sous-commande.

TABLEAU B-8 Codes de retour de la sous-commande `access get group`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_NotFound`	`5`	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.

Sous-commande access get groups

Description : Retourne la liste des groupes définis, groupes standard inclus.

Format

```
access get groups
```

Codes de retour

Le TABLEAU B-9 liste les codes de retour pour cette sous-commande.

TABLEAU B-9 Codes de retour de la sous-commande `access get groups`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.

Sous-commandes d'accès relatives au mappage

Les sous-commandes du TABLEAU B-10 gèrent les mappages entre les groupes existants spécifiés du site et un des groupes administratifs standard.

TABLEAU B-10 `Sous-commandes d'accès relatives au mappage`

Sous-commande	Description
`access get map`	Retourne les noms de tous les groupes spécifiés du site mappés à un groupe administratif spécifique.
`access map`	Mappe un nom de groupe spécifié de site existant (le groupe de service d'annuaire) vers l'un des groupes administratifs standard.
`access unmap`	Supprime le mappage entre le groupe du service d'annuaire et le groupe administratif.

Sous-commande access get map

Description : Retourne les noms de tous les groupes spécifiés du site mappés vers un groupe administratif spécifique.

Format

```
access get map [{-H | --noheader}]
[{-D | --Delim <SÉPARATEUR>}]
```

Remarque – Pour retourner les mappages pour tous les groupes, n'indiquez pas de nom de groupe sur la ligne de commande.

Le TABLEAU B-11 liste les arguments pour cette sous-commande.

TABLEAU B-11 Arguments de la sous-commande `access get map`

Argument	Description
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU B-12 liste les codes de retour pour cette sous-commande.

TABLEAU B-12 Codes de retour de la sous-commande `access get map`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.

Sous-commandes access map

Description : mappe un nom de groupe spécifié de site existant (le groupe de services d'annuaire) vers l'un des groupes administratifs standard.

Format

```
access map {-d | --dsgroup} GROUPE-RÉPERTOIRES-SERVICES
{-g | --group} GROUPE-LOCAL {-v | --verify}
```

Le TABLEAU B-13 liste les arguments de cette sous-commande.

TABLEAU B-13 Arguments de la sous-commande `access map`

Argument	Description
`{-d | --dsgroup}`	Nom du groupe de services d'annuaire pour lequel vous voulez effectuer le mappage vers un groupe administratif standard.
`{-g | --group}`	Nom du groupe administratif standard vers lequel vous voulez mapper le groupe de services d'annuaire.
`{-v | --verify}`	Vérifie l'existence du groupe.

Codes de retour

Le TABLEAU B-14 liste les codes de retour pour cette sous-commande.

TABLEAU B-14 Codes de retour de la sous-commande `access map`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NotFound`	`5`	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_InvalidOpForState`	`22`	Opération incorrecte pour l'état courant.

Sous-commande access unmap

Description : Supprime le mappage entre le groupe du service d'annuaire et le groupe administratif.

Format

```
access unmap [-a | --all] GROUPE-SERVICES-ANNUAIRE
```

Le TABLEAU B-15 liste les arguments de cette sous-commande.

TABLEAU B-15 Arguments de la sous-commande `access unmap`

Argument	Description
`GROUPE-SERVICES-ANNUAIRE`	Nom du groupe de services d'annuaire pour lequel vous voulez annuler un mappage.
`[-a | --all]`	Supprime les mappages pour tous les groupes de services d'annuaire.

Codes de retour

Le TABLEAU B-16 liste les codes de retour pour cette sous-commande.

TABLEAU B-16 Codes de retour de la sous-commande `access unmap`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

Sous-commandes d'accès relatives aux services d'annuaire

Définit un mécanisme de services d'annuaire qui détermine l'appartenance d'un utilisateur à un groupe. Les utilisateurs distants accèdent aux fonctions du SP uniquement au travers des mappages de groupes qui lient un groupe de service d'annuaire à un groupe administratif du SP local.

Par conséquent, en utilisant la commande `access map`, l'administrateur doit définir la configuration de services d'annuaire appropriée et créer des mappages entre les groupes des services d'annuaire et les groupes administratifs du SP local.

Le TABLEAU B-17 liste les sous-commandes de `Access Directory Services`.

TABLEAU B-17 Sous-commandes `Access Directory Services`

Sous-commande	Description
`access disable service`	Désactive un service d'annuaire.
`access enable service`	Active un service d'annuaire.
`access get services`	Définit un mécanisme de services d'annuaire qui détermine l'appartenance d'un utilisateur à un groupe.

Sous-commande access disable service

Description : désactive un service d'annuaire (NIS ou ADS) du système de recherche de services de noms sur le SP.

Format

```
access disable service {nis | ads}
```

Le TABLEAU B-18 liste les arguments pour cette sous-commande.

TABLEAU B-18 Arguments de la sous-commande `access disable service`

Argument	Description
`{nis	ads }`	Spécifie le type du service : NIS ou ADS.

Codes de retour

Le TABLEAU B-19 liste les codes de retour pour cette sous-commande.

TABLEAU B-19 Codes de retour de la sous-commande `access disable service`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	4	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.
`NWSE_InvalidOpForState`	22	Opération incorrecte pour l'état courant.

Sous-commande access enable service

Description : active un service d'annuaire (NIS ou ADS) pour le système de recherche de services de noms sur le SP.

Format

```
access enable service NIS {-d | --domain} NOM DOMAINE {-s | --server
} SERVEUR
```

```
access enable service ADS {-d | --domain} NOM DOMAINE {-s | --server
} SERVEUR {-k | --keytab} NOMFICHIER KEYTAB {-o | --ou} UNITÉ
ORGANISATIONNELLE {-l|--logon} CONNEXION
```

Le TABLEAU B-20 liste les arguments de cette sous-commande.

TABLEAU B-20 Arguments de la sous-commande `access enable service`

Argument	Description
`{-d | --domain}`	Spécifie le nom du domaine.
`{-s | --server}`	Spécifie le serveur.
`{-k | --keytab}`	Pour ADS uniquement : spécifie le nom du fichier keytab d'ADS.
`{-o | --ou}`	Pour ADS uniquement : spécifie l'unité organisationnelle sous laquelle la bibliothèque du service d'attribution de noms recherche les données du groupe.
`{-l | --logon}`	Pour ADS uniquement : spécifie l'ID d'ouverture de sessions pour le compte d'annuaire actif.

Pour utiliser ADS en tant que service d'annuaire sur le SP, vous devez créer un compte d'annuaire actif. La bibliothèque du service d'attribution de noms sur le SP utilise ce compte pour s'authentifier auprès de l'interface LDAP du serveur d'annuaire actif. Un administrateur Windows pourra créer le keytab pour ce compte en utilisant la commande suivante :

```
ktpass -princ <connexion>@<domaine> -pass <motpasse> -mapuser
<connexion> -out <nomfichier sortie>
```

Le fichier keytab doit être transféré de façon sécurisée au SP en utilisant un mécanisme de transfert de fichiers chiffré.

L'horloge du SP doit être exacte et DNS doit être installé (ce qui signifie que le SP doit avoir un enregistrement DNS).

Si un service d'annuaire a été activé au préalable, vous pouvez spécifier les commandes et options suivantes ; les paramètres enregistrés seront ensuite utilisés pour réactiver le service.

```
access enable service -t <nis | ads>
```

Codes de retour

Le TABLEAU B-21 liste les codes de retour pour cette sous-commande.

TABLEAU B-21 Codes de retour de la sous-commande `access enable service`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	4	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NotFound`	5	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.
`NWSE_FileError`	18	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.
`NWSE_InvalidOpForState`	22	Opération incorrecte pour l'état courant.

Sous-commande access get services

Description : retourne une chaîne contenant l'option de service d'attribution de noms courante (NIS ou ADS).

Format

```
access get services [ {-t | --type } NIS
[{-d | --domain} | {-s | --server}]
[-H | --noheader]] [{-D | --Delim <SÉPARATEUR>}]

access get services [ {-t | --type } ADS
[{ -d | --domain} | {-s | --server} |
{-l | --logonID} | {-o | --ou}]
[-H | --noheader]] [{-D | --Delim <SÉPARATEUR>}
```

Le TABLEAU B-22 liste les arguments de cette sous-commande.

TABLEAU B-22 Arguments de la sous-commande `access get services`

Argument	Description
`{-t | --type }`	Retourne les informations relatives à la configuration du service NIS ou ADS. Vous devez spécifier `-t` pour obtenir la liste des services activés.
`{-d | --domain}`	Retourne les informations relatives au domaine. Un seul des paramètres `-d` et `-s` est autorisé à la fois.
`{-s | --server}`	Retourne les informations relatives au serveur. Un seul des paramètres `-d` et `-s` est autorisé à la fois.
`{-l | --ID}`	Pour ADS uniquement : retourne l'ID d'ouverture de session d'ADS. Un seul des paramètres `-o` et `-l` est autorisé à la fois.
`{-o | --ou}`	Pour ADS uniquement : retourne les informations relatives à l'unité organisationnelle. Un seul des paramètres `-o` et `-l` est autorisé à la fois.
`[-H | --noheader]`	Supprime les titres de la sortie.
`{-D | --Delim` *<SÉPARATEUR>*`}`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU B-23 liste les codes de retour pour cette sous-commande.

TABLEAU B-23 Codes de retour de la sous-commande `access get services`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.

Sous-commandes d'accès relatives à la confiance

Ajouter des relations de confiance basées sur l'hôte fournit des solutions d'écriture de scripts de type plusieurs à un. Une fois une relation d'équivalence d'hôte créée avec un client, les utilisateurs de ce client peuvent exécuter à distance des commandes sur le SP sans être invités à entrer de mot de passe.

Le TABLEAU B-24 liste les commandes liées aux relations d'hôte de confiance.

TABLEAU B-24 Sous-commandes de `access trust`

Sous-commande	Description
`access add trust`	Crée une relation de confiance basée sur l'hôte pour l'hôte spécifié.
`access delete trust`	Supprime une relation de confiance basée sur l'hôte pour l'hôte spécifié.
`access get trusts`	Demande une liste des hôtes engagés dans des relations de confiance avec le SP.

Sous-commande access add trust

Description : Crée une relation de confiance basée sur l'hôte pour l'hôte spécifié. Ajouter des relations de confiance basées sur l'hôte fournit des solutions d'écriture de scripts de type plusieurs à un. Une fois une relation d'équivalence d'hôte créée avec un client, les utilisateurs de ce client peuvent exécuter à distance des commandes sur le SP sans être invités à entrer de mot de passe, du moment que l'une des conditions suivantes est remplie :

- Leur nom de connexion sur le client est identique à celui d'un utilisateur local sur le SP.
- Leur connexion sur le client se trouve dans un groupe de services d'annuaire qui est mappé vers un groupe administratif du SP.

Format

`access add trust {-c | --client}` *`HÔTE`* `{-k | --keyfile}` *`FICHIER CLÉ PUBLIQUE`*

Le TABLEAU B-25 liste les arguments de cette sous-commande.

TABLEAU B-25 Arguments de la sous-commande `access add trust`

Argument	Description
`{-c | --client}`	Spécifie l'hôte pour lequel la relation va être créée.
`{-k | --keyfile}`	Spécifie le fichier de clé publique.

Si la connexion est autorisée par le biais du mappage d'un groupe de services d'annuaire, la commande -service group, the `ssh` est exécutée en tant qu'utilisateur proxy sur le SP : au choix *rmonitor*, *radmin* ou *rmanager*.

La prise en charge est disponible uniquement pour les types de clés de la version 2 du protocole SSH (RSA ou DSA).

Si DNS est activé sur le SP, la machine cliente doit être spécifiée par son nom DNS (pas par son adresse IP).

Génération de clés d'hôte

L'installation `ssh` de l'hôte devrait générer les clés d'hôte. Si ce n'est pas le cas, suivez ces étapes pour générer manuellement la paire de clés :

1. **Entrez la commande suivante :**

   ```
   ssh-keygen -q -t rsa -f rsa_key -C '' -N ''
   ```

2. **Copiez** `rsa_key` **dans** `/etc/ssh/ssh_host_rsa_key`**.**

3. **Assurez-vous que seul l'utilisateur *root* a des permissions de lecture ou d'écriture dans ce fichier. Le fichier** `rsa_key.pub` **est le fichier que vous transférerez au SP.**

Remarque – Seuls les types de clé de la version 2 du protocole et les tailles de clé de 1024 bits (la clé par défaut générée par `ssh-keygen`) sont pris en charge.

---

4. **Copiez la clé publique de l'hôte (le fichier** `rsa_key.pub`**) sur le SP en utilisant** `scp` **(copie sécurisée) ou en copiant la clé de l'hôte sur un système de fichiers externe qui a été monté sur le SP.**

Remarque – Utilisez `scp` pour copier les fichiers dans le répertoire `/tmp` ou dans votre répertoire personnel. Les commandes sp installeront ensuite le fichier spécifié sur le ligne de commande en `/pstore`.

Remarque – Si DNS est activé sur le SP, vous devez spécifier le client qui est utilisé dans les commandes de confiance par son nom DNS (pas par son adresse IP).

Codes de retour

Le TABLEAU B-26 liste les codes de retour pour cette sous-commande.

TABLEAU B-26 Codes de retour de la sous-commande `access add trust`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_FileError`	`18`	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.
`NWSE_Exist`	`19`	Entité (utilisateur, service ou autre) déjà présente.

Sous-commande access delete trust

Description : Supprime une relation de confiance basée sur l'hôte pour l'hôte spécifié.

Format

`access delete trust` *`NOMHÔTE CLIENT`* `[-a | --all] [-q | --quiet]`

Le TABLEAU B-27 liste les arguments de cette sous-commande.

TABLEAU B-27 Arguments de la sous-commande `access delete trust`

Argument	Description
`NOMHÔTE CLIENT`	Spécifie le nom du client à supprimer.
`[-a | --all]`	Supprime toutes les relations de confiance.
`[-q | --quiet]`	Cet argument spécifie qu'aucune erreur ne sera retournée si la relation de confiance à supprimer est introuvable.

Codes de retour

Le TABLEAU B-28 liste les codes de retour pour cette sous-commande.

TABLEAU B-28 Codes de retour de la sous-commande `access delete trust`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_NotFound`	`5`	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_DeviceError`	`25`	Erreur lors de la suppression de l'hôte de confiance. Espace insuffisant dans `/tmp`.

Sous-commande access get trusts

Description : Demande une liste des hôtes engagés dans des relations de confiance avec le SP.

Format

```
access get trusts
```

Codes de retour

Le TABLEAU B-29 liste les codes de retour pour cette sous-commande.

TABLEAU B-29 Codes de retour de la sous-commande `access get trusts`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.

Sous-commandes d'accès relatives aux clés publiques

Les sous-commandes listées dans le TABLEAU B-30 vous permettent de gérer les clés publiques et leurs utilisateurs.

TABLEAU B-30 Sous-commandes d'accès relatives aux clés publiques

Sous-commande	Description
`access add public key`	Installe une clé publique pour l'authentification SSH.
`access get public key users`	Détermine les utilisateurs qui ont des clés publiques installées.
`access delete public key`	Supprime la clé publique d'un utilisateur.

Sous-commande access add public key

Description : installe une clé publique pour l'authentification SSH, qui autorise les connexions SSH et l'exécution de commandes à distance sans demander de mot de passe. Vous devez d'abord générer une paire de clés (RSA ou DSA), ce qui peut être fait en utilisant la commande `ssh-keygen` incluse dans OpenSSH.

- Seuls les utilisateurs locaux peuvent installer des clés publiques (pas les utilisateurs qui obtiennent une autorisation par le mappage d'un groupe de services d'annuaire) ;
- Les gestionnaires peuvent ajouter des clés publiques pour tout utilisateur local ;
- Un maximum de 10 utilisateurs peuvent installer des clés publiques ; une seule clé est autorisée par utilisateur ;
- La longueur de clé maximale prise en charge est de 4 096 bits.

Format

`access add public key {-k | --keyfile}` *`FICHIER_CLÉ_PUBLIQUE`* `[-u | --user]` *`UTILISATEUR`*

Le TABLEAU B-31 liste les arguments de cette sous-commande.

TABLEAU B-31 Arguments de la sous-commande `access add public key`

Argument	Description
`{-k | --keyfile}`	Supprime la clé publique RSA ou DSA de l'utilisateur.
`{-u | --user}`	Spécifie l'utilisateur pour lequel la clé en question va être installée. La valeur par défaut est l'utilisateur courant si aucun utilisateur n'est spécifié.

Codes de retour

Le TABLEAU B-32 liste les codes de retour pour cette sous-commande.

TABLEAU B-32 Codes de retour de la sous-commande `access add public key`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	4	Un ou plusieurs arguments étaient incorrects ou invalides. Le groupe spécifié par -g est un groupe administratif invalide du SP local ou la longueur du nom de l'utilisateur ou du mot de passe dépasse la longueur maximale.
`NWSE_NotFound`	5	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.
`NWSE_Exist`	19	L'utilisateur existe déjà.
`NWSE_LimitExceeded`	26	Limite dépassée.

Sous-commande access get public key users

Description : Détermine les utilisateurs qui ont des clés publiques installées.

Format

```
access get public key users
```

Codes de retour

Le TABLEAU B-33 liste les codes de retour pour cette sous-commande.

TABLEAU B-33 Codes de retour de la sous-commande `access get public key users`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

Sous-commande access delete public key

Description : tous les utilisateurs peuvent exécuter cette commande pour supprimer leur propre clé publique individuelle. Les utilisateurs de niveau gestionnaire peuvent l'exécuter pour supprimer une clé publique pour tout utilisateur.

Format

`access delete public key [-u | --user]` *`UTILISATEUR`* `[-a | --all] [-q | --quiet]`

Le TABLEAU B-34 liste les arguments de cette sous-commande.

TABLEAU B-34 Arguments de la sous-commande `access delete public key`

Argument	Description
`[-u | --user]`	L'utilisateur dont la clé publique va être supprimée. Passe par défaut à l'utilisateur courant si aucun UTILISATEUR n'est spécifié. Cet argument peut être répété pour supprimer plusieurs clés publiques à la fois.
`[-a | --all]`	Supprime toutes les clés publiques.
`[-q | --quiet]`	Cet argument spécifie qu'aucune erreur ne sera retournée si l'utilisateur à supprimer est introuvable.

Codes de retour

Le TABLEAU B-35 liste les codes de retour pour cette sous-commande.

TABLEAU B-35 Codes de retour de la sous-commande `access delete public key`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NotFound`	5	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.

Sous-commandes d'accès relatives aux utilisateurs

Les sous-commandes listées dans le TABLEAU B-36 vous permettent de gérer un utilisateur individuel ou un groupe d'utilisateurs.

TABLEAU B-36 Sous-commandes de `access user`

Sous-commande	Description
`access add user`	Ajoute l'utilisateur local spécifié au groupe spécifié.
`access delete user`	Supprime l'utilisateur spécifié.
`access get users`	Récupère tous les utilisateurs d'un groupe administratif ou tous les utilisateurs de tous les groupes.
`access update password`	Met à jour le mot de passe de l'utilisateur spécifié.
`access update user`	Retourne les informations de connexion pour l'utilisateur spécifié.

Sous-commande access add user

Description : Ajoute l'utilisateur local spécifié au groupe spécifié avec l'ID d'utilisateur et le mot de passe indiqués.

Format

`access add user {-p | --password}` *`MOT_DE_PASSE`* `{-g | --group}` *`GROUPE`* `{-u | --user}` *`NOMUTILISATEUR`*

Le TABLEAU B-37 liste les arguments de cette sous-commande.

TABLEAU B-37 Arguments de la sous-commande `access add user`

Argument	Description
`{-p | --password}`	Met à jour le mot de passe du nouvel utilisateur. Le mot de passe est optionnel et s'il n'est pas spécifié, une invite demandant confirmation s'affiche.
`{-g | --group}`	Spécifie le groupe auquel le nouvel utilisateur appartiendra.
`{-u | --user}`	Spécifie le nom du nouvel utilisateur à ajouter. Cet argument peut être répété pour ajouter plusieurs utilisateurs à la fois.

Codes de retour

Le TABLEAU B-38 liste les codes de retour pour cette sous-commande.

TABLEAU B-38 Codes de retour de la sous-commande `access add user`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides. Le groupe spécifié par `-g` est un groupe administratif du SP local invalide ou la longueur du nom de l'utilisateur ou du mot de passe dépasse la longueur maximale.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_Exist`	`19`	L'utilisateur existe déjà.

Sous-commande access delete user

Description : supprime un utilisateur.

Format

`access delete user` *`NOMUTILISATEUR`* `[-a | --all] [-q | --quiet]`

Le TABLEAU B-39 liste les arguments de cette sous-commande.

TABLEAU B-39 Arguments de la sous-commande `access delete user`

Argument	Description
`NOMUTILISATEUR`	Spécifie le nom de l'utilisateur à supprimer. Cet argument peut être répété pour supprimer plusieurs utilisateurs à la fois.
`[-a | --all]`	Supprime tous les comptes d'utilisateur. L'utilisateur de niveau gestionnaire n'est pas supprimé lorsque cette commande est exécutée.
`[-q | --quiet]`	Cet argument spécifie qu'aucune erreur ne sera retournée si l'utilisateur à supprimer est introuvable.

Codes de retour

Le TABLEAU B-40 liste les codes de retour pour cette sous-commande.

TABLEAU B-40 Codes de retour de la sous-commande `access delete user`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_NotFound`	`5`	L'utilisateur spécifié est introuvable.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

Sous-commande access get users

Description : récupère tous les utilisateurs locaux d'un groupe administratif.

Format

```
access get users {-g | --group} [{-H | noheader}][{-D | --Delim
<SÉPARATEUR>}]
```

Le TABLEAU B-41 liste les arguments de cette sous-commande.

TABLEAU B-41 Arguments de la sous-commande `access get users`

Argument	Description
`{-g	--group}`	Spécifie le groupe duquel tous les utilisateurs doivent être récupérés.
`{-H	--noheader}`	Spécifie que les titres des colonnes doivent être supprimés.
`{ -D	--Delim }`	Indique d'utiliser le séparateur spécifié pour délimiter les colonnes. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU B-42 liste les codes de retour pour cette sous-commande.

TABLEAU B-42 Codes de retour de la sous-commande `access get users`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	4	Un ou plusieurs arguments étaient incorrects ou invalides.

Sous-commande access update password

Remarque – Cette commande permet aux gestionnaires de changer les mots de passe des autres utilisateurs ; chaque utilisateur peut changer son propre mot de passe.

Description : change le mot de passe d'un utilisateur existant.

Format

`access update password {-p | --password}` *`MOTDEPASSE`* `{u | --user}` *`UTILISATEUR`*

Le TABLEAU B-43 liste les arguments de cette sous-commande.

TABLEAU B-43 Arguments de la sous-commande `access update password`

Argument	Description
`{-u	--user}`	Nom de l'utilisateur dont vous voulez mettre à jour le mot de passe. Utilise par défaut l'utilisateur courant si aucun utilisateur n'est spécifié. Vous devez avoir un accès de niveau gestionnaire pour changer le mot de passe d'un autre utilisateur. Cet argument peut être répété pour mettre à jour les mots de passe de plusieurs utilisateurs à la fois.
`{-p	--password}`	Nouveau mot de passe de l'utilisateur. Si aucun mot de passe n'est spécifié, un message vous invitant à entrer le mot de passe puis à le confirmer s'affiche.

Codes de retour

Le TABLEAU B-44 liste les codes de retour pour cette sous-commande.

TABLEAU B-44 Codes de retour de la sous-commande `access update password`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	4	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NotFound`	5	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.

Sous-commande access update user

Description : met à jour les informations de connexion (mot de passe ou groupe) pour l'utilisateur.

Format

```
access update user {-u | --user} UTILISATEUR {-p | --password}
MOT_DE_PASSE
{-g | --group} GROUPE
```

Le TABLEAU B-45 liste les arguments de cette sous-commande.

Remarque – Les arguments `-p` et `-g` sont optionnels mais vous devez en spécifier au moins un.

TABLEAU B-45 Arguments de la sous-commande `access update user`

Argument	Description
`{-u | --user}`	Nom de l'utilisateur à mettre à jour.
`{-p | --password}`	Nouveau mot de passe de l'utilisateur. Les options `-p` et `-g` sont optionnelles mais vous devez en spécifier au moins une.
`{-g | --group}`	Nouveau groupe auquel l'utilisateur va être réaffecter. Les options `-p` et `-g` sont optionnelles mais vous devez en spécifier au moins une.

Codes de retour

Le TABLEAU B-45 liste les codes de retour pour cette sous-commande.

TABLEAU B-46 Codes de retour de la sous-commande `access update user`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_NotFound`	`5`	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

ANNEXE **C**

Commandes de diagnostic

Les commandes `diags` vous permettent de gérer les tests de diagnostic.

Le TABLEAU C-1 liste les sous-commandes de `diags`.

Remarque – Chaque sous-commande retourne un code de retour à la fin de l'opération.

Remarque – Les commandes de diagnostic sont également données dans le *Serveurs Sun Fire V20z et Sun Fire V40z — Guide des techniques de dépannage et de diagnostic*, 819-2924-12.

TABLEAU C-1 Sous-commandes de diagnostic

Sous-commande	Description
`diags cancel tests`	Annule un ou plusieurs tests de diagnostic, ce qui entraîne la suppression des données de résultat.
`diags get modules`	Retourne la liste des modules de test disponibles. Interroge la structure pour obtenir les informations du module de test.
`diags get state`	Retourne l'état du serveur de contrôle des diagnostics de la plate-forme.
`diags get tests`	Retourne des données décrivant les tests de diagnostic disponibles ainsi que les leurs exigences et paramètres.
`diags run tests`	soumet un ou plusieurs tests de diagnostic à exécution.
`diags start`	Démarre la structure de diagnostics du processeur de service et de la plate-forme.
`diags terminate`	Met fin à tous les tests de diagnostic et arrête le sous-système de diagnostic.

Avant de commencer

Ne pas accéder au SP quand les diagnostics sont chargés

Remarque – Ce problème apparaît dans la version 2.1.0.16 de NSV et les versions antérieures. Il est corrigé dans la version 2.2.0.6 de NVS et les versions ultérieures.

Pendant que vous exécutez les diagnostics sur votre serveur, n'interagissez pas avec le SP par le biais de l'interface de ligne de commande ou d'IPMI.

Les commandes des capteurs ne peuvent pas être utilisées de façon fiable lorsque les diagnostics sont en cours d'exécution. Émettre des commandes de capteur alors que les diagnostics sont chargés peut entraîner l'enregistrement d'événements critiques erronés ou « fausses alertes » dans le journal d'événements. Les valeurs retournées par les capteurs ne sont pas fiables dans ce cas.

Problèmes connus

Message d'erreur bénigne

Lorsque les diagnostics sont lancés sur la plate-forme, le système essaie de monter l'unité de disquette. L'erreur suivante est retournée :

```
mount : Mounting /dev/fd0 on /mnt/floppy failed. No such device.
```

Vous pouvez sans risque ignorer ce message d'erreur.

Sous-commande diags cancel tests

Description : annule un ou plusieurs tests de diagnostic, ce qui entraîne la suppression des données de résultat.

Format

```
diags cancel tests [[{ -t | --test} TEST HANDLE] | [{-a|--all}]
[{-H | --noheader}]]
```

Le TABLEAU C-2 liste les arguments de cette sous-commande.

Remarque – Ne spécifier aucun argument annule tous les tests pour chaque périphérique du serveur.

TABLEAU C-2 Arguments de la sous-commande `diags cancel tests`

Argument	Description
`{ -t | --test}`	Spécifie le test à annuler. REMARQUE - Le `TEST HANDLE` correspond au `TEST HANDLE` qui s'affiche à l'écran lorsque vous soumettez le test.
`{-a | --all}`	Annule tous les tests.
`{-H | --noheader}`	Supprime les titres de la sortie.

Codes de retour

TABLEAU C-3 liste les codes de retour pour cette sous-commande.

TABLEAU C-3 Arguments de la sous-commande `diags cancel tests`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_MissingArgument`	`7`	Argument(s) manquant(s).
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande diags get modules

Description : Retourne la liste des modules de test disponibles. La commande diags get modules interroge la structure pour obtenir les informations des modules de test.

```
diags get modules [{-v|--verbose}]
```

Voici quelques exemples de sortie signalant une réussite :

```
diags get modules
Module
fan
flash
memory


diags get modules -v
Module Host Type
fan    SP
flash  SP
memory PF
```

TABLEAU C-4 Arguments de `diags get modules`

Argument	Description
`[ { -v|--verbose}]`	Affiche toutes les colonnes dans la sortie.

TABLEAU C-5 Codes de retour de `diags get modules`

Code de retour	ID	Description
`NWSE_RPCTimeout`	`0`	La requête a été émise mais n'a pas été traitée par le serveur.
`NWSE_RPCNotConnected`	`1`	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible. Les diagnostics du CD sont en cours d'exécution, l'utilisateur essaye d'exécuter des diagnostics sur le processeur de services.

Sous-commande diags get state

Description : Retourne l'état du serveur de contrôle des diagnostics de la plate-forme.

Format

```
diags get state
```

Si le résultat retourné par la commande indique que la plate-forme est activée et prête pour les diagnostics, vous pouvez soumettre les tests de diagnostic de la plate-forme à exécution.

Les messages de texte de réussite suivants peuvent être retournés :

```
SP Diagnostics is ready to accept tests. Run 'diags get state' to
determine availability of Platform Diagnostics.

SP Diagnostics (in no-platform mode) is ready to accept tests.

Platform and SP Diagnostics are ready to accept tests.
```

Le message de texte d'erreur suivant peut être retourné :

```
Error. Verify that the platform state is 'off' and retry or use the
'diags start --forced' option to ignore the current state.

Error. Platform CD Diagnostics is currently running.

Error. Diagnostics is currently running. Run 'diags terminate' and
try again.

Error. Unable to load Platform Diagnostics. Diagnostics terminated.

Error. Unable to load SP Diagnostics. Diagnostics terminated.

Error. SP no-platform Diagnostics is already running.
```

Codes de retour

Le TABLEAU C-6 liste les codes de retour pour cette sous-commande.

TABLEAU C-6 Codes de retour de la sous-commande `diags get state`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.
`NWSE_DeviceError`	`25`	Impossible de lire ou d'écrire sur le périphérique.

Sous-commande diags get tests

Description : retourne des données décrivant les tests de diagnostic disponibles. Ces données incluent le nom des tests concernés et le module auquel chaque test s'applique.

Format

```
diags get tests [{-H | --noheader}] [{-D |--Delim} <SÉPARATEUR>]
[-v | --verbose]
```

Remarque – Si la sortie contient des tests imbriqués, vous pouvez rediriger la sortie dans un fichier que vous afficherez dans un éditeur pour en faciliter la lecture.

Le TABLEAU C-7 liste les arguments de cette sous-commande.

TABLEAU C-7 Arguments de la sous-commande `diags get tests`

Argument	Description
`{-H | --noheader}`	Supprime les titres de la sortie.
`{-D | --Delim <SÉPARATEUR>}`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.
`[-v | --verbose]`	Si spécifié, **Host Type** (type d'hôte), **Services** (services) et **Devices** (périphériques) s'affichent en plus de **Module** (module) et **Testname** (nom du test).

Codes de retour

Le TABLEAU C-8 liste les codes de retour pour cette sous-commande.

TABLEAU C-8 Codes de retour de la sous-commande `diags get tests`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_MissingArgument`	`7`	Argument(s) manquant(s).
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande diags run tests

Description : soumet un ou plusieurs tests de diagnostic à exécution.

Format

```
diags run tests [ [{ -n | --name} NOM TEST ] [{-a| --all}]
[-H | --noheader] [-P | --noprogress] [{-m | --module} NOM MODULE]
[-v | --verbose]
```

Remarque – Si la sortie contient des tests imbriqués, vous pouvez rediriger la sortie dans un fichier que vous afficherez dans un éditeur pour en faciliter la lecture.

Le TABLEAU C-9 liste les arguments de cette sous-commande.

TABLEAU C-9 Arguments de la sous-commande `diags run tests`

Argument	Description
`{-n | --name}`	Spécifie le ou les tests spécifiques à exécuter. Exécutez `diags get tests` pour obtenir la liste des noms des différents tests.
`{-a | --all}`	Spécifie que tous les tests doivent être exécutés. Exécutez `diags get tests` pour obtenir la liste de tous les tests disponibles. Ne spécifier aucun argument exécute tous les tests pour chaque périphérique du serveur.
`{-H | --noheader}`	Supprime les titres de la sortie.
`{-P | --noprogress}`	Supprime les points de progression lors de l'attente des résultats des tests.
`{-m | --module}`	Spécifie que seuls les tests relatifs au module spécifié doivent être exécutés. Exécutez `diags get tests` pour obtenir la liste des modules.
`[-v | --verbose]`	Si spécifié, les `Test Details` (détails du test) s'affichent à la suite de la ligne des résultats du test.

Les données suivantes s'affichent après l'exécution d'un test :

- nom du test soumis ;
- Test Handle ;
- Test Result (par exemple : Passed, Failed) ;
- Details. Si vous spécifiez l'option `-v`, les détails du test s'affichent. Ils contiennent des informations détaillées sur le test, telles que les valeurs maximale, minimale et nominale, les valeurs courantes, etc. En cas d'échec, les Failure Details (détails de l'échec) s'affichent avec un message de texte indiquant la cause de l'échec.

Codes de retour

TABLEAU C-10 liste les codes de retour pour cette sous-commande.

TABLEAU C-10 Codes de retour de la sous-commande `diags run tests`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_MissingArgument`	`7`	Argument(s) manquant(s).
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande diags start

Description : démarre la structure de diagnostics du SP et de la plate-forme. Vous devez exécuter cette commande avant d'exécuter un test quelconque.

Format

```
diags start {--noplatform} [{-f|--forced}]
```

Argument	Description
`{--noplatform}`	Indique de démarrer les diagnostics sur le SP depuis le montage NFS, sans redémarrer la plate-forme en mode `diags`. ***Remarque*** **-** Cette option n'est pas disponible lorsque les diagnostics sont exécutés depuis le CD-ROM.
`{-f | --forced}`	Force les diagnostics à démarrer.

Vous pouvez exécuter les tests du SP immédiatement après l'exécution de cette commande.

Cette commande redémarre la plate-forme en mode diagnostics. Ce processus peut prendre deux à trois minutes. Vous pouvez commencer à exécuter les diagnostics sur le SP pendant le chargement des diagnostics de la plate-forme. Veuillez toutefois patienter une minute avant d'exécuter les diagnostics de la plate-forme pour que le noyau de diagnostic soit complètement chargé sur la plate-forme.

Pour vérifier si les tests de diagnostics sont prêts à être exécutés, exécutez la sous-commande `diags get state`. Voir « Sous-commande diags get state », page 168.

Cette sous-commande retourne l'un des états suivants :

- **Message de texte de réussite**. Les diagnostics de la plate-forme sont activés et disponibles pour recevoir des requêtes de test.
- **Message de texte d'échec.**Les diagnostics de la plate-forme ne sont pas activés.

Si l'état retourné par la commande indique que la plate-forme est activée et prête pour les diagnostics, vous pouvez soumettre les tests de diagnostic de la plate-forme à exécution. Vous pouvez en option démarrer les diagnostics sur le SP depuis le montage NFS, sans redémarrer la plate-forme en mode `diags`. Cela vous permet de continuer à exécuter le SE de production tout en effectuant les tests de diagnostic du SP.

Pour cela, exécutez la sous-commande `diags start` avec l'option suivante :

```
diags start --no platform
```

L'état de la plate-forme doit être soit off soit OS Communicating. Pour plus de détails sur ces états, voir la sous-commande `platform get os state`.

Codes de retour

Le TABLEAU C-11 liste les codes de retour pour cette sous-commande.

TABLEAU C-11 Codes de retour de la sous-commande `diags start`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoRouteToHost`	`13`	Pas de route vers l'hôte (réseau hors service). Se produit lorsque CD Diagnostics est incapable d'envoyer un paquet au SP sur un port spécifique.
`NWSE_InvalidOpForState`	`22`	Opération incorrecte pour l'état courant.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande diags terminate

Description : met fin à tous les tests de diagnostic et arrête la session de diagnostic.

Format

```
diags terminate
```

Codes de retour

Le TABLEAU C-12 liste les codes de retour pour cette sous-commande.

TABLEAU C-12 Codes de retour de la sous-commande `diags terminate`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	4	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.
`NWSE_MissingArgument`	7	Argument(s) manquant(s).
`NWSE_NoRouteToHost`	13	Pas de route vers l'hôte (réseau hors service). Se produit lorsque CD Diagnostics est incapable d'envoyer un paquet au SP sur un port spécifique.
`NWSE_ServiceNotAvailable`	24	Le service demandé n'est pas disponible.

ANNEXE **D**

Commandes d'inventaire

La commande `inventory` dresse l'inventaire du matériel et des logiciels d'un serveurs Sun Fire V20z et V40z.

Le TABLEAU D-1 liste les sous-commandes de `inventory` que vous pouvez utiliser pour récupérer des informations spécifiques sur le matériel ou les logiciels.

Remarque – Chaque sous-commande retourne un code de retour à la fin de l'opération.

TABLEAU D-1 Sous-commandes d'inventaire

Sous-commande	Description
`inventory compare versions`	Retourne la liste de tous les packages installés et les différences de version existant avec les versions listées dans le document correspondant.
`inventory get hardware`	retourne des informations détaillées sur tous les composants matériels remplaçables sur le site.
`inventory get software`	Retourne des informations d'inventaire pour tous les logiciels installés et non.
`inventory get remote-software`	Retourne la liste des versions des packages disponibles pour le téléchargement ou l'installation d'un serveur de mise à jour en cours d'exécution.
`inventory get all`	Retourne des informations détaillées sur tous les composants matériels et logiciels.

Sous-commande inventory compare versions

Description : retourne la liste de tous les packages installés et les différences de version existant avec les versions listées dans le document correspondant ou celles disponibles sur un serveur de mise à jour en cours d'exécution. Vous pouvez utiliser cette commande pour vérifier si votre installation est cohérente avec une version prise en charge et pour déterminer les packages qui ont été mis à jour dans une nouvelle version.

Format

```
inventory compare versions
[{-f | --file} FICHIER_MANIFESTE_VERSION |
{{-i | --ipaddress} IP_SERVEUR_DISTANT]
{-p | --port} PORT_SERVEUR_DISTANT]
{-v | --verbose} [{-H | --noheader}]
[{-D | --Delim <SÉPARATEUR>}]
```

Le TABLEAU D-2 liste les arguments de cette sous-commande.

TABLEAU D-2 Arguments de la sous-commande `inventory compare versions`

Argument	Description
`{-f | --file}`	Fichier qui décrit tous les packages et versions d'une version de distribution du logiciel. Ces fichiers se trouvent dans le répertoire `root` d'un fichier NSV décompressé et l'on y accède en général via le point de partage en `/mnt`.
`{-i | --ipaddress}`	Adresse IP d'un serveur de mise à jour en cours d'exécution.
`{-p | --port}`	Numéro du port utilisé par le serveur de mise à jour.
`{-v | --verbose}`	Affiche des informations supplémentaires, notamment le chemin du package correspondant sur le NSV, la description du package installé et la description du package correspondant du manifeste. Cette option est ignorée en cas de comparaison avec le serveur de mise à jour (en utilisant les options `-i` et `-p`).
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU D-3 liste les codes de retour pour cette sous-commande.

TABLEAU D-3 Codes de retour de la sous-commande `inventory compare versions`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NotFound`	5	Erreur. L'inventaire des logiciels à distance n'est pas disponible.
`NWSE_ServiceNotAvailable`	24	Le service demandé n'est pas disponible.

Sous-commande inventory get hardware

Description : cette commande retourne des informations pour les composants matériels remplaçables sur site. Les informations retournées incluent le nom, le type de périphérique, les attributs, l'OEM, la date de fabrication, la révision du matériel, le numéro de série et la référence du composant.

Format

```
inventory get hardware [{-v|--verbose}]
[{-H|--noheader}] [{-D|--Delim}]
```

Pour obtenir la révision de la carte, exécutez la commande suivante :

```
inventory get hardware -D : |grep Motherboard|awk -F : '{print $5}'
```

Pour obtenir la révision PRS, exécutez la commande suivante :

```
inventory get hardware -D : |grep PRS|awk -F : '{print $5}'
```

Remarque – Vous pouvez aussi utiliser la commande **sensor get** pour trouver ces informations.

La sortie de la commande, sans l'argument -v, inclut les informations suivantes, dans les colonnes de gauche à droite :

- Name (nom du périphérique)
- Device Type (type du périphérique)
- Attributes (informations diverses sur le composant tels que la vitesse de la CPU)
- OEM (entité qui distribue la pièce)
- Manufacture Date (date de fabrication)
- HW Revision (numéro de révision)
- Serial # (numéro de série)
- Part # (référence)

Voici un exemple de sortie d'une commande réussie, sans l'argument -v (compte tenu de l'espace limité à disposition, les colonnes **Hardware Revision** et **Part #** n'apparaissent pas).

```
localhost # inventory get hardware
Name            Type            OEM               Manufacture Date
CPU 0 DIMM 0    memory          127f000000000000  2000-01-01
CPU 0 DIMM 1    memory          127f000000000000  2000-01-01
CPU 0 DIMM 2    memory          127f000000000000  2000-01-01
CPU 0 DIMM 3    memory          127f000000000000  2000-01-01
DDR 0 VRM       memvrm                            NA
CPU 0           cpu             AuthenticAMD      NA
Family 15 Model 5 Stepping 1
CPU 0 VRM       vrm                               NA
CPU 1 DIMM 0    memory          127f000000000000  2000-01-01
CPU 1 DIMM 1    memory          127f000000000000  2000-01-01
CPU 1 DIMM 2    memory          127f000000000000  2000-01-01
CPU 1 DIMM 3    memory          127f000000000000  2000-01-01
DDR 1 VRM       memvrm                            NA
CPU 1           cpu             AuthenticAMD      NA
Family 15 Model 5 Stepping 1
CPU 1 VRM       vrm                               NA
Motherbrd         planarS-SCI14312004-10-31
PRS Software    os                                2005-03-16
SCSI backplane scsi_backplane                     NA
```

Les autres titres de colonnes qui s'affichent dans la sortie, si vous utilisez l'argument -v sont les suivants :

- MfgAssy#
- MfgAssyRev
- FirmwareID (ID du microprogramme)
- FirmwareRev (révision du microprogramme)
- SoftwareRev (révision du logiciel)
- SoftwareID (ID du logiciel)
- Identifier (identificateur)

Le TABLEAU D-4 liste les arguments de cette sous-commande.

TABLEAU D-4 Arguments de la sous-commande `inventory get hardware`

Argument	Description
`{ -v | --verbose }`	Affiche toutes les colonnes.
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU D-5 liste les codes de retour pour cette sous-commande.

TABLEAU D-5 Codes de retour de la sous-commande `inventory get hardware`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.

Sous-commande inventory get software

Description : Retourne des informations d'inventaire pour tous les logiciels installés et non (qui se trouvent sur le système de fichiers externe optionnel).

Format

```
inventory get software [{-a | --all}][{-H | --noheader}]
[{-D | --Delim <SÉPARATEUR>}]
```

Le TABLEAU D-6 liste les arguments de cette sous-commande.

TABLEAU D-6 Arguments de la sous-commande `inventory get software`

Argument	Description
`{-a | --all}`	Optionnel : Recherche dans le répertoire `/sw_images` du processeur de service les packages et les logiciels non-installés.
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU D-7 liste les codes de retour pour cette sous-commande.

TABLEAU D-7 Codes de retour de la sous-commande `inventory get software`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.

Sous-commande inventory get remote software

Description : Retourne la liste des versions des packages disponibles pour le téléchargement ou l'installation d'un serveur de mise à jour en cours d'exécution.

Format

```
inventory get remote-software [{-D|--Delim} SÉPARATEUR]
[{-H|--noheader}] [{-i|--ipaddress} ADRESSE_DISTANTE]
[{-p|--port} PORT_DISTANT]
```

Le TABLEAU D-8 liste les arguments de cette sous-commande.

TABLEAU D-8 Arguments de la sous-commande `inventory get remote-software`

Argument	Description
`{-i | --ipaddress}`	Adresse IP d'un serveur de mise à jour en cours d'exécution.
`{-p | --port}`	Numéro du port utilisé par le serveur de mise à jour.
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU D-9 liste les codes de retour pour cette sous-commande.

TABLEAU D-9 Codes de retour de la sous-commande `inventory get remote-software`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NotFound`	`5`	Error. L'inventaire des logiciels à distance n'est pas disponible.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande inventory get all

Description : retourne des informations détaillées sur tous les composants matériels remplaçables sur le site et tous les logiciels installés et non.

Format

```
inventory get all {-a | --all} {-v | --verbose} [{-H | --noheader}]
[{-D | --Delim <SÉPARATEUR>}]
```

Le TABLEAU D-10 liste les arguments de cette sous-commande.

TABLEAU D-10 Arguments de la sous-commande `inventory get all`

Argument	Description
`{-a | --all}`	*(Optionnel)*Recherche dans le répertoire `/sw_images` du processeur de service les packages et les logiciels non-installés.
`{ -v | --verbose }`	Affiche toutes les colonnes.
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU D-11 liste les codes de retour pour cette sous-commande.

TABLEAU D-11 Codes de retour de la sous-commande `inventory get all`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.

ANNEXE **E**

Commandes IPMI

La commande `ipmi` gère les fonctions IPMI.

Le TABLEAU E-1 liste les sous-commandes de `ipmi`.

Remarque – Chaque sous-commande retourne un code de retour à la fin de l'opération.

TABLEAU E-1 Sous-commandes IPMI

Sous-commande	Description
`ipmi disable channel`	Désactive un des deux canaux IPMI.
`ipmi enable channel`	Active un des deux canaux IPMI.
`ipmi disable pef`	Désactive le filtrage d'événements de la plate-forme.
`ipmi enable pef`	Active le filtrage d'événements de la plate-forme.
`ipmi get channels`	Affiche la liste des canaux IPMI et indique s'ils sont activés ou désactivés.
`ipmi get global enables`	Affiche la liste des activations globales IPMI et leur valeurs courantes.
`ipmi set global enable`	Définit la valeur de plusieurs variables d'activation globales de l'IPMI.
`ipmi get sel`	Affiche les éléments du journal d'événements du système (SEL) au format brut.
`ipmi clear sel`	Efface le journal d'événements du système (SEL).
`ipmi reset`	ramène les informations IPMI aux paramètres par défaut définis en usine.

Sous-commande ipmi disable channel

Description : vous permet de désactiver un des deux canaux IPMI.

Format

```
ipmi disable channel {sms | lan}
```

Le TABLEAU E-2 liste les arguments de cette sous-commande.

TABLEAU E-2 Arguments de la sous-commande `ipmi disable channel`

Argument	Description
`sms`	ID du canal à désactiver pour l'interface système ; n'est pas sensible à la casse.
`lan`	ID du canal à désactiver pour l'interface LAN ; n'est pas sensible à la casse.

Codes de retour

Le TABLEAU E-3 liste les arguments pour cette sous-commande.

TABLEAU E-3 Codes de retour de la sous-commande `ipmi disable channel`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

Sous-commande ipmi enable channel

Description : vous permet d'activer un des deux canaux IPMI.

Format

```
ipmi enable channel {sms | lan}
```

Le TABLEAU E-4 liste les arguments de cette sous-commande.

TABLEAU E-4 Arguments de la sous-commande `ipmi enable channel`

Argument	Description
`sms`	ID du canal à activer pour l'interface système ; n'est pas sensible à la casse.
`lan`	ID du canal à activer pour l'interface LAN ; n'est pas sensible à la casse. Si vous activez le canal pour la première fois, vous êtes invité à entrer le mot de passe associé à l'utilisateur *null*.

Codes de retour

Le TABLEAU E-5 liste les codes de retour de cette sous-commande.

TABLEAU E-5 Codes de retour de la sous-commande `ipmi enable channel`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande ipmi disable pef

Description : Vous permet de désactiver le filtrage d'événements de la plate-forme (PEF).

Format

```
ipmi disable pef
```

Codes de retour

Le TABLEAU E-6 liste les codes de retour de cette sous-commande.

TABLEAU E-6 Codes de retour de la sous-commande `ipmi disable pef`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

Sous-commande ipmi enable pef

Description : Vous permet d'activer le filtrage d'événements de la plate-forme (PEF).

Format

```
ipmi enable pef
```

Codes de retour

Le TABLEAU E-7 liste les codes de retour de cette sous-commande.

TABLEAU E-7 Codes de retour de la sous-commande `ipmi enable pef`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande ipmi get channels

Description : affiche la liste des canaux IPMI et indique si chaque canal est activé ou désactivé.

Format

```
ipmi get channels
```

Codes de retour

Le TABLEAU E-8 liste les codes de retour de cette sous-commande.

TABLEAU E-8 Codes de retour de la sous-commande `ipmi get channels`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.

Sous-commande ipmi get global enables

Description : affiche la liste des activations globales IPMI et la valeur courante de chacune.

Format

```
ipmi get global enables
```

Codes de retour

Le TABLEAU E-9 liste les codes de retour de cette sous-commande.

TABLEAU E-9 Codes de retour de la sous-commande `ipmi get global enables`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.

Sous-commande ipmi get sel

Description : Affiche les éléments du journal d'événements du système en format brut.

Format

```
ipmi get sel
```

La sortie de cette commande retourne les informations suivantes, dans des colonnes de gauche à droite :

- Record ID (ID de l'enregistrement)
- Record Type (type de l'enregistrement)
- Tiimestamp (horodatage)
- Generator ID (Id générateur)
- Format Version (version du format)
- Sensor Type (type du capteur)
- Sensor # (n° du capteur)
- Event Dir/Type Event (rép. événement/type)
- Data (données)

Voici un exemple de **sortie réussie** de la commande (compte-tenu de l'espace à disposition, la colonne **Timestamp**, qui est la troisième à partir de la gauche, n'apparaît pas).

```
localhost # ipmi get sel
Record           RecordGeneratorFormatSensorSensorEventData
ID               TypeID  Ver Type#   Dir/
0001             0x020x00200x040x100xfc0x6f02ffff
0002             0x020x00000x040x510x060x0708090a
0003             0x020x00000x040x510x060x0708090a
0004             0x020x00000x040x510x060x0708090a
0005             0x020x00200x040x120x270x6fc500ff
0006             0x020x00200x040x120x270x6fc580ff
0007             0x020x00200x040x040x310x01520121
localhost # ipmi get sel -H
0001             0x020x00200x040x100xfc0x6f02ffff
0002             0x020x00000x040x510x060x0708090a
0003             0x020x00000x040x510x060x0708090a
0004             0x020x00000x040x510x060x0708090a
```

```
0005              0x020x00200x040x120x270x6fc500ff
0006              0x020x00200x040x120x270x6fc580ff
0007              0x020x00200x040x040x310x01520121
localhost # ipmi get sel -H -D ,
0001,0x02,02/28/2005 18:53:17,0x0020,0x04,0x10,0xfc,0x6f,02ffff
0002,0x02,02/28/2005 18:53:17,0x0000,0x04,0x51,0x06,0x07,08090a
0003,0x02,02/28/2005 18:53:17,0x0000,0x04,0x51,0x06,0x07,08090a
0004,0x02,02/28/2005 18:53:17,0x0000,0x04,0x51,0x06,0x07,08090a
0005,0x02,02/28/2005 18:53:17,0x0020,0x04,0x12,0x27,0x6f,c500ff
0006,0x02,06/14/1906 21:02:57,0x0020,0x04,0x12,0x27,0x6f,c580ff
0007,0x02,06/15/1906 00:00:05,0x0020,0x04,0x04,0x31,0x01,520121
```

TABLEAU E-10 Arguments de `ipmi get sel`

Argument	Description
`[{-H|--noheader}]`	Supprime les titres des colonnes.
`[{-D|--Delim}]`	Spécifie un séparateur de champ différent.

TABLEAU E-11 Codes de retour de `ipmi get sel`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_Busy`	9	Périphérique ou ressource occupé.

sous-commande ipmi clear sel

Description : Cette commande efface le journal d'événements du système.

```
ipmi clear sel
```

Une **sortie réussie** est la suivante :

```
localhost # ipmi clear sel
```

TABLEAU E-12 Codes de retour de `ipmi clear sel`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_Busy`	`9`	Impossible de réserver SEL.
`NWSE_NotRecognized`	`20`	La requête n'est pas reconnue/comprise.
`NWSE_DeviceError`	`25`	Impossible d'accéder aux informations SEL.

Sous-commande ipmi set global enable

Description : vous permet de définir la valeur de plusieurs variables d'activation globales IPMI.

Format

```
ipmi set global enable {-n |--name} NOM_GLOBAL {{-e|--enabled} |
{-d|--disabled}}
```

Le TABLEAU E-13 liste les arguments de cette sous-commande.

Le TABLEAU E-14 contient des informations sur les alias.

TABLEAU E-13 Codes de retour de la sous-commande `ipmi set global enable`

Argument	Description
`{-n | --name}`	Nom de l'une des variables d'activation globales IPMI, voir le TABLEAU E-14. Vous pouvez utiliser au choix une chaîne longue entre guillemets anglo-saxons doubles soit un alias sans guillemets pour la liste des activations globales.
`{-e|--enabled}`	Active le canal.
`{-d|--disabled}`	Désactive le canal.

TABLEAU E-14 Informations sur les alias

Alias	Chaîne de nom	Valeurs	Valeur par défaut
`oem0`	OEM0 Enable	Enabled/ Disabled	Disabled
`oem1`	OEM1 Enable	Enabled/ Disabled	Disabled
`oem2`	OEM 2 Enable	Enabled/ Disabled	
`logging`	Enable System Event Logging	Enabled/ Disabled	Enabled
`msg_buf`	Enable Event Message Buffer	Enabled/ Disabled	
`msg_buf_interrupt`	Enable the Event Message Buffer Full	Enabled/ Disabled	
`msg_queue_interrupt`	Enable Receive Message Queue Interrupt	Enabled/ Disabled	Enabled

Codes de retour

Le TABLEAU E-15 liste les codes de retour pour cette sous-commande.

TABLEAU E-15 Codes de retour de la sous-commande `ipmi set global enable`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

Sous-commande ipmi reset

Description : ramène les informations IPMI aux paramètres par défaut définis en usine.

Format

```
ipmi reset {-s | --sdrr} {-c | --config} {-p | --password} {-a | --all}
```

Le TABLEAU E-16 liste les arguments de cette sous-commande.

TABLEAU E-16 Codes de retour de la sous-commande `ipmi reset`

Argument	Description
`{-s | --sdrr}`	Copie le fichier de base de données original dans `pstore`.
`{-c | --config}`	Supprime le fichier de configuration et les activations globales.
`{-p | --password}`	Supprime le fichier du mot de passe.
`{-a | --all}`	Effectue les fonctions pour tous les paramètres.

Codes de retour

Le TABLEAU E-17 liste les codes de retour de cette sous-commande.

TABLEAU E-17 Codes de retour de la sous-commande `ipmi reset`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.

ANNEXE **F**

Commandes de la plate-forme

La commande `platform` rapport ou modifie certains aspects de l'état de la plate-forme.

Le TABLEAU F-1 liste les groupes de sous-commandes de la commande `platform`.

Remarque – Chaque sous-commande retourne un code de retour à la fin de l'opération.

TABLEAU F-1 Groupes des sous-commandes de plate-forme

Groupe de sous-commandes	Description
`platform console`	Gère l'accès à la console série de la plate-forme.
`platform os state`	Gère l'état courant du système d'exploitation (SE).
`platform power state`	Gère l'état courant de l'alimentation de la plate-forme.
`platform get hostname`	Affiche le nom d'hôte de la plate-forme courante principale.
`platform get mac`	Retourne les adresses MAC des deux NIC embarquées de la plate-forme.
`platform get product id`	Affiche l'ID de produit du système courant.

Sous-commandes de plate-forme relatives à la console

Les sous-commandes listées dans le TABLEAU F-2 vous permettent de gérer l'accès à la console série de la plate-forme.

TABLEAU F-2 Sous-commandes de `Platform Console`

Sous-commande	Description
`platform console`	Fournit l'accès à la console série de la plate-forme.
`platform get console`	Récupère la configuration de l'accès SP à la console série du système.
`platform set console`	Configure l'accès SP à la console série de la plate-forme.

Sous-commande platform console

Description : pour des fonctions de gestion à distance, cette commande fournit l'accès à la console série de la plate-forme. Utilisée conjointement avec la sous-commande `platform set console` et les paramètres de SE BIOS/plate-forme appropriés, cette commande vous permet d'afficher la console série de la plate-forme lorsque vous êtes connecté au SP.

Format

```
platform console
```

Vous devez configurer les paramètres du BIOS en utilisant l'utilitaire BIOS Setup. Pour actualiser l'écran BIOS Setup, appuyez sur **Contrôle-R**. Choisissez l'onglet **Advanced** pour définir la configuration.

Le TABLEAU F-3 liste les valeurs COM1 courantes, le TABLEAU F-4 les valeurs de redirection de console courantes.

TABLEAU F-3 Valeurs COM1 courantes

Configuration des périphériques E/S	
Serial port A	Enabled
Base I/O address	3F8
Interrupt	IRQ 4

TABLEAU F-4 Valeur de redirection de console courantes

Redirection de la console	
Com Port Address	On-board COM A
Console connection :	Direct
Baud Rate	19.2K
Flow Control	Ne rien faire
Console Type	ANSI

Remarque – Vous pouvez changer ces valeurs à condition de toujours utiliser des valeurs identiques à celles du port série du système d'exploitation (SE). Si votre système d'exploitation prend en charge les valeurs COM2-4, vous pouvez les définir pour les paramètres du BIOS.

Les paramètres de la console série dans le SE de la plate-forme doivent être définis de façon à correspondre aux paramètres du BIOS.

Entrez ce qui suit lorsque vous êtes connecté à la console :

`^Ec` *`caractère`*

Où ^E représente **Contrôle-E** et *caractère* est l'une des entrées du TABLEAU F-5 :

TABLEAU F-5 Valeurs de la console série

Caractère	Fonction
.	Déconnecte une lecture/écriture connectée.
b	Envoie un message de diffusion.
c	Faite basculer le contrôle de flux.
d	Met une console hors service.
e	Change la séquence d'échappement.
f	Force une lecture/écriture connectée.
g	Regroupe les informations.
i	Vidage d'informations.
L	Bascule entre journalisation activée/désactivée.
l?	Interrompt la liste de la séquence. ***Remarque -*** *Le premier caractère est un L minuscule.*
l0	Envoie une interruption par fichier de configuration. ***Remarque -*** *Le premier caractère est un L minuscule.*
l1-9	Envoie une séquence d'interruption spécifique. ***Remarque -*** *Le premier caractère est un L minuscule.*
o	Rouvre le tty et le fichier journal.
p	Relit les 60 dernières lignes.
r	Relit les 20 dernières lignes.
s	Espionner la lecture uniquement.
u	Affiche le statut de l'hôte.
v	Affiche les informations relatives à la version.
w	Affiche la personne connectée à cette console.
x	Affiche les informations sur la vitesse en bauds de la console.
z	Suspend la connexion.
<cr>	Ignore/abandonne la commande.
?	Imprime ce message.
^R	Relit la dernière ligne.
\ooo	Envoie le caractère par code octal.

Dans certaines circonstances, il peut être nécessaire d'envoyer une séquence d'interruption série au SE de la plate-forme (par exemple, pour simuler la touche SysRq quand CONFIG_MAGIC_SYSRQ est défini et activé dans un noyau Linux).

Pour effectuer cette opération, utilisez la séquence suivante :

```
^Ecl0
```

(**Contrôle-E**, suivie d'un « c » minuscule, d'un « l » minuscule et du chiffre « 0 »).

La commande `platform console` répond en affichant la chaîne `[halt sent]`, confirmant que la séquence d'interruption a été générée.

Dans le cas où la sortie de la console est corrompue, `^Ecd ^Eco` rétablit en général un fonctionnement normal ; ce problème est normalement dû aux problèmes de contrôle de flux.

Exemple :

L'exemple suivant liste les étapes à suivre pour activer et exécuter la console de la plate-forme :

1. **Contrôlez ou définissez les paramètres du BIOS.**
2. **Exécutez la commande suivante :**

   ```
   platform set console -s sp -S 19200 -e
   ```

3. **Exécutez la commande suivante :**

   ```
   platform set console
   ```

Codes de retour

TABLEAU F-6 liste les codes de retour pour cette sous-commande.

TABLEAU F-6 Codes de retour de la sous-commande `platform console`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.

Sous-commande platform get console

Description : récupère les informations de configuration relatives à l'accès SP à la console série de la plate-forme.

Format

```
platform get console [{-H|--noheader}] [{-D | --Delim
<SÉPARATEUR>}]
```

Le TABLEAU F-7 liste les arguments de cette sous-commande.

TABLEAU F-7 Arguments de la sous-commande `platform get console`

Argument	Description
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Les puces qui suivent donnent des exemples de la sortie obtenue dans le cadre d'une exécution réussie de cette commande.

- Port série de la plate-forme dirigé sur le panneau arrière :

```
Rear Panel
Platform COMA
```

- Port série de la plate-forme dirigé sur le SP ; port série du SP dirigé sur le panneau arrière, console de la plate-forme désactivée :

```
Rear PanelConsole Redirection
SP ConsoleDisabled
```

- Console de la plate-forme activée :

```
Rear PanelConsole Redirection
SpeedPruningLog Trigger
19200No244 KB
SP ConsoleEnabled
```

Si le port série externe n'est pas connecté à la plate-forme mais l'est à la console du SP, vous pouvez accéder à la console série de la plate-forme en utilisant la sous-commande `platform console`.

Le TABLEAU F-8 liste les informations qui s'affichent, selon si le port série du panneau arrière est connecté à la plate-forme ou au SP.

TABLEAU F-8 Données affichées

Colonne	Description
`Enabled`	Affiche `No` si le port série externe est connecté à la plate-forme. Sinon, le port série externe est connecté à la console du SP ; vous pouvez accéder à la console série de la plate-forme via la ligne de commande du SP en exécutant la sous-commande `platform console`.
`Speed`	Indique la vitesse de communication de la liaison.
`Prune`	Indique si l'élagage des informations de code d'échappement ANSI et en double est activé.
`Log Trigger`	Indique la taille approximative à laquelle se produit la rotation des journaux (par exemple lorsque le fichier `console.0` est supprimé, que le journal courant est transféré dans `console.0` et qu'un nouveau fichier journal est ouvert). L'élagage du contenu du fichier journal n'a lieu qu'en cas de rotation. La taille minimale d'un fichier journal est de 64 Ko ; la taille maximale de 1 024 Ko.

Codes de retour

Le TABLEAU F-9 liste les codes de retour pour cette sous-commande.

TABLEAU F-9 Codes de retour de la sous-commande `platform get console`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

Platform Set Console

Description : vous permet de configurer l'accès du SP à la console série de la plate-forme, définir la vitesse de la connexion et limiter la taille des fichiers journaux créés.

Format

Deux options sont disponibles :

- Configurer le port série externe de sorte qu'il soit connecté à la console série de la plate-forme (configuration par défaut).
- Configurer le port série externe de sorte qu'il soit connecté à la console série du processeur de service.

La configuration par défaut du port série externe le connecte à la console série de la plate-forme. Utilisez la syntaxe suivante pour la configuration par défaut :

```
platform set console {--serial|-s} platform
```

Utilisez la syntaxe suivante pour configurer le port série externe de sorte qu'il se connecte à la console série du SP. Avec cette configuration, vous pouvez accéder à la console série de la plate-forme par le biais de la ligne de commande du SP en exécutant la sous-commande `platform console`.

```
platform set console {--serial|-s} sp
{{--enable|-e}|{--disable|-d}}]
[{{--prune|-p}|{--noprune|-n}}]
[{--speed|-S} {1200|2400|4800|9600|19200|38400|115200}]
[{--log|-l} size]
```

Le TABLEAU F-10 liste les arguments de cette sous-commande.

Remarque – Si `-s` est défini sur la plate-forme, aucun des arguments suivant ne pourra être utilisé.

TABLEAU F-10 Arguments de la sous-commande `platform set console`

Argument	Description
`{-S | --speed} {1200|2400|4800|9600| 19200|38400|115200}`	Sélectionnez la vitesse du port pour la console de la plate-forme. Le BIOS, le SE de la plate-forme et la console doivent tous être configurés à la même vitesse.
`{-d | --disable}`	Indique que le moniteur de la console de la plate-forme est inactif. Ne peut pas être utilisé avec : `-e`.
`{-e | --enable}`	Indique que le moniteur de la console de la plate-forme est actif. Ne peut pas être utilisé avec : `-d`.

TABLEAU F-10 Arguments de la sous-commande `platform set console` *(suite)*

Argument	Description
`{-l | --log} size`	Sélectionne la taille en Ko déclenchant la rotation des journaux de la console. Les valeurs de taille de journal acceptables sont comprises entre 64 et 1 024 inclus.
`{-n | --noprune}`	Indique que le journal de la console de la plate-forme doit contenir des données de console brutes. Ne peut pas être utilisé avec : `-p`.
`{-p | --prune}`	Indique que le journal de la console de la plate-forme va être nettoyé des séquences ANSI et que les informations en double vont en être élaguées. Ne peut pas être utilisé avec : `-n`.
`{-s | --serial} {sp|platform}`	Spécifie si le port série est connecté au port COMA de la plate-forme ou à la console série du SP. Ne peut pas être utilisé avec : `-e` [platform] `-d` [platform] `-p` [platform] `-n` [platform] `-S` [platform] `-l` [platform].

Codes de retour

Le TABLEAU F-11 liste les codes de retour pour cette sous-commande.

TABLEAU F-11 Codes de retour de la sous-commande `platform set console`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	4	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	8	Mémoire insuffisante.
`NWSE_DeviceError`	25	Impossible de lire ou d'écrire sur le périphérique.

Sous-commandes de la plate-forme relatives à l'état du SE

Les sous-commandes listées dans le TABLEAU F-12 permettent de gérer le système d'exploitation (SE).

TABLEAU F-12 Sous-commandes `de la plate-forme relatives à l'état du SE`

Sous-commande	Description
`platform get os state`	Récupère l'état courant du SE de la plate-forme (par exemple : running, booting, off, etc.).
`platform set os state reboot`	Redémarre la plate-forme dans le SE par défaut, la configuration BIOS ou la mise à jour BIOS ou arrête la plate-forme.
`platform set os state boot`	Sert d'alias pour la sous-commande `platform set os state reboot` et ne fonctionne que quand l'état de l'alimentation de la plate-forme est « off » (désactivé).
`platform set os state shutdown`	Arrête la plate-forme.
`platform set os state update bios`	Permet la mise à jour du BIOS de la plate-forme avec un nouveau fichier d'image BIOS local ou distant.

Si la plate-forme est désactivée, la sous-commande `platform set os state reboot` l'active et initialise le SE. Si la plate-forme est déjà en cours d'exécution, cette commande redémarre le SE. La sous-commande `platform set os state reboot` attend que la plate-forme s'initialise.

La sous-commande `platform set power state` assure que la plate-forme est en cours d'exécution. Elle n'a aucun effet sur la plate-forme si celle-ci est en cours d'exécution ; elle la met sous tension et initialise le SE si elle est désactivée. La sous-commande `platform set power state` attend uniquement que l'alimentation soit activée. (Voir « Sous-commandes de la plate-forme relatives à l'état de l'alimentation », page 216).

Sous-commande platform get os state

Description : récupère l'état courant du SE de la plate-forme.

Format

```
platform get os state
```

Les valeurs d'état courant sont les suivantes :

- Off
- On
- Communicating
- Diagnostics
- Sleeping
- BIOS booting
- BIOS setup
- OS booting
- OS shutting down

Lorsque l'état de la plate-forme est *Communicating* (état dans lequel le SE communique avec le SP) et que les pilotes de la plate-forme sont désinstallés, le SP reste dans l'état *Communicating* même s'il ne peut plus communiquer avec la plate-forme.

Pour plus d'informations sur la définition de l'état, voir « Sous-commandes platform set os state », page 210.

Codes de retour

Le TABLEAU F-13 liste les codes de retour pour cette sous-commande.

TABLEAU F-13 Codes de retour de la sous-commande `platform get os state`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.

Sous-commandes platform set os state

Ce groupe de sous-commandes permet de redémarrer la plate-forme dans le SE par défaut, la configuration BIOS ou la mise à jour BIOS ou d'arrêter la plate-forme. Redémarrer en mode de configuration du BIOS permet de configurer les paramètres du BIOS tandis que le faire en mode de mise à jour du BIOS vous permet de reflasher l'image du BIOS.

Pour arrêter la plate-forme, les pilotes de la plate-forme doivent être installés (sauf si vous utilisez l'argument `-f`). Utiliser cette sous-commande vous permet d'arrêter progressivement la plate-forme et permet au SE de couper l'alimentation.

platform set os state reboot

Description : vous permet de redémarrer la plate-forme. Si la plate-forme est déjà en cours d'exécution, cette sous-commande redémarre le SE.

Format

```
platform set os state reboot [{-W | --nowait}]
[{-b | --bios}] [{-d | --device}][{-f|--forced}] [-q | --quiet]
```

Le TABLEAU F-14 liste les arguments de cette sous-commande.

TABLEAU F-14 Arguments de la sous-commande `platform set os state reboot`

Argument	Description
`[-W | --nowait]`	Si spécifié, la sous-commande retourne immédiatement les informations voulues au lieu d'attendre la fin de l'opération.
`[-b | --bios]`	Retourne à BIOS Setup. Vous permet de changer les paramètres du BIOS. Ne peut pas être utilisé avec : `-d`.
`[-d | --device]`	Fait que le BIOS tente d'abord d'utiliser le périphérique spécifié comme périphérique d'initialisation, avant de revenir à l'ordre d'initialisation du BIOS configuré. Le seul argument de périphérique pris en charge actuellement est le réseau. En spécifiant « –device network », le BIOS tentera une initialisation réseau via PXE. Ne peut pas être utilisé avec l'argument : -b.
`{-f | --forced}`	Entraîne une mise hors tension matérielle. Force la mise hors tension ou réinitialise le serveur : • au bout d'un délai d'attente de plusieurs minutes si la plate-forme n'a pas répondu ou • immédiatement si la plate-forme n'est pas dans l'état SE en cours d'exécution (aucun pilote n'a été installé ou le serveur s'est arrêté brusquement).
`[-q | --quiet]`	Supprime les messages d'avertissement interactifs. Aucun message d'erreur n'est bloqué.

Codes de retour

Le TABLEAU F-15 liste les codes de retour pour cette sous-commande.

TABLEAU F-15 Codes de retour de la sous-commande `platform set os state reboot`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.
`NWSE_Busy`	9	Périphérique ou ressource occupé.
`NWSE_FileError`	18	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.
`NWSE_InvalidOpForState`	22	Opération incorrecte pour l'état courant.

platform set os state boot

Description : Sert d'alias pour la sous-commande `platform set os state reboot`. Fonctionne uniquement lorsque l'état de l'alimentation de la plate-forme est « off » (désactivé).

Format

```
platform set os state boot [{-W | --nowait}]
[{-b | --bios}] [{-d|--device}] [{-f|--forced}] [-q | --quiet]
```

Le TABLEAU F-16 liste les arguments de cette sous-commande.

TABLEAU F-16 Arguments de la sous-commande `platform set os state boot`

Argument	Description
`[-W | --nowait]`	Si spécifié, la sous-commande retourne immédiatement les informations voulues au lieu d'attendre la fin de l'opération.
`[-b | --bios]`	L'initialisation ouvre sur la configuration du BIOS et non pas sur le SE. Ne peut pas être utilisé avec : -d.
`[-d|--device]`	Fait que le BIOS tente d'abord d'utiliser le périphérique spécifié comme périphérique d'initialisation, avant de revenir à l'ordre d'initialisation du BIOS configuré. Le seul argument de périphérique pris en charge actuellement est le réseau. En spécifiant « –device network », le BIOS tentera une initialisation réseau via PXE. Ne peut pas être utilisé avec l'argument : -b.
`{-f | --forced}`	Entraîne une mise hors tension matérielle. Cette option est ignorée
`[-q | --quiet]`	Supprime les messages d'avertissement interactifs. Aucun message d'erreur n'est bloqué.

Codes de retour

Le TABLEAU F-17 liste les codes de retour pour cette sous-commande.

TABLEAU F-17 Codes de retour de la sous-commande `platform set os state boot`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.
`NWSE_Busy`	9	Périphérique ou ressource occupé.
`NWSE_InvalidOpForState`	22	Opération incorrecte pour l'état courant.

platform set os state shutdown

Description : vous permet d'arrêter la plate-forme. Cette action exige que les pilotes de la plate-forme soient installés à moins que vous n'exécutiez cette sous-commande avec l'argument `-f`.

Format

```
platform set os state shutdown [{-W | --nowait}]
[{-f|--forced}] [-q | --quiet]
```

Le TABLEAU F-18 liste les arguments de cette sous-commande.

TABLEAU F-18 Arguments de la sous-commande `platform set os state shutdown`

Argument	Description
`[-W | --nowait]`	Si spécifié, la sous-commande retourne immédiatement les informations voulues au lieu d'attendre la fin de l'opération.
`{-f | --forced}`	Entraîne une mise hors tension matérielle. Force la mise hors tension ou réinitialise le serveur : • au bout d'un délai d'attente de plusieurs minutes si la plate-forme n'a pas répondu ou • immédiatement si la plate-forme n'est pas dans l'état SE en cours d'exécution (aucun pilote n'a été installé ou le serveur s'est arrêté brusquement).
`[-q | --quiet]`	Supprime les messages d'avertissement interactifs. Aucun message d'erreur n'est bloqué.

Codes de retour

Le TABLEAU F-19 liste les codes de retour pour cette sous-commande.

TABLEAU F-19 Codes de retour de la sous-commande `platform set os state shutdown`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.

TABLEAU F-19 Codes de retour de la sous-commande `platform set os state shutdown` *(suite)*

Code de retour	ID	Description
`NWSE_Busy`	9	Périphérique ou ressource occupé.
`NWSE_FileError`	18	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.
`NWSE_InvalidOpForState`	22	Opération incorrecte pour l'état courant.

platform set os state update-bios

Description : Vous permet de mettre à jour le BIOS de la plate-forme avec un nouveau fichier d'image BIOS local ou distant.

Format

```
platform set os state update-bios {-f| --filename} IMAGE BIOS
{-i| --ipaddress} ADRESSE_DISTANTE {-r| --remote} VERSION_DISTANTE
[{-p| --port} PORT_DISTANT] [{-W| --nowait}] [{-q| --quiet}]
```

Le TABLEAU F-20 liste les arguments de cette sous-commande.

TABLEAU F-20 Arguments de la sous-commande `platform set os state update-bios`

Argument	Description
`{-f | --filename}`	Indique le nom du fichier contenant la nouvelle image de BIOS à utiliser pour la mise à jour du BIOS.
`{-i | --ipaddress}`	Adresse IP du serveur sur lequel le serveur de mise à jour (application java) est en cours d'exécution.
`{-r | --remote}`	Spécifiez une version (par exemple, V1.2.3.4) ou utilisez LATEST pour effectuer la mise à jour en utilisant la dernière version disponible sur le serveur de mise à jour.
`{-p | --port}`	*(facultatif)* Numéro du port du serveur distant sur lequel le programme `java sp update` écoute les requêtes de mise à jour de la flash du SP. Si ce numéro de port n'est pas indiqué, la commande essaie de se connecter au port par défaut. La valeur par défaut est 52 708 secondes.
`[-W | --nowait]`	Si spécifié, la sous-commande retourne immédiatement les informations voulues au lieu d'attendre la fin de l'opération.
`[-q | --quiet]`	Supprime les messages d'avertissement interactifs. Aucun message d'erreur n'est bloqué.

Si la plate-forme est désactivée, la sous-commande `platform set os state reboot` l'active et initialise le SE. Si la plate-forme est déjà en cours d'exécution, cette commande redémarre le SE. La sous-commande `platform set os state reboot` attend que la plate-forme s'initialise.

La sous-commande `platform set power state` assure que la plate-forme est en cours d'exécution. Elle n'a aucun effet sur la plate-forme si celle-ci est en cours d'exécution ; elle la met sous tension et initialise le SE si elle est désactivée. La sous-commande `platform set power state` attend uniquement que l'alimentation soit activée. (Voir « Sous-commandes de la plate-forme relatives à l'état de l'alimentation », page 216).

Codes de retour

Le TABLEAU F-21 liste les codes de retour pour cette sous-commande.

TABLEAU F-21 Arguments de la sous-commande `platform set os state update-bios`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NotFound`	5	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.
`NWSE_FileError`	18	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.
`NWSE_InvalidOpForState`	22	Opération incorrecte pour l'état courant.
`NWSE_ServiceNotAvailable`	24	Le service demandé n'est pas disponible.

Sous-commandes de la plate-forme relatives à l'état de l'alimentation

Les sous-commandes listées dans le TABLEAU F-22 permettent de gérer l'alimentation de la plate-forme.

TABLEAU F-22 Sous-commandes `Platform Power State`

Sous-commande	Description
`platform get power state`	Permet de déterminer l'état de l'alimentation de la plate-forme (par exemple, si elle est activée ou désactivée).
`platform set power state`	Permet d'activer/désactiver l'alimentation de la plate-forme.

La sous-commande `platform set power state` n'a aucun effet sur la plate-forme si celle-la est déjà en cours d'exécution ; si la plate-forme est désactivée, elle la met sous tension et initialise le SE. En d'autres mots, la sous-commande `platform set power state` assure que la plate-forme est activée mais ne la redémarre pas si elle n'est pas activée.

La sous-commande `platform set os state` attend uniquement que la plate-forme s'initialise ; la sous-commande `platform set power state` attend la mise sous tension.

Sous-commande platform get power state

Description : Permet de déterminer l'état de l'alimentation de la plate-forme depuis un script (par exemple, si la plate-forme est activée ou désactivée).

Format

```
platform get power state
```

Codes de retour

Le TABLEAU F-23 liste les codes de retour pour cette sous-commande.

TABLEAU F-23 Codes de retour de la sous-commande `platform get power state`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.

Sous-commande platform set power state

Description : Vous permet d'activer/désactiver l'alimentation de la plate-forme depuis un script. Cette sous-commande n'informe pas le SE de la requête au travers des canaux fournis.

La sous-commande `platform set power state` coupe brusquement l'alimentation ou force la plate-forme à lancer un arrêt pour panique.

Elle revient au même qu'à appuyer sur la bouton d'alimentation pendant moins de une seconde ou pendant plus de cinq secondes (argument `-f`).

Remarque – Des commandes moins destructrices mais tout aussi efficaces sont disponibles. Si les pilotes de la plate-forme sont installés, utilisez la sous-commande `platform set os state shutdown` pour arrêter progressivement le serveur. Pour plus d'informations, voir « platform set os state shutdown », page 213.

Format

```
platform set power state [{-W|--nowait}] [{-f|--forced}]
[{-t|--timeout} TEMPS] {off|on|cycle}
```

Le TABLEAU F-24 liste les arguments de cette sous-commande.

TABLEAU F-24 Arguments de la sous-commande `platform set power state`

Argument	Description
`{-W | --nowait}`	Si spécifié, la commande retourne immédiatement les informations voulues au lieu d'attendre la fin de l'opération.
`{-f | --forced}`	Entraîne une mise hors tension matérielle.
`{-t | --timeout}`	Spécifie le délai d'attente maximal pendant lequel le système attend que l'opération se termine (en secondes).
`{off | on | cycle}`	Spécifie si activer/désactiver l'alimentation de la plate-forme ou soumettre cette dernière à un cycle d'alimentation. Spécifier l'argument cycle entraîne la mise hors tension puis sous tension de la plate-forme.

Si la plate-forme est désactivée, la sous-commande `platform set os state reboot` l'active et initialise le SE. Si la plate-forme est déjà en cours d'exécution, cette commande redémarre le SE. La sous-commande `platform set os state reboot` attend que la plate-forme s'initialise (voir « Sous-commandes platform set os state », page 210).

La sous-commande `platform set power state` assure que la plate-forme est en cours d'exécution. Elle n'a aucun effet sur la plate-forme si celle-ci est en cours d'exécution ; elle la met sous tension et initialise le SE si elle est désactivée. La sous-commande `platform set power state` attend uniquement que l'alimentation soit activée.

Codes de retour

Le TABLEAU F-25 liste les codes de retour pour cette sous-commande.

TABLEAU F-25 Codes de retour de la sous-commande `platform set power state`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_MissingArgument`	`7`	Argument(s) manquant(s).
`NWSE_TimedOut`	`23`	Opération arrivée à échéance.

Sous-commande platform get hostname

Description : Affiche le nom d'hôte de la plate-forme courante principale. Les données ne sont actualisées que lorsque la plate-forme est redémarrée.

Format

```
platform get hostname [{-H|--noheader}]
```

Le TABLEAU F-26 liste les arguments pour cette sous-commande.

TABLEAU F-26 Arguments de la sous-commande `platform get hostname`

Argument	Description
`{-H | --noheader}`	Supprime les titres des colonnes.

Codes de retour

Le TABLEAU F-27 liste les codes de retour pour cette sous-commande.

TABLEAU F-27 Codes de retour de la sous-commande `platform get hostname`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_Busy`	`9`	Périphérique ou ressource occupé.
`NWSE_RPCConnected`	`11`	Client RPC déjà connecté.
`NWSE_RPCConnRefused`	`12`	Connexion RPC refusée.
`NWSE_NoRouteToHost`	`13`	Pas de route vers l'hôte (réseau hors service).
`NWSE_HostDown`	`14`	Hôte hors service.

Sous-commande platform get mac

Description : Retourne les adresses MAC des deux NIC embarquées de la plate-forme.

Format

```
platform get mac
```

Codes de retour

Le TABLEAU F-28 liste les codes de retour pour cette sous-commande.

TABLEAU F-28 Codes de retour de la sous-commande `platform get mac`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande platform get product id

Description : Affiche l'ID de produit du système courant.

Format

```
platform get product-id
```

Remarque – Vous pouvez aussi récupérer l'ID du produit, le numéro de révision de la carte et le numéro de révision PRS en exécutant les sous-commandes `sensor get` et `inventory get hardware`.

Codes de retour

Le TABLEAU F-29 liste les codes de retour pour cette sous-commande.

TABLEAU F-29 Codes de retour de la sous-commande `platform get product-id`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NotFound`	`5`	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_FileError`	`18`	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

ANNEXE **G**

Commandes relatives aux capteurs

La commande `sensor` rapporte ou définit la valeur d'un capteur ou d'un dispositif de contrôle environnemental.

Le TABLEAU G-1 liste les sous-commandes de `sensor`.

Remarque – Chaque sous-commande retourne un code de retour à la fin de l'opération.

TABLEAU G-1 Sous-commandes relatives aux capteurs

Sous-commande	Description
`sensor get`	Retourne toutes les données associées à un capteur.
`sensor set`	Définit certaines des données associées à un capteur spécifique ou à une catégorie de capteurs.

Remarque – Il y a des capteurs dont les valeurs ne changent pas, d'autres qui sont là pour fournir des informations en cas de problème et d'autres encore qui facilitent le bon fonctionnement du logiciel.

Nombre de ces capteurs n'ont pas de composant connexe (parent) associé. Par exemple, dans le cas d'un capteur de température de mort de CPU, la CPU est le composant parent et dans celui d'un capteur de vitesse de ventilateur, le ventilateur est le composant parent tandis que pour un capteur d'ID de produit, seule une valeur statique est retournée et il n'y a pas de relation de parenté.

Cette relation établit le ou les composants qui sont affectés par les changements de valeur du capteur. Vous ne pouvez pas modifier les seuils des capteurs qui n'ont pas de relation de parenté puisqu'aucun événement lié au dépassement de ces seuils ne surviendra jamais.

Sous-commande sensor get

Description : Retourne toutes les données associées à un capteur.

Par défaut, seul l'ID du capteur et sa valeur courante s'affichent. Vous pouvez spécifier sur la ligne de commande l'ordre des données dans la sortie.

Remarque – Le champ *identifier* s'affiche toujours en premier sauf si vous le supprimez avec l'option `-I` .

Format

```
sensor get [{{-i | --id} ID | {-t | --type} ID_TYPE}]
[{-v | --value}] [{-n | --nominal}]
[{-C | --crithigh}] [{-c | --critlow}]
[{-W | --warnhigh}] [{-w | --warnlow}]
[{-N | --name}] [{-d | --description}]
[{-S | --sensor-type}] [{-p | --parent-comp}]
[{-s | --severity}] | [{--verbose}]
[{-I | --noid}] [{-H | noheader}]
[{-D | --Delim <SÉPARATEUR>}]
```

Le TABLEAU G-2 liste les arguments de cette sous-commande.

TABLEAU G-2 Arguments de la sous-commande `sensor get`

Argument	Description
`{-i | --id}`	ID_CAPTEUR, ID_PRODUIT, RÉVISION_CARTE, RÉVISION_PRS Spécifie le capteur pour lequel vous désirez obtenir des données. Vous pouvez spécifier cet argument plusieurs fois, cas dans lequel les données des capteurs sont rapportées dans l'ordre indiqué. Vous pouvez aussi récupérer l'ID du produit, le numéro de révision de la carte et le numéro de révision PRS en utilisant cet indicateur. Spécifiez `[-vIH]` suivi de l'ID pour convertir la sortie en fonction de l'ID de produit approprié. Par exemple, l'ID de produit 255 correspond au serveur 2100 et l'ID de produit 239 au serveur 4300. Vous pouvez aussi obtenir ces informations en exécutant la commande `inventory get hardware`.
`{-t | --type }`	Spécifie la catégorie de capteurs pour laquelle vous désirez obtenir des données. Vous pouvez spécifier cet argument plusieurs fois, cas dans lequel la sortie des capteurs est regroupée par type dans l'ordre indiqué. Les catégories de capteurs sont les suivantes : tension, ventilateur, température, alimentation et commutateur.
`{-v | --value}`	Affiche la valeur courante du capteur.
`{-n | --nominal}`	Affiche la valeur nominale du capteur.
`{-C | --crithigh}`	Affiche la valeur du seuil *critical high* (supérieur critique) du capteur. Les seuils configurés sur une valeur autre que celle par défaut définie en usine s'affichent suivis d'un astérisque (`*`).
`{-c | --critlow}`	Affiche la valeur du seuil *critical low* (inférieur critique) du capteur.
`{-W | --warnhigh}`	Affiche la valeur du seuil *warning high* (supérieur avertissement) du capteur.
`{-w | --warnlow}`	Affiche la valeur du seuil *warning low* (inférieur avertissement) du capteur.
`{-N | --name}`	Affiche le nom du capteur.
`{-d | --description}`	Affiche une description du capteur.
`{-S | --sensor-type}`	Affiche le type du capteur (à utiliser avec `--type`).
`{-p | --parent-comp}`	Affiche la liste des composants parents du capteur. Il s'agit des composants qui sont affectés par les changements de valeur d'un capteur (par exemple, les composants qui changent la gravité en cas de changement de gravité du capteur).
`{-s | --severity}`	Affiche le niveau de gravité courant du capteur (nominal, avertissement ou critique).

TABLEAU G-2 Arguments de la sous-commande `sensor get` *(suite)*

Argument	Description
`{--verbose}`	Affiche toutes les colonnes ; cet argument ne peut être utilisé avec aucune des autres options de colonne supplémentaires.
`{-I | --noid}`	Supprime l'affichage de la colonne de l'ID du capteur. Par défaut, cette colonne s'affiche toujours lorsque plusieurs capteurs sont sélectionnés.
`[-H | --noheader]`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU G-3 liste les arguments de cette sous-commande.

Remarque – Il y a des capteurs dont les valeurs ne changent pas, d'autres qui sont là pour fournir des informations en cas de problème et d'autres encore qui facilitent le bon fonctionnement du logiciel.

Nombre de ces capteurs n'ont pas de composant connexe (parent) associé. Par exemple, dans le cas d'un capteur de température de mort de CPU, la CPU est le composant parent et dans celui d'un capteur de vitesse de ventilateur, le ventilateur est le composant parent tandis que pour un capteur d'ID de produit, seule une valeur statique est retournée et il n'y a pas de relation de parenté.

Cette relation établit le ou les composants qui sont affectés par les changements de valeur du capteur. Vous ne pouvez pas modifier les seuils des capteurs qui n'ont pas de relation de parenté puisqu'aucun événement lié au dépassement de ces seuils ne surviendra jamais.

TABLEAU G-3 Codes de retour de la sous-commande `sensor get`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.

TABLEAU G-3 Codes de retour de la sous-commande `sensor get` *(suite)*

Code de retour	ID	Description
NWSE_RPCNotConnected	3	Connexion au serveur RPC impossible.
NWSE_InvalidArgument	4	Un ou plusieurs arguments étaient incorrects ou invalides.
NWSE_NotFound	5	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
NWSE_NoPermission	6	Pas autorisé à effectuer cette opération.

Sous-commande sensor set

Description : permet de définir certaines des données associées à un capteur spécifique ou à une catégorie de capteurs.

Format

```
sensor set [{-i | --id} ID_CAPTEUR [{-i | --id} ID_CAPTEUR] …]
{[{-C | --crithigh} VALEUR] [[{-c | --critlow} VALEUR]
[{-W | --warnhigh] VALEUR] [{-w | --warnlow} VALEUR] [{-v | --value}
{on|off}] | {-r | --reset}}
```

```
sensor set [{-t | --type] ID_TYPE] {[{-C | --crithigh} VALEUR]
[[{-c| --critlow} VALEUR] [{-W | --warnhigh] VALEUR] [{-w | --warnlow}
VALEUR] [{-v | --value} {on|off}] | {-r | --reset}}
```

```
sensor set [{-R | --resetall}]
```

Le TABLEAU G-4 liste les arguments de cette sous-commande.

TABLEAU G-4 Arguments de la sous-commande `sensor set`

Argument	Description
`{-i | --id}`	Spécifie le capteur spécifique objet de la ou des opérations. Vous pouvez spécifier plusieurs capteurs en répétant `--id`.
`{-t | --type }`	Spécifie la catégorie de capteurs objet de la ou des opérations (par exemple : ventilateur, tension, etc.).
`{-C | --crithigh}`	Spécifie la valeur du seuil *critical high* (supérieur critique) du capteur. • Définir la chaîne sur `clear` désactive le seuil. • Définir la chaîne sur `reset` définit la valeur sur la valeur d'origine spécifiée en usine. • Si la valeur spécifiée se termine par le signe des pour cent (%), le seuil est défini sur le pourcentage correspondant de la valeur nominale du capteur. • Toute autre valeur est interprétée comme la valeur courante sur laquelle définir le seuil.
`{-c | --critlow}`	Spécifie la valeur du seuil *critical low* (inférieur critique) du capteur. Définir la chaîne sur `clear` désactive le seuil.
`{-W | --warnhigh}`	Spécifie la valeur du seuil *warning high* (supérieur avertissement) du capteur. Définir la chaîne sur `clear` désactive le seuil.
`{-w | --warnlow}`	Spécifie la valeur du seuil *warning low* (inférieur avertissement) du capteur. Définir la chaîne sur `clear` désactive le seuil.
`{-v | --value}`	Définit la valeur du capteur.
`{-r | --reset}`	Ramène tous les seuils du ou des capteurs spécifiés aux valeurs par défaut définies en usine.
`{-R | --resetall}`	Ramène tous les seuils de tous les capteurs aux valeurs par défaut définies en usine.

Codes de retour

Le TABLEAU G-5 liste les arguments de cette sous-commande.

Remarque – Il y a des capteurs dont les valeurs ne changent pas, d'autres qui sont là pour fournir des informations en cas de problème et d'autres encore qui facilitent le bon fonctionnement du logiciel.

Nombre de ces capteurs n'ont pas de composant connexe (parent) associé. Par exemple, dans le cas d'un capteur de température de mort de CPU, la CPU est le composant parent et dans celui d'un capteur de vitesse de ventilateur, le ventilateur est le composant parent tandis que pour un capteur d'ID de produit, seule une valeur statique est retournée et il n'y a pas de relation de parenté.

Cette relation établit le ou les composants qui sont affectés par les changements de valeur du capteur. Vous ne pouvez pas modifier les seuils des capteurs qui n'ont pas de relation de parenté puisqu'aucun événement lié au dépassement de ces seuils ne surviendra jamais.

TABLEAU G-5 Codes de retour de la sous-commande `sensor set`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NotFound`	`5`	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

ANNEXE **H**

Commandes du processeur de service

La commande `sp` récupère ou définit les valeurs de configuration du processeur de service, génère ou gère des événements et des avis, ou ajoute et modifie des abonnés, des routes d'événements et des groupes de -notification par e-mail pour le gestionnaire d'événements du SP.

Le TABLEAU H-1 liste les groupes de sous-commandes de la commande `sp`.

Remarque – Chaque sous-commande retourne un code de retour à la fin de l'opération.

TABLEAU H-1 Groupes de sous-commandes du processeur de service

Sous-commande	Description
`Date`	Définit ou récupère la date et l'heure de la RTC du SP.
`DNS`	Affiche ou configure la configuration du client DNS sur le SP.
`Events`	Retourne des informations détaillées ou efface un événement.
`Hostname`	Affiche ou réinitialise le nom d'hôte ou le nom de domaine du SP.
`IP`	Définit, modifie ou récupère la configuration réseau du SP.
`JNET Address`	Définit ou récupère l'adresse jnet.
`Locate Light`	Définit l'état ou lit la valeur du commutateur du voyant de localisation.
`Logfile`	Récupère ou configure le fichier journal d'événements.
`Adresse MAC`	récupère l'adresse MAC du SP.
`Miscellaneous`	Lit le statut d'un composant, récupère le dernier code POST du port 80, rétablit les valeurs par défaut des paramètres, stocke les données dans le format tar compressé ou capture les données de débogage.

TABLEAU H-1 Groupes de sous-commandes du processeur de service *(suite)*

Sous-commande	Description
`Mount`	Affiche, crée, réinitialise ou supprime un point de montage.
`SMTP`	Gère les informations relatives à l'expédition d'e-mails SMTP.
`SNMP`	Gère les fonctions SNMP.
`SSL`	Gère les fonctions SSL.
`Update Flash`	Définit l'indicateur de mise à jour pour démarrer une mise à jour complète de la flash ou copie le fichier Value-Add dans le composant Value-Add de la flash du SP.

Sous-commandes du SP relatives à la date

Les sous-commandes du TABLEAU H-2 gèrent la date et l'heure sur le SP.

TABLEAU H-2 Sous-commandes `SP Date`

Sous-commande	Description
`sp get date`	Récupère la date et l'heure de la RTC du SP.
`sp set date`	Définit la date et l'heure sur la RTC du SP.

Sous-commande sp get date

Description : Récupère la date et l'heure de la RTC du SP.

Format

```
sp get date
```

Codes de retour

Le TABLEAU H-3 liste les codes de retour pour cette sous-commande.

TABLEAU H-3 Codes de retour de la sous-commande `sp get date`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.

Sous-commande sp set date

Description : Définit la date et l'heure sur la RTC du SP.

Format

`sp set date` *`CHAÎNE DATE`*

Le TABLEAU H-4 liste les arguments pour cette sous-commande.

TABLEAU H-4 Arguments de la sous-commande `sp set date`

Argument	Description
`CHAÎNE DATE`	Spécifie la date et l'heure sur la RTC du SP. La chaîne de date est une date UTC de la forme AAAA-MM-JJ HH:MM:SS.

Vous pouvez utiliser cette commande pour définir au départ la RTC de la plate-forme après une coupure de l'alimentation de secours CMOS. Si la plate-forme est dans l'état dans lequel le système d'exploitation (SE) communique avec le SP, l'heure de la plate-forme supplantera l'heure du SP, ce qui permettra aux heures des événements de la plate-forme et du SP d'être synchronisées dans le journal d'événements.

Codes de retour

Le TABLEAU H-5 liste les codes de retour de cette sous-commande.

TABLEAU H-5 Codes de retour de la sous-commande `sp set date`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_FileError`	`18`	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.

Sous-commandes du SP relatives à DNS

Les sous-commandes du TABLEAU H-6 gèrent la configuration DNS sur le SP.

TABLEAU H-6 Sous-commandes `SP DNS`

Sous-commande	Description
`sp disable dns`	Désactive la configuration DNS sur le SP.
`sp enable dns`	Configure la configuration DNS sur le SP.
`sp get dns`	Affiche la configuration DNS courante sur le SP.

Sous-commande sp disable dns

Description : désactive la configuration DNS sur le SP.

```
sp disable dns
```

Lorsque le SP est configuré pour utiliser DHCP, DHCP configure automatiquement les paramètres DNS. Les changements apportés aux paramètres DNS dans cette configuration peuvent être remplacés avec le client DHCP.

Codes de retour

TABLEAU H-7 liste les codes de retour de cette commande :

TABLEAU H-7 Codes de retour de la sous-commande `sp disable dns`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

Sous-commande sp enable dns

Description : configure la configuration DNS sur le SP.

Vu que les applications ne voient pas les configurations d'interpréteur DNS (dans `/etc/resolv.conf`) tant qu'elles ne sont pas redémarrées, cette commande redémarre les processus serveurs qui dépendent de DNS. Ce terme inclut actuellement le démon `sshd` et le Gestionnaire de la sécurité.

Format

`sp enable dns { -n | --nameserver}` *`IP NOMSERVEUR…`*
`{-s | --searchdomain }` *`DOMAINE RECHERCHE…`*

Le TABLEAU H-8 liste les arguments de cette sous-commande.

TABLEAU H-8 Arguments de la sous-commande `sp enable dns`

Argument	Description
`{ -n | --nameserver}`	Affiche les adresses IP du nom de serveur en question. S'il y en a plusieurs, elles s'affichent sur des lignes séparées.
`{ -s | --searchdomain }`	Affiche le ou les domaines de recherche. S'il y en a plusieurs, ils s'affichent sur des lignes séparées.

Codes de retour

Le TABLEAU H-9 liste les codes de retour pour cette sous-commande.

TABLEAU H-9 Codes de retour de la sous-commande `sp enable dns`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

Sous-commande sp get dns

Description : affiche la configuration DNS courante sur le SP.

Format

```
sp get dns [{-n | --nameserver } | -s | --searchdomain } |
{-H | --noheader }] [{-D | --Delim <SÉPARATEUR>}]
```

Le TABLEAU H-10 liste les arguments de cette sous-commande.

TABLEAU H-10 Arguments de la sous-commande `sp get dns`

Argument	Description
`{ -n | --nameserver}`	Affiche le ou les serveur(s) de noms. S'il y en a plusieurs, ils s'affichent sur des lignes séparées.
`{ -s | --searchdomain }`	Affiche le ou les domaines de recherche. S'il y en a plusieurs, ils s'affichent sur des lignes séparées.
`{-H | --noheader}`	Supprime les titres des colonnes.
`[{-D | --Delim <SÉPARATEUR>}]`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU H-11 liste les codes de retour pour cette sous-commande.

TABLEAU H-11 Codes de retour de la sous-commande `sp get dns`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.

Sous-commandes du SP relatives aux événements

Les sous-commandes du TABLEAU H-12 gèrent les événements sur le SP.

TABLEAU H-12 Sous-commandes `SP Events`

Sous-commande	Description
`sp delete event`	Efface un événement existant en utilisant son ID d'événement.
`sp get events`	Retourne des informations détaillées sur tous les événements actifs du SP.

Sous-commande sp delete event

Description : efface un événement existant en utilisant son ID d'événement.

Format

```
sp delete event { ID ÉVÉNEMENT | {-a | --all}} [-q | --quiet]
```

Le TABLEAU H-13 liste les arguments de cette sous-commande.

TABLEAU H-13 Arguments de la sous-commande `sp delete event`

Argument	Description
`ID ÉVÉNEMENT`	Spécifie l'événement existant à effacer. Cet argument peut être répété pour supprimer plusieurs événements à la fois.
`[-a | --all]`	Supprime tous les événements.
`[-q | --quiet]`	Cet argument spécifie qu'aucune erreur ne sera retournée si l'événement à supprimer est introuvable.

Codes de retour

TABLEAU H-14 liste les codes de retour pour cette sous-commande.

TABLEAU H-14 Arguments de la sous-commande `sp delete event`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NotFound`	5	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	8	Mémoire insuffisante.
`NWSE_InvalidOpForState`	22	Opération incorrecte pour l'état courant.

Sous-commande sp get events

Description : retourne des informations détaillées sur tous les événements actifs du SP. Par défaut, l'ID de l'événement, la dernière mise à jour, le composant, la gravité et un message s'affichent.

Les administrateurs peuvent afficher des informations détaillées sur tous les événements système couramment actifs et effectuer diverses actions liées à chaque événement.

Vous pouvez afficher ces informations en utilisant cette commande. Pour la liste de tous les événements possibles, voir le TABLEAU 3-4 au chapitre 3.

Format

```
sp get events [ {-i | --id} <ID ÉVÉNEMENT> ] [{-d | --detail} ]
[{ -v | --verbose}] [{-H | noheader}][{-D | --Delim <SÉPARATEUR>}]
```

Le TABLEAU H-15 liste les arguments de cette sous-commande.

TABLEAU H-15 Arguments de la sous-commande `sp get events`

Argument	Description
`{-i | --id}`	Spécifie de limiter l'affichage des informations à l'événement en question ; sinon des informations sur tous les événements existants sont retournées.
`{-d | --detail}`	Spécifier d'afficher l'historique d'un ou de tous les événements.
`{ -v | --verbose }`	Spécifie d'afficher toutes les colonnes.
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Indique d'utiliser le séparateur spécifié pour délimiter les colonnes. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

TABLEAU H-16 liste les codes de retour pour cette sous-commande.

TABLEAU H-16 Codes de retour de la sous-commande `sp get events`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NotFound`	`5`	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.

Sous-commandes du SP relatives au nom de l'hôte

Les sous-commandes du TABLEAU H-17 gèrent l'hôte du SP et le domaine.

TABLEAU H-17 Sous-commandes `SP Hostname`

Sous-commande	Description
`sp get hostname`	Affiche le nom de l'hôte courant et, en option, le nom du domaine du SP.
`sp set hostname`	redéfinit le nom de l'hôte ou le nom du domaine du SP au nom spécifié.

Sous-commande sp get hostname

Description : affiche le nom de l'hôte courant et, en option, le nom du domaine du SP. Ce nom est utilisé par de nombreux programmes de mise en réseau pour identifier la machine. Il l'est également pour identifier un sous-répertoire de journalisation pour les journaux d'événements.

Format

```
sp get hostname [-f | --fqdn]
```

Le TABLEAU H-18 liste les arguments pour cette sous-commande.

TABLEAU H-18 Arguments de la sous-commande `sp get hostname`

Argument	Description
`[-f | --fqdn]`	Entraîne l'affichage du nom complet de l'hôte.

Codes de retour

Le TABLEAU H-19 liste les codes de retour pour cette sous-commande.

TABLEAU H-19 Codes de retour de la sous-commande `sp get hostname`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_Busy`	`9`	Périphérique ou ressource occupé.
`NWSE_RPCConnected`	`11`	Client RPC déjà connecté.
`NWSE_RPCConnRefused`	`12`	Connexion RPC refusée.
`NWSE_NoRouteToHost`	`13`	Pas de route vers l'hôte (réseau hors service).
`NWSE_HostDown`	`14`	Hôte hors service.

Sous-commande sp set hostname

Description : redéfinit le nom de l'hôte ou le nom du domaine du SP au nom spécifié. Ce nom est utilisé par de nombreux programmes de mise en réseau pour identifier la machine.

Format

`sp set hostname` *`NOMHÔTE`*

Le TABLEAU H-20 liste les arguments pour cette sous-commande.

TABLEAU H-20 Arguments de la sous-commande `sp set hostname`

Argument	Description
`NOMHÔTE`	Spécifie le nom de l'hôte à définir.

Codes de retour

Le TABLEAU H-21 liste les codes de retour pour cette sous-commande.

TABLEAU H-21 Codes de retour de la sous-commande `sp set hostname`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_Busy`	`9`	Périphérique ou ressource occupé.
`NWSE_RPCConnected`	`11`	Client RPC déjà connecté.
`NWSE_RPCConnRefused`	`12`	Connexion RPC refusée.
`NWSE_NoRouteToHost`	`13`	Pas de route vers l'hôte (réseau hors service).
`NWSE_HostDown`	`14`	Hôte hors service.

Sous-commandes du SP relatives à IP

Les sous-commandes du TABLEAU H-22 gèrent la configuration réseau du SP.

TABLEAU H-22 Sous-commandes `SP IP`

Sous-commande	Description
`sp get ip`	Récupère les informations de configuration du réseau basé sur Ethernet pour le SP.
`sp set ip`	Définit ou modifie la configuration réseau du SP.

Sous-commande sp get ip

Description : récupère les informations de configuration du réseau basé sur Ethernet pour le SP, adresse IP, masque réseau et passerelle compris. En sus, elle indique si le SP est configuré pour utiliser DHCP ou une adresse IP statique.

Format

`sp get ip [-H | noheader] [{-D | --Delim <`*`SÉPARATEUR`*`>}]`

Le TABLEAU H-23 liste les arguments de cette sous-commande.

TABLEAU H-23 Arguments de la sous-commande `sp get ip`

Argument	Description
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU H-24 liste les arguments pour cette sous-commande.

TABLEAU H-24 Codes de retour de la sous-commande `sp get ip`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_Busy`	`9`	Périphérique ou ressource occupé.
`NWSE_RPCConnected`	`11`	Client RPC déjà connecté.
`NWSE_RPCConnRefused`	`12`	Connexion RPC refusée.
`NWSE_NoRouteToHost`	`13`	Pas de route vers l'hôte (réseau hors service).
`NWSE_HostDown`	`14`	Hôte hors service.

Sous-commande sp set ip

Description : définit ou modifie la configuration réseau du SP.

Format

```
sp set ip dhcp [--nowait]
```

```
sp set ip static {-i | --ipaddress} ADRESSE IP
[{-n | --netmask} MASQUERÉSEAU] [{-g | --gateway} PASSERELLE}] [-w |
--nowait]
```

Le TABLEAU H-25 liste les arguments de cette sous-commande.

TABLEAU H-25 Arguments de la sous-commande `sp set ip`

Argument	Description
`{-i | --ipaddress}`	Spécifie l'adresse IP que vous voulez définir.
`{-n | --netmask}`	Spécifie le masque réseau, la valeur par défaut est 255.255.255.0.
`{-g | --gateway}`	Spécifie la passerelle, la valeur par défaut est la passerelle existante.
`{-w | --nowait}`	Si vous spécifiez l'option `-nowait`, une perte de connectivité surviendra quelques temps après le retour de la commande. Si vous ne spécifiez pas l'option `-nowait`, votre connexion avec le SP sera perdue avant le retour de la commande.

Codes de retour

Le TABLEAU H-26 liste les codes de retour pour cette sous-commande.

TABLEAU H-26 Codes de retour de la sous-commande `sp set ip`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_Busy`	`9`	Périphérique ou ressource occupé.
`NWSE_RPCConnected`	`11`	Client RPC déjà connecté.
`NWSE_RPCConnRefused`	`12`	Connexion RPC refusée.
`NWSE_NoRouteToHost`	`13`	Pas de route vers l'hôte (réseau hors service).
`NWSE_HostDown`	`14`	Hôte hors service.
`NWSE_UnknownError`	`15`	Erreur de type divers pas capturée par d'autres erreurs.
`NWSE_GatewayOffNet`	`16`	L'adresse de la passerelle n'est pas sur le réseau.
`NWSE_NetMaskIncorrect`	`17`	Un masque de réseau inapproprié a été spécifié.

Sous-commandes du SP relatives à l'adresse JNET

L'adresse JNET est utilisée pour les communications entre le SP et la plate-forme. Les sous-commandes du TABLEAU H-27 gèrent l'adresse JNET du SP.

TABLEAU H-27 Sous-commandes `SP JNET`

Sous-commande	Description
`sp get jnet`	Récupère l'adresse JNET.
`sp set jnet`	Définit l'adresse JNET.

Sous-commande sp get jnet

Description : récupère l'adresse IP du pilote JNET de la plate-forme.

Format

`sp get jnet [{-H | --noheader}] [{-D | --Delim <`*`SÉPARATEUR`*`>}]`

Le TABLEAU H-28 liste les arguments de cette sous-commande.

TABLEAU H-28 Arguments de la sous-commande `sp get jnet`

Argument	Description
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU H-29 liste les codes de retour pour cette sous-commande.

TABLEAU H-29 Codes de retour de la sous-commande `sp get jnet`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_Busy`	`9`	Périphérique ou ressource occupé.
`NWSE_HostDown`	`14`	Hôte hors service.

Sous-commande sp set jnet

Description : définit ou modifie les adresses du SP et réseau de la plate-forme pour JNET. Compte tenu du pare-feu présent entre ces pilotes, vous devez spécifier les deux adresses en même temps.

Les deux adresses JNET du SP et de la plate-forme doivent être sous le même sous-réseau de classe C.

Format

`sp set jnet {-p | --platform}` *`ADRESSE IP`* `{-s | --sp}` *`ADRESSE IP`*

Le TABLEAU H-30 liste les arguments de cette sous-commande.

TABLEAU H-30 Arguments de la sous-commande `sp set jnet`

Argument	Description
`{-p	--platform}`	Spécifie l'adresse IP pour la plate-forme.
`{-s	--sp}`	Spécifie l'adresse IP pour le SP.

Remarque – Si vous changez les adresses par défaut de JNET en utilisant cette commande puis réinstallez le SE de la plate-forme ou réinitialisez le SP par le biais de la sous-commande `sp reset to default-settings`, vous devez ré-émettre la sous-commande `sp set jnet` pour rétablir la connexion JNET.

Sinon, la connexion ne sera plus synchronisée (l'une des adresses sera modifiée tandis que l'autre sera ramenée à l'adresse par défaut).

Codes de retour

Le TABLEAU H-31 liste les codes de retour pour cette sous-commande.

TABLEAU H-31 Codes de retour de la sous-commande `sp set jnet`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_Busy`	`9`	Périphérique ou ressource occupé.
`NWSE_HostDown`	`14`	Hôte hors service.

Sous-commandes du SP relatives au voyant de localisation

Les sous-commandes du TABLEAU H-32 gèrent l'adresse le commutateur du voyant de localisation.

TABLEAU H-32 Sous-commandes `SP Locatelight`

Sous-commande	Description
`sp get locatelight`	Lit la valeur du commutateur du voyant de localisation (qui représente l'état des voyants d'identification des panneaux frontal et arrière).
`sp set locatelight`	Définit l'état du commutateur du voyant de localisation.

Sous-commande sp get locatelight

Description : lit la valeur du commutateur du voyant de localisation (qui représente l'état des voyants d'identification des panneaux frontal et arrière). Les états possibles sont les suivants : blinking (clignotant) ou off (désactivé).

Format

```
sp get locatelight
```

Codes de retour

Le TABLEAU H-33 liste les codes de retour pour cette sous-commande.

TABLEAU H-33 Codes de retour de la sous-commande `sp get locatelight`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.

Sous-commande sp set locatelight

Description : définit l'état du commutateur du voyant de localisation (qui décrit l'état des voyants d'identification des panneaux frontal et arrière).

Format

```
sp set locatelight {BLINK | OFF}
```

Codes de retour

Le TABLEAU H-34 liste les codes de retour pour cette sous-commande.

TABLEAU H-34 Codes de retour de la sous-commande `sp set locatelight`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.

Sous-commandes du SP relatives aux fichiers journaux

Les sous-commandes du TABLEAU H-35 gèrent les fichiers journaux du SP.

TABLEAU H-35 Sous-commandes `SP Logfile`

Sous-commande	Description
`sp get logfile`	Récupère la configuration du fichier journal d'événements.
`sp set logfile`	Configure le fichier journal d'événements qui est la destination de tous les événements et avis du gestionnaire d'événements.

Sous-commande sp get logfile

Description : récupère la configuration du fichier journal d'événements.

Format

`sp get logfile [-H | --noheader] [{-D | --Delim <`*`SÉPARATEUR`*`>}]`

Le TABLEAU H-36 liste les arguments de cette sous-commande.

TABLEAU H-36 Arguments de la sous-commande `sp get logfile`

Argument	Description
`{-H	--noheader}`	Supprime les titres des colonnes.
`{ -D	--Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU H-37 liste les codes de retour pour cette sous-commande.

TABLEAU H-37 Codes de retour de la sous-commande `sp get logfile`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.

Sous-commande sp set logfile

Description : configure le fichier journal d'événements qui est la destination de tous les événements et avis du gestionnaire d'événements.

Format

`sp set logfile [ {-f | --file} NOMFICHIER] [ {-s | --size} TAILLE]`

Vous devez spécifier le nom du fichier auquel le gestionnaire d'événements envoie les journaux. Lorsque vous définissez le fichier journal en utilisant cette commande, il suffit d'en spécifier le nom sans le chemin. Les noms des fichiers ne doivent pas contenir de barre oblique (/), de référence de chemin relatif (..) ni le symbole inférieur à (<).

Le TABLEAU H-38 liste les arguments de cette sous-commande.

TABLEAU H-38 Arguments de la sous-commande `sp set logfile`

Argument	Description
`{-f | --file}`	Vous devez spécifier le nom du fichier dans le répertoire auquel le gestionnaire d'événements envoie les journaux.
`{-s | --size}`	Spécifie la taille du fichier en méga-octets. Une taille minimale de 0,01 Mo est requise pour ce fichier journal.

Codes de retour

Le TABLEAU H-39 liste les arguments pour cette sous-commande.

TABLEAU H-39 Codes de retour de la sous-commande `sp set logfile`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	8	Mémoire insuffisante.

Sous-commandes diverses du SP

Les sous-commandes du TABLEAU H-40 gèrent diverses fonctions du SP.

TABLEAU H-40 Sous-commandes diverses du SP

Sous-commande	Description
`sp create test events`	Teste et valide les différents types de configurations que vous pouvez envisager d'utiliser pour le SP.
`sp get mac address`	Récupère l'adresse MAC du SP.
`sp get port 80`	Récupère le dernier code POST du port 80 du registre Port80 PRS.
`sp get status`	Retourne le statut du système dans son ensemble.
`sp get tdulog`	Capture les données et les stocke sur le SP dans un format compressé.
`sp autoconfigure`	Configure un SP avec la même configuration qu'un autre processeur de service.
`sp reboot`	Redémarre le SP.
`sp reset`	Ramène des paramètres sélectionnés du SP à la configuration par défaut définie en usine.

Sous-commande create test events du SP

Description : cette commande vous aide à tester et valider les différents types de configurations que vous pouvez envisager d'utiliser pour le SP (par exemple, des configurations impliquant la transmission d'événements, tels que SNMP, SMTP, des fichiers journaux ou des services d'annuaire).

Lorsque vous exécutez cette commande, le SP génère trois nouveaux événements présentant chacun un niveau de sécurité différent. Pour afficher ces événements, exécutez la sous-commande `sp get events`. Récupérez ensuite les paramètres de configuration relatifs à SNMP, à SMTP et aux fichiers journaux et contrôlez s'ils ont bien atteint les destinations configurées.

SNMP

Pour configurer des destinations pour les trappes SNMP, exécutez la sous-commande `sp add snmp-destination`. Pour afficher vos paramètres courants, exécutez la sous-commande `sp get snmp-destinations`. Tous les événements du SP sont traduits en déroutements SNMP et envoyés à toutes les destinations configurées.

SMTP

Vous pouvez configurer les destinations des événements sous la forme d'adresses SMTP. Vous devez d'abord exécuter la sous-commande `sp set smtp server` pour configurer votre *serveur* SNMP et l'adresse *from* (de). Exécutez ensuite la sous-commande `sp update smtp subscriber` pour configurer les adresses et les formats de destination à utiliser pour les événements de gravité différente. Cette commande vous permet de configurer le format (long ou court) des événements qui sont fournis et le ou les destinataires des événements de gravités différentes.

Tous les événements du SP sont traduits en alertes et envoyés à toutes les destinations SMTP configurées en fonction de leur gravité (les abonnés). Vous pouvez exécuter les sous-commandes `sp get smtp server` et `sp get smtp subscribers` pour afficher les paramètres courants.

Fichiers journaux

Tous les événements qui sont générés sur le SP sont consignés dans le fichier journal par défaut ou dans un fichier journal spécifié par l'utilisateur si un point de montage est configuré. Pour ajouter un point de montage, exécutez la sous-commande `sp add mount`. Vous pouvez ensuite exécuter la sous-commande `sp set logfile` pour configurer le nom et la taille du fichier cible sur le système de fichiers monté. Pour afficher vos paramètres courants, exécutez les sous-commandes `sp get mounts` et `sp get logfile`.

Format

```
sp create test events
```

Codes de retour

Le TABLEAU H-41 liste les codes de retour de cette commande.

TABLEAU H-41 Codes de retour de la sous-commande `sp create test events`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NoMemory`	8	Mémoire insuffisante.

Sous-commande d'adresse sp get mac

Description : récupère l'adresse MAC du SP.

Format

```
sp get mac
```

Codes de retour

Le TABLEAU H-42 liste les codes de retour pour cette sous-commande.

TABLEAU H-42 Codes de retour de la sous-commande `sp get mac`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande sp get port80

Description : récupère le dernier code POST du port 80 du registre Port80 PRS. Le registre est écrit par le BIOS de la plate-forme pendant l'initialisation de la plate-forme. Vous pouvez utiliser cette sous-commande pour déboguer des problèmes d'initialisation de la plate-forme.

Format

```
sp get port80 {-m | --monitor}
```

Le TABLEAU H-43 liste les arguments de cette sous-commande.

TABLEAU H-43 Arguments de la sous-commande `sp get port80`

Argument	Description
`{-m | --monitor}`	Permet un contrôle continu du trafic du port 80.

Vous pouvez aussi récupérer les dix derniers codes POST du port 80 en utilisant le panneau de l'opérateur.

Pour plus de détails sur l'utilisation des menus du panneau de l'opérateur, voir le *Serveurs Sun Fire V20z et Sun Fire V40z — Guide de l'utilisateur* (819-2914-17).

Pour la liste des codes du POST pour le BIOS Phoenix, voir le TABLEAU H-45.

Pour la liste des codes des blocs d'initialisation dans la ROM Flash, voir le TABLEAU H-46.

Codes de retour

Le TABLEAU H-44 liste les codes de retour pour cette sous-commande.

TABLEAU H-44 Codes de retour de la sous-commande `sp get port80`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Codes de POST du BIOS

Le TABLEAU H-45 liste les codes du POST pour le BIOS Phoenix.

TABLEAU H-45 Codes de POST du BIOS

Code POST	Description
`02`	Vérifier le mode réel
`03`	Désactiver l'interruption non-masquable (NMI)
`04`	Obtenir le type de la CPU
`06`	Initialiser le matériel système
`07`	Désactiver le double et exécuter le code de la ROM
`08`	Initialiser le chipset avec les valeurs de POST initiales
`09`	Définir l'indicateur IN POST
`0A`	Initialiser les registres de la CPU
`0B`	Activer le cache de la CPU

TABLEAU H-45 Codes de POST du BIOS *(suite)*

Code POST	Description
0C	Initialiser les caches aux valeurs de POST initiales
0E	Initialiser le composant d'E/S
0F	Initialiser l'IDE du bus local
10	Initialiser la gestion de l'alimentation
11	Charger les registres de réserve avec les valeurs de POST initiales
12	Restaurer le mot de contrôle CPU lors d'une initialisation à chaud
13	Initialiser les périphériques maîtrisant le bus PCI
14	Initialiser le contrôleur du clavier
16	Somme de contrôle de la ROM du BIOS
17	Initialiser le cache avant l'auto-dimensionnement de la mémoire
18	8254 Initialisation de l'horloge d'interruptions programmables
1A	8237 Initialisation du contrôleur DMA
1C	Réinitialiser le contrôleur d'interruptions programmables
20	Tester le rafraîchissement de la DRAM
22	Tester le contrôleur du clavier 8742
24	Définir le registre de segment d'ES sur 4 Go
26	Activer la ligne gate A20
28	Autodimensionner la DRAM
29	Initialiser le gestionnaire de mémoire du POST
2A	Effacer la RAM de base de 512 Ko
2C	Échec de la RAM sur la ligne d'adresse xxxx
2E	Échec de la RAM sur les bits de données xxxx d'octet bas du bus de mémoire
2F	Activer le cache avant le double du BIOS du système
30	Échec de la RAM sur les bits de données xxxx d'octet haut du bus de mémoire
32	Tester la fréquence d'horloge du bus de la CPU
33	Initialiser le Phoenix Dispatch Manager
36	Arrêt de démarrage à chaud
38	Doubler la ROM du BIOS du système
3A	Autodimensionner le cache
3C	Configuration avancée des registres du chipset

TABLEAU H-45 Codes de POST du BIOS *(suite)*

Code POST	Description
3D	Charger les registres de réserve avec les valeurs de CMOS
41	Initialiser la mémoire étendue pour RomPilot
42	Initialiser les vecteurs d'interruption
45	Initialisation du périphérique POST
46	Contrôler l'avis de copyright de la ROM
47	Initialiser la prise en charge I20
48	Contrôler la configuration vidéo par rapport à CMOS
49	Initialiser le bus et les périphériques PCI
4A	Initialiser tous les adaptateurs vidéo du système
4B	Démarrage QuietBoot (optionnel)
4C	Doubler la ROM du BIOS vidéo
4E	Afficher l'avis de copyright du BIOS
4F	Initialiser MultiBoot
50	Afficher le type et la vitesse de la CPU
51	Initialiser la carte EISA
52	Tester le clavier
54	Définir le clic de la clé si activé
55	Activer les périphériques USB
58	Tester pour voir s'il y a des interruptions inattendues
59	Initialiser le service d'affichage du POST
5A	Afficher l'invite « Press F2 to enter SETUP »
5B	Désactiver le cache de la CPU
5C	Tester la RAM entre 512 Ko et 640 Ko
60	Tester la mémoire étendue
62	Tester les lignes d'adresse de la mémoire étendue
64	Aller directement à UserPatch1
66	Configurer les registres de cache avancés
67	Initialiser l'APIC multiprocesseur
68	Activer les caches externe et de la CPU
69	Configurer la zone SMM (system management mode)

TABLEAU H-45 Codes de POST du BIOS *(suite)*

Code POST	Description
6A	Afficher la taille du cache L2 externe
6B	Charger les valeurs par défaut personnalisées (facultatif)
6C	Afficher le message de la zone double
6E	Afficher l'adresse élevée possible pour la récupération UMB
70	Afficher les messages d'erreur
72	Rechercher des erreurs de configuration
76	Rechercher des erreurs de clavier
7C	Configurer les vecteurs d'interruption du matériel
7D	Initialiser le contrôle système intelligent
7E	Initialiser le coprocesseur s'il y en a un
80	Désactiver les super ports d'E/S embarqués et les IRQ
81	Initialisation tardive du périphérique POST
82	Détecter et installer les ports RS-232 externes
83	Configurer les contrôleurs IDE non-MCD
84	Détecter et installer les ports parallèles externes
85	Initialiser les périphériques ISA PnP compatibles PC
86	Réinitialiser les ports d'E/S embarqués
87	Configurer les périphériques configurables de la carte mère (facultatif)
88	Initialiser la zone de données du BIOS
89	Activer les interruptions non-masquables (NMI)
8A	Initialiser la zone de données étendue du BIOS
8B	Tester et initialiser la souris PS/2
8C	Initialiser le contrôleur de disquettes
8F	Déterminer le nombre de disques ATA (facultatif)
90	Initialiser les contrôleurs des disques durs
91	Initialiser les contrôleurs des disques durs du bus local
92	Aller directement à UserPatch2
93	Compiler MPTABLE pour les cartes multiprocesseurs
95	Installer le CD-ROM pour l'initialisation
96	Effacer le registre de segment ES de grande taille

TABLEAU H-45 Codes de POST du BIOS *(suite)*

Code POST	Description
97	Réparer le tableau multiprocesseur
98	Rechercher les ROM d'option
99	Rechercher un disque SMART (facultatif)
9A	Doubler les ROM d'option
9C	Configurer la gestion de l'alimentation
9D	Initialiser le moteur de sécurité (facultatif)
9E	Activer les interruptions du matériel
9F	Déterminer le nombre de disques ATA et SCSI (facultatif)
A0	Définir la date du jour
A2	Contrôler le verrou à clé
A4	Initialiser le taux d'impression automatique
A8	Effacer l'invite F2
AA	Balayer pour la frappe de la touche F2
AC	Entrer dans la configuration
AE	Effacer l'indicateur d'initialisation
B0	Rechercher des erreurs
B1	Informer RomPilot sur la fin du POST
B2	POST terminé - préparer l'initialisation du système d'exploitation
B4	Un bip court
B5	Terminer QuietBoot (optionnel)
B6	Contrôler le mot de passe
B7	Initialiser le BIOS de l'ACPI
B9	Préparer l'initialisation
BA	Initialiser les paramètres DMI
BB	Initialiser les ROM d'option PnP
BC	Effacer les contrôleurs de parité
BD	Afficher le menu multi-initialisation
BE	Effacer l'écran
BF	Contrôler les rappels de virus et de sauvegarde
C0	Essayer d'initialiser avec l'interruption 19

TABLEAU H-45 Codes de POST du BIOS *(suite)*

Code POST	Description
C1	Initialiser le POST Error Manager (PEM)
C2	Initialiser l'enregistrement des erreurs
C3	Initialiser la fonction d'affichage des erreurs
C4	Initialiser le gestionnaire d'erreurs du système
C5	CMOS double PnP (facultatif)
C6	Initialiser l'ancrage du portable (facultatif)
C7	Initialiser le taux d'ancrage du portable
C8	Forcer le contrôle (optionnel)
C9	Somme de contrôle étendue (facultatif)
CA	Rediriger Int 15h pour activer le clavier à distance
CB	Rediriger Int 13 sur les périphériques de technologies de mémoire (MTD) tels que ROM, RAM, PCMCIA et le disque série
CC	Rediriger Int 10h pour activer la vidéo série à distance
CD	Re-mapper les E/S et la mémoire pour PCMCIA
CE	Initialiser le numérisateur et afficher le message
D2	Interruption inconnue

Codes des blocs d'initialisation pour la ROM Flash

Le TABLEAU H-46 liste les codes des blocs d'initialisation dans la ROM Flash.

TABLEAU H-46 Codes de blocs d'initialisation dans la ROM Flash

Code POST	Description
E0	Initialiser le chipset
E1	Initialiser le pont
E2	Initialiser la CPU
E3	Initialiser l'horloge du système
E4	Initialiser la carte d'E/S du système
E5	Contrôler l'initialisation de récupération de force
E6	Somme de contrôle de la ROM du BIOS
E7	Aller au BIOS
E8	Définir le segment de grande taille
E9	Initialiser le multiprocesseur
EA	Initialiser le code spécial OEM
EB	Initialiser PIC et DMA
EC	Initialiser le type de mémoire
ED	Initialiser la taille de la mémoire
EE	Doubler le bloc d'initialisation
EF	Test de la mémoire système
F0	Initialiser les vecteurs d'interruption
F1	Initialiser l'horloge d'exécution
F2	Initialiser la vidéo
F3	Initialiser le System Management Manager
F4	Émettre un bip
F5	Effacer le segment de grande taille
F6	Initialiser en mini DOS
F7	Initialiser en Full DOS

Sous-commande du SP relative à la configuration automatique

Description : copie les paramètres de configuration d'un SP sur un ou plusieurs autres SP. Vous obtenez un SP avec la même configuration qu'un autre SP.

Vous pouvez aussi effectuer la configuration automatique depuis le panneau de l'opérateur pour exécuter cette même fonction. Pour plus d'informations, voir « Configuration automatique du SP (méthode optionnelle) », page 43.

La commande invoque une série de requêtes https portant sur tous les fichiers de configuration de la machine source puis charge les données de configuration sur le second SP. Les fichiers obtenus sont copiés dans le fichier `pstore` local et le second SP est réinitialisé. Vous ne pouvez pas effectuer d'autres changements de configuration tant que l'opération est en cours.

Par défaut, le partage de la configuration est désactivé et vous devez l'activer sur la machine source.

- Pour identifier le statut du partage de configuration sur un serveur, voir « Sous-commande access get config-sharing », page 134.
- Pour activer le partage de configuration, voir « Sous-commande access enable config-sharing », page 132.
- Pour désactiver le partage de configuration, voir « Sous-commande access disable config-sharing », page 133.

Une fois la commande exécutée, un message s'affiche indiquant que le SP va être redémarré. La connexion SSH s'arrête.

Format

```
sp autoconfigure {{ -s | --sp } IP_SP_OU_HÔTE [-H |--noheader]
```

Le TABLEAU H-47 liste les arguments de cette sous-commande.

TABLEAU H-47 Arguments de la sous-commande `sp autoconfigure`

Argument	Description
`{-s | --sp}`	Nom d'hôte DNS ou adresse IP de la machine de laquelle copier les informations de configuration.
`[-H | --noheader]`	Supprime les titres de la sortie.

Codes de retour

Le TABLEAU H-48 liste les codes de retour pour cette sous-commande.

TABLEAU H-48 Codes de retour de la sous-commande `sp autoconfigure`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_HostDown`	`14`	Hôte hors service.
`NWSE_TimedOut`	`23`	Opération arrivée à échéance.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande sp get status

Description : retourne le statut du système dans son ensemble.

Format

```
sp get status
```

Le TABLEAU H-49 liste les arguments de cette sous-commande.

TABLEAU H-49 Arguments de la sous-commande `sp get status`

Argument	Description
`Nominal`	Tous les composants fonctionnent dans les paramètres normaux.
`Avertissement`	Un ou plusieurs composants fonctionnent à des niveaux d'avertissement.
`Critique`	Un ou plusieurs composants fonctionnent hors spécification ou sont tombés en panne.

Codes de retour

Le TABLEAU H-50 liste les codes de retour pour cette sous-commande.

TABLEAU H-50 Codes de retour de la sous-commande `sp get status`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.

Sous-commande sp get tdulog

Description : L'utilitaire TDU (Troubleshooting Dump Utility) capture les données de débogage. Lorsque vous exécutez cette commande, ces données sont rassemblées et stockées sur le SP dans un fichier tar compressé.

Format

```
sp get tdulog [{-f | --filename} NOMFICHIER ou STDOUT ]
[{-c | --cpuregs} REGISTRES CPU]
[{-p | --pciregs} REGISTRES PCI]
[{-r | --reset} RESET PLATFORM]
```

Le TABLEAU H-51 liste les arguments de cette sous-commande.

TABLEAU H-51 Arguments de la sous-commande `sp get tdulog`

Argument	Description
`{-f | --filename}`	*Facultatif*. Nom du fichier de sortie sous lequel les fichiers journaux sont copiés ou nom complet du chemin. Les noms des fichiers ne doivent pas contenir de barre oblique (/), de référence de chemin relatif (..) ni le symbole inférieur à (<). Les fichiers journaux suivants sont créés par défaut : `envLog`: contient les variables d'environnement `vpdLog`: contient des données VPD brutes Des fichiers journaux supplémentaires sont créés pour les registres CPU2 et CPU3. Les données de TDU peuvent aussi être redirigées sur `stdout`. Si le nom du fichier est `stdout`, la sortie est envoyée à `stdout` et les fichiers journaux ne sont pas créés. Un partage de fichier monté sur NFS doit être utilisé pour stocker le fichier de sortie. Si vous n'indiquez pas de nom de fichier, un fichier nommé `tdulog.tar` est créé dans `/logs/`<*nomhôte*>, où <*nomhôte*> est le nom de l'hôte du SP. Si le nom d'hôte est `localhost`, c'est l'adresse MAC qui est utilisée.
`{-c | --cpuregs}`	Lit les registres K-8 (GPR, MSR, TCB et contrôle machine) de jusqu'à quatre CPU.
`{-p | --pciregs}`	Lit tous les registres PCI sur le système.
`{-r | --reset}`	Réinitialise la plate-forme s'il est impossible d'accéder au mode HDT.

Le nom du registre, son adresse et les données sont enregistrés dans un fichier. Par exemple, les informations relatives à CPU0 figurent dans le TABLEAU H-52.

TABLEAU H-52 Exemple d'informations pour la sous-commande `sp get tdulog` sur CPU0

Reg Name	Reg Addr	Reg Data
MSR_MCG_CAP_MSR	0xc0020179	0x0000000000000105
MSR_MCG_STAT_MSR	0xc002017a	0x0000000000000000
MSR_MCG_CTL_MSR	0xc002017b	0x000000000000001F
MSR_MC0_CTL	0xc0020400	0x000000000000007F

Codes de retour

Le TABLEAU H-53 liste les codes de retour pour cette sous-commande.

TABLEAU H-53 Codes de retour de la sous-commande `sp get tdulog`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NotFound`	`5`	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_MissingArgument`	`7`	Argument(s) manquant(s).
`NWSE_UnknownError`	`15`	Erreur de type divers pas capturée par d'autres erreurs.
`NWSE_FileError`	`18`	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.
`NWSE_NotMounted`	`21`	Le système de fichiers n'est pas monté.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande sp reboot

Description : redémarre le SP. Cette commande est pratique dans les situations d'urgence dans lesquelles vous pouvez ne pas pouvoir accéder physiquement à une machine.

Format

```
sp reboot [ {-f | --forced} ]
```

Le TABLEAU H-54 liste les arguments de cette commande.

TABLEAU H-54 Arguments de la sous-commande `sp reboot`

Argument	Description
{-f | --forced}	Entraîne une mise hors tension matérielle.

Codes de retour

Le TABLEAU H-55 liste les codes de retour de cette sous-commande.

TABLEAU H-55 Codes de retour de la sous-commande `sp reboot`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NoMemory`	8	Mémoire insuffisante.

Sous-commande sp reset

Description : Ramène des paramètres sélectionnés du SP à la configuration par défaut définie en usine.

Les fichiers de configuration du SP sont stockés dans le répertoire `/pstore`. Quand vous initialisez le système, le SP copie ces fichiers de configuration de`/pstore` à `/etc` si des fichiers manquent dans `/etc`. La restauration de la configuration par défaut du SP se fait en supprimant les fichiers de configuration du répertoire `/pstore`. Un redémarrage du SP est nécessaire pour que la réinitialisation du SP soit appliquée.

Par défaut, le SP redémarre 60 secondes après l'exécution de la sous-commande `sp reset to default-settings` sauf si vous spécifiez l'option `--nowait`, cas dans lequel le redémarrage a lieu immédiatement.

Un message s'affiche toutes les 20 secondes pour indiquer qu'un redémarrage va avoir lieu.

Format

```
sp reset to default-settings {-a | --all} {-c | --config}
{-n | --network} {-s | --ssh} {-u | --users} {-W | --nowait}
```

Le TABLEAU H-56 liste les arguments de cette commande.

TABLEAU H-56 Arguments de la sous-commande `sp reset`

Argument	Description
`{-a | --all}`	Ramène tous les paramètres du SP à leur configuration par défaut. Lorsque le SP redémarre, les paramètres sont ramenés à leurs valeurs par défaut. Cette option inclut aussi des événements et les paramètres de l'IPMI.
`{-c | --config}`	Ramène les autres paramètres de configuration du système à leur configuration par défaut. Lorsque le SP redémarre, les paramètres du système sont ramenés à leurs valeurs par défaut.
`{-n | --network}`	Ramène tous les paramètres du réseau à leur configuration par défaut. Lorsque le SP redémarre, il n'a plus de fonctions réseau ni de nom d'hôte. Ses montages NFS échouent et vous ne pouvez pas vous connecter au SP à distance via `ssh`. Configurez la configuration réseau pour le SP par le biais du panneau de l'opérateur pour restaurer les fonctions réseau. Définissez le nom d'hôte du SP afin de pouvoir faire référence à ce dernier par un nom et configurez le fichier `resolv.conf` afin de faire référence à d'autres systèmes par leur nom au lieu de le faire par leurs adresses IP pointées. Cette option supprime les fichiers réseau du répertoire `/pstore`.
`{-s | --ssh}`	Ramène tous les paramètres SSH à leur configuration par défaut. Lorsque le SP redémarre, de nouvelles clés `ssh` publique et privée sont générées. Utiliser `ssh` pour accéder au SP depuis un système distant qui s'est connecté au préalable au SP entraîne une défaillance accompagnée d'un message relatif à un changement de « Remote Host Identification » pour cause de changement de la clé `ssh` sur le SP. Le système distant doit supprimer son entrée de clé publique `ssh` pour le SP pour se réussir à se connecter via `ssh` au SP. Cette option supprime tous les fichiers du répertoire `/pstore/ssh/`.
`{-u | --users}`	Ramène tous les paramètres d'authentification des utilisateurs à leur configuration par défaut. Lorsque le SP redémarrera, tous les comptes d'utilisateur auront été supprimés et vous ne pourrez pas vous connecter à distance au SP via `ssh`.
`[-W | --nowait]`	Redémarre immédiatement le SP.

Remarque – Si vous changez les adresses par défaut de JNET en utilisant cette commande puis réinstallez le SE de la plate-forme ou réinitialisez le SP en exécutant la sous-commande `sp reset to default-settings`, vous devez réémettre la sous-commande `sp set jnet` pour rétablir la connexion JNET.

Sinon, la connexion ne sera plus synchronisée (l'une des adresses sera modifiée tandis que l'autre sera ramenée à l'adresse par défaut).

Codes de retour

Le TABLEAU H-57 liste les codes de retour de cette commande.

TABLEAU H-57 Codes de retour de la sous-commande `sp reset`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_Busy`	`9`	Périphérique ou ressource occupé.
`NWSE_RPCConnected`	`11`	Client RPC déjà connecté.
`NWSE_RPCConnRefused`	`12`	Connexion RPC refusée.
`NWSE_NoRouteToHost`	`13`	Pas de route vers l'hôte (réseau hors service).
`NWSE_HostDown`	`14`	Hôte hors service.

Sous-commandes du SP relatives au montage

Les sous-commandes du TABLEAU H-58 gèrent les points de montage du SP.

TABLEAU H-58 Sous-commandes `SP Mount`

Sous-commande	Description
`sp add mount`	Crée ou réinitialise un point de montage.
`sp delete mount`	Supprime le point de montage spécifié.
`sp get mounts`	Affiche les points de montage courants sur le SP.

Sous-commande sp add mount

Description : crée ou réinitialise un point de montage.

Format

```
sp add mount {-r | --remote} SYSTÈME_FICHIERS_DISTANT
[{-l | --local} POINT_MONTAGE_LOCAL] [{-u | --user} NOMUTILISATEUR]
[{-p | --password} MOTDEPASSE] [{-W | --nowait}]
```

Le TABLEAU H-59 liste les arguments de cette sous-commande.

TABLEAU H-59 Arguments de la sous-commande `sp add mount`

Argument	Description

`{-r | --remote}`	Spécifie le serveur distant et le système de fichiers à utiliser.
	Si le système de fichiers distant est exporté sur NFS, utilisez le format suivant pour le spécifier :
	`-r <ID_nom_serveur>:<chemin>`
	Si le système de fichiers distant est exporté sur CIFS (partage réseau Windows), utilisez le format suivant pour le spécifier :
	`-r //<nom_serveur>/<nom_partage>`
	Les options de nom et de mot de passe de l'utilisateur ne sont appropriées que lors du montage de systèmes de fichiers CIFS. Dans ces exemples, *nom_serveur* est l'adresse IP ou le nom d'hôte du serveur distant.
	Le format requis pour les points de montage NFS ou SMB est le suivant :
	• NFS : *nom_serveur*`:`*/pointmontage_exporté_serveur*
	• SMB : `//`*nom_serveur/nom_partage_windows*

`{-l | --local}`	*(facultatif)* Spécifie le point de montage local. Le seul point de montage pris en charge est `/mnt`.
`{-u | --user}`	Spécifie le nom d'utilisateur du compte Windows. Si les domaines Windows sont en vigueur, il se peut que vous deviez spécifier le domaine comme dans l'exemple suivant : `-u <domaine_serveur_fichiers>\<nomutilisateur>`
`{-p | --password}`	Spécifie le mot de passe du compte Windows.
`{-W | --nowait}`	Si `--nowait` est spécifié, il n'y aucun délai d'attente de la fin des commandes asynchrones.

Remarque – Plusieurs messages d'erreur peuvent s'afficher lors de l'exécution d'un point de montage `smb` pendant le montage de partitions windows. Contrôlez la réussite du montage en exécutant la sous-commande `sp get mounts`.

Codes de retour

Le TABLEAU H-60 liste les codes de retour pour cette sous-commande.

TABLEAU H-60 Codes de retour de la sous-commande `sp add mount`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_Busy`	`9`	Périphérique ou ressource occupé.
`NWSE_RPCConnected`	`11`	Client RPC déjà connecté.
`NWSE_RPCConnRefused`	`12`	Connexion RPC refusée.
`NWSE_NoRouteToHost`	`13`	Pas de route vers l'hôte (réseau hors service).
`NWSE_HostDown`	`14`	Hôte hors service.
`NWSE_UnknownError`	`15`	Erreur de type divers pas capturée par d'autres erreurs.

Sous-commande sp delete mount

Description : supprime un point de montage.

Format

```
sp delete mount POINT MONTAGE LOCAL [-q | --quiet]
```

Le TABLEAU H-61 liste les arguments de cette sous-commande.

TABLEAU H-61 Arguments de la sous-commande `sp delete event`

Argument	Description
`POINT MONTAGE LOCAL`	Spécifie le point de montage à supprimer. Si vous ne spécifiez pas de point de montage local, `/mnt` est utilisé car il s'agit de la valeur par défaut.
`[-q | --quiet]`	Cet argument spécifie qu'aucune erreur ne sera retournée si le point de montage à supprimer est introuvable.

Codes de retour

Le TABLEAU H-62 liste les codes de retour pour cette sous-commande.

TABLEAU H-62 Codes de reour de la sous-commande `sp delete mount`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_Busy`	`9`	Périphérique ou ressource occupé.
`NWSE_RPCConnected`	`11`	Client RPC déjà connecté.
`NWSE_RPCConnRefused`	`12`	Connexion RPC refusée.
`NWSE_NoRouteToHost`	`13`	Pas de route vers l'hôte (réseau hors service).
`NWSE_HostDown`	`14`	Hôte hors service.
`NWSE_UnknownError`	`15`	Erreur de type divers pas capturée par d'autres erreurs.

Sous-commande sp get mount

Description : affiche les points de montage courants sur le SP.

Format

```
sp get mounts [{-l | --local} POINT_MONTAGE] [-H | --noheader]
[{-D | --delim <SÉPARATEUR>}]
```

Le TABLEAU H-63 liste les arguments de cette sous-commande.

TABLEAU H-63 Arguments de la sous-commande `sp get mount`

Argument	Description
`{-l | --local}`	Spécifie le point de montage local. Si vous ne spécifiez pas `-l`, `/mnt` est utilisé car il s'agit de la valeur par défaut.
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU H-64 liste les codes de retour pour cette sous-commande.

TABLEAU H-64 Codes de retour de la sous-commande `sp get mount`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_InvalidArgument`	4	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NotFound`	5	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoMemory`	8	Mémoire insuffisante.
`NWSE_Busy`	9	Périphérique ou ressource occupé.
`NWSE_RPCConnected`	11	Client RPC déjà connecté.
`NWSE_RPCConnRefused`	12	Connexion RPC refusée.
`NWSE_NoRouteToHost`	13	Pas de route vers l'hôte (réseau hors service).
`NWSE_HostDown`	14	Hôte hors service.
`NWSE_NotMounted`	21	Le système de fichiers n'est pas monté.

Sous-commandes du SP relatives à SMTP

Les sous-commandes du TABLEAU H-65 gèrent les communications SMTP.

TABLEAU H-65 Sous-commandes `SP SMTP`

Sous-commande	Description
`sp get smtp server`	Récupère les informations relatives au serveur SMTP.
`sp get smtp server`	Configure le client SMTP du SP avec l'adresse du serveur SMTP distant.
`sp get smtp subscribers`	Retourne des informations détaillées sur un ou plusieurs abonnés à SMTP.
`sp update smtp subscriber`	Met à jour les informations d'un abonné SMTP existant.

Sous-commande sp get smtp server

Description : récupère les informations relatives au serveur SMTP, dont l'adresse *from* (de).

Format

`sp get smtp server [-H | --noheader] [{-D | --Delim <`*SÉPARATEUR*`>}]`

Le TABLEAU H-66 liste les arguments de cette sous-commande.

TABLEAU H-66 Arguments de la sous-commande `sp get smtp server`

Argument	Description
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

Le TABLEAU H-67 liste les codes de retour pour cette sous-commande.

TABLEAU H-67 Codes de retour de la sous-commande `sp get smtp server`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.

Sous-commande sp set smtp server

Description : configure le client SMTP du SP avec l'adresse du serveur SMTP distant, adresse et numéro de port optionnel compris.

Format

`sp set smtp server [{-f | --from}` *`DU CHAMP`* `]` *`IP OU NOMHÔTE DU SERVEUR SMTP`*

Le TABLEAU H-68 liste les arguments de cette sous-commande.

TABLEAU H-68 Arguments de la sous-commande `sp set smtp server`

Argument	Description
`{-f | --from}`	Spécifie le champ *from* (de) pour le serveur SMTP.
`IP OU NOMHÔTE DU SERVEUR SMTP`	Spécifie l'adresse IP ou le nom de l'hôte du serveur SMTP.

La valeur que vous indiquez est rattachée comme un préfixe à `@nomhôte | adresse_ip`. La valeur par défaut est `system`.

Par exemple, si vous entrez *admin* pour `sp_22`, les messages e-mail sont envoyés depuis `admin@sp_22`.

Si le nom d'hôte n'est pas défini, l'adresse IP est utilisée comme illustré dans l'exemple suivant : `admin@10.10.30.55`.

Codes de retour

Le TABLEAU H-69 liste les codes de retour pour cette sous-commande.

TABLEAU H-69 Codes de retour de la sous-commande `sp set smtp server`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.

Sous-commande sp get smtp subscribers

Description : retourne des informations détaillées sur un ou plusieurs abonnés à SMTP.

Format

`sp get smtp subscribers [{-n | --name} <`*`NOM`*`>] [-H | noheader] [{-D | --Delim <`*`SÉPARATEUR`*`>}]`

Le TABLEAU H-70 liste les arguments de cette sous-commande.

Le TABLEAU H-71 liste les abonnés à SMTP par défaut.

TABLEAU H-70 Arguments de la sous-commande `sp get smtp subscribers`

Argument	Description
`{ -n | --namserver }`	Spécifie le nom de l'abonné SMTP pour lequel vous voulez récupérer des informations. Si vous ne spécifiez pas cette option, la commande retourne des informations sur tous les abonnés.
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

TABLEAU H-71 Abonnés à SMTP par défaut

Abonné	Description
SMTP_Info_Short	Message e-mail court, gravité de type informative
SMTP_Info_Long	Message e-mail long, gravité de type informative
SMTP_Warning_Short	Message e-mail court, gravité de type avertissement
SMTP_Warning_Long	Message e-mail long, gravité de type avertissement
SMTP_Critical_Short	Message e-mail court, gravité critique
SMTP_Critical_Long	Message e-mail long, gravité critique

Les messages e-mail longs contiennent des détails complets sur les événements dans le corps du message tandis que les messages e-mail courts n'ont pas de corps de message. Les deux types ont une ligne de sujet descriptive.

Le format d'e-mail court a été conçu pour s'utiliser avec des pagers et d'autres périphériques sans fil présentant des limites au niveau de la taille des messages pouvant empêcher la réception de messages au format long.

Codes de retour

Le TABLEAU H-72 liste les codes de retour pour cette sous-commande.

TABLEAU H-72 Codes de retour de la sous-commande `sp get smtp subscribers`

Code de retour	ID	Description
NWSE_Success	0	La commande a réussi.
NWSE_InvalidUsage	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
NWSE_RPCTimeout	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
NWSE_RPCNotConnected	3	Connexion au serveur RPC impossible.
NWSE_NotFound	5	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.

Sous-commande sp update smtp subscriber

Description : met à jour les informations d'un abonné SMTP existant.

Format

```
sp update smtp subscriber
{-n | --name} NOM {-r | --recipients} LISTE ADRESSES
```

Le TABLEAU H-73 liste les arguments de cette sous-commande.

Le TABLEAU H-74 liste les abonnés à SMTP par défaut.

Remarque – Toutes les options remplacent les valeurs existantes par la nouvelle valeur. Les options non-spécifiées conservent leurs paramètres tels quels.
Par exemple, si vous ne spécifiez que l'option `-r` pour un abonné existant, l'adresse e-mail existante sera remplacée par la nouvelle liste spécifiée dans la commande.

TABLEAU H-73 Arguments de la sous-commande `sp update smtp subscriber`

Argument	Description
`{-n | --name}`	Spécifie le nom de l'abonné SMTP à mettre à jour. Cet argument peut être répété pour mettre à jour plusieurs abonnés SMTP à la fois.
`{-r | --recipients}`	Spécifie la liste d'adresses des destinataires pour l'abonné à SMTP.

TABLEAU H-74 Abonnés à SMTP par défaut

Abonné	Description
`SMTP_Info_Short`	Message e-mail court, gravité de type informative
`SMTP_Info_Long`	Message e-mail long, gravité de type informative
`SMTP_Warning_Short`	Message e-mail court, gravité de type avertissement
`SMTP_Warning_Long`	Message e-mail long, gravité de type avertissement
`SMTP_Critical_Short`	Message e-mail court, gravité critique
`SMTP_Critical_Long`	Message e-mail long, gravité critique

Les messages e-mail longs contiennent des détails complets sur les événements dans le corps du message tandis que les messages e-mail courts n'ont pas de corps de message. Les deux types ont une ligne de sujet descriptive.

Le format d'e-mail court a été conçu pour s'utiliser avec des pagers et d'autres périphériques sans fil présentant des limites au niveau de la taille des messages pouvant empêcher la réception de messages au format long.

Codes de retour

Le TABLEAU H-75 liste les codes de retour de cette sous-commande.

TABLEAU H-75 Codes de retour de la sous-commande `sp update smtp subscriber`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NotFound`	5	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.

Sous-commandes du SP relatives à SNMP

Les sous-commandes du TABLEAU H-76 gèrent les communications SNMP.

TABLEAU H-76 Sous-commandes `SP SNMP`

Sous-commande	Description
sp add snmp destination	Ajoute une destination SNMP.
sp delete snmp-destination	Supprime une destination SNMP.
sp get snmp destinations	Affiche les destinations SNMP disponibles (adresse IP ou nom d'hôte) pour l'envoi auxquelles le SP est configuré.
sp get snmp proxy community	Retourne le nom de communauté couramment utilisé par le SNMPD du SP pour relayer par proxy l'agent SNMP de la plate-forme.
sp set snmp proxy community	Définit les entrées de proxy qui spécifient l'OID auquel faire référence, l'adresse IP à laquelle ils sont renvoyés et la chaîne de communauté à utiliser pendant la création de proxy.

Sous-commande sp add snmp-destination

Description : ajoute une unique destination SNMP (une adresse IP ou un nom d'hôte).

Format

`sp add snmp-destination` *`ADRESSE IP/NOMHÔTE`*

Le TABLEAU H-77 liste les arguments pour cette sous-commande.

TABLEAU H-77 Arguments de la sous-commande `sp add snmp-destination`

Argument	Description
`ADRESSE IP/NOMHÔTE`	Spécifie l'adresse IP ou le nom de l'hôte pour la destination que vous voulez ajouter. Cet argument peut être répété pour ajouter plusieurs destinations à la fois ; le nombre des destinations que vous pouvez créer est toutefois limité par la mémoire.

Codes de retour

Le TABLEAU H-78 liste les codes de retour pour cette sous-commande.

TABLEAU H-78 Codes de retour de la sous-commande `sp add snmp-destination`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_InvalidArgument`	4	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	8	Mémoire insuffisante.
`NWSE_RPCConnRefused`	12	Connexion RPC refusée.
`NWSE_UnknownError`	15	Erreur de type divers pas capturée par d'autres erreurs.
`NWSE_FileError`	18	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.
`NWSE_Exist`	19	Entité (utilisateur, service ou autre) déjà présente.

Sous-commande sp delete snmp-destination

Description : supprime une unique destination SNMP (une adresse IP ou un nom d'hôte).

Format

```
sp delete snmp-destination { ADRESSE IP/NOMHÔTE | {-a | --all}
[-q | --quiet]
```

Le TABLEAU H-79 liste les arguments de cette sous-commande.

TABLEAU H-79 Arguments de la sous-commande `sp delete snmp-destination`

Argument	Description
`ADRESSE IP/NOMHÔTE`	Spécifie l'adresse IP ou le nom de l'hôte de la destination à supprimer. Cet argument peut être répété pour supprimer plusieurs destinations à la fois.
`[-a | --all]`	Supprime toutes les destinations SNMP.
`[-q | --quiet]`	Cet argument spécifie qu'aucune erreur ne sera retournée si la destination SNMP à supprimer est introuvable.

Codes de retour

Le TABLEAU H-80 liste les codes de retour pour cette sous-commande.

TABLEAU H-80 Codes de retour de la sous-commande `sp delete snmp-destination`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_InvalidArgument`	4	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_NotFound`	5	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	6	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	8	Mémoire insuffisante.
`NWSE_RPCConnRefused`	12	Connexion RPC refusée.
`NWSE_UnknownError`	15	Erreur de type divers pas capturée par d'autres erreurs.
`NWSE_FileError`	18	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.

Sous-commande sp get snmp-destinations

Description : affiche les destinations SNMP disponibles (adresse IP ou nom d'hôte) pour l'envoi auxquelles le SP est configuré. De nombreux programmes de mise en réseau utilisent ces informations pour identifier la machine.

Format

```
sp get snmp-destinations
```

Codes de retour

Le TABLEAU H-81 liste les codes de retour pour cette sous-commande.

TABLEAU H-81 Codes de retour de la sous-commande `sp get snmp-destinations`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.
`NWSE_NoMemory`	8	Mémoire insuffisante.
`NWSE_UnknownError`	15	Erreur de type divers pas capturée par d'autres erreurs.
`NWSE_FileError`	18	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.

Sous-commande sp get snmp proxy community

Description : retourne le nom de communauté couramment utilisé par le SP pour servir de proxy pour l'agent SNMP de la plate-forme.

Format

```
sp get snmp proxy community
```

Codes de retour

Le TABLEAU H-82 liste les codes de retour pour cette sous-commande.

TABLEAU H-82 Codes de retour de la sous-commande `sp get snmp proxy community`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	`2`	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	`3`	Connexion au serveur RPC impossible.

Sous-commande sp set snmp proxy community

Description : l'agent SNMP du SP agit comme un proxy pour l'agent SNMP maître s'exécutant sur la plate-forme. Ces entrées de proxy spécifient l'OID auquel faire référence, l'adresse IP à laquelle ils sont renvoyés et la chaîne de communauté à utiliser pendant la création de proxy. La chaîne de communauté est la valeur configurée dans la configuration SNMP côté plate-forme.

Format

`sp set snmp proxy community` *`CHAÎNE COMMUNAUTÉ`*

Le TABLEAU H-83 liste les arguments pour cette sous-commande.

TABLEAU H-83 Arguments de la sous-commande `sp set snmp proxy community`

Argument	Description
`CHAÎNE COMMUNAUTÉ`	Spécifie le nom de la communauté à configurer.

Il n'y a pas de restrictions au niveau de la longueur des chaînes de communauté ; les noms courants sont *private* et *public*. Le nom par défaut de la chaîne de communauté est *private*.

Si vous exécutez la sous-commande `sp get snmp proxy community` sans la définir, la valeur de retour est `private`. Sinon, vous pouvez la définir sur la chaîne de votre choix.

Codes de retour

Le TABLEAU H-84 liste les codes de retour pour cette sous-commande.

TABLEAU H-84 Codes de retour de la sous-commande `sp set snmp proxy community`

Code de retour	ID	Description
`NWSE_Success`	0	La commande a réussi.
`NWSE_InvalidUsage`	1	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_RPCTimeout`	2	La requête a été émise mais n'a pas été traitée par le serveur. La procédure RPC a échoué et la requête peut avoir été ou ne pas avoir été traitée par le serveur.
`NWSE_RPCNotConnected`	3	Connexion au serveur RPC impossible.

Sous-commandes du SP relatives à SSL

Les sous-commandes du TABLEAU H-85 gèrent les fonctions SSL.

TABLEAU H-85 Sous-commandes `SP SSL`

Sous-commande	Description
`sp disable ssl-required`	Désactive l'utilisation forcée du protocole HTTP sécurisé (HTTPS).
`sp enable ssl-required`	Active l'utilisation forcée du protocole HTTP sécurisé (HTTPS).
`sp get ssl`	Détermine si le serveur Web Apache utilise les fichiers fournis en usine ou des fichiers fournis par l'utilisateur.
`sp set ssl`	Vous permet d'utiliser les certificats SSL du site dans l'environnement SP.

Sous-commande sp disable ssl-required

Description : désactive la redirection automatique pour sécuriser les URL HTTP. Avec SSL désactivé, les requêtes HTTP sont traitées directement sans redirection sur HTTPS. Les requêtes HTTPS continuent à être sécurisées.

Format

```
sp disable ssl-required
```

Codes de retour

Le TABLEAU H-86 liste les codes de retour de cette commande.

TABLEAU H-86 Codes de retour de la sous-commande `sp disable ssl-required`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_FileError`	`18`	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande sp enable ssl-required

Description : active la redirection automatique pour sécuriser les URL HTTP. Avec SSL activé, les requête HTTP sont automatiquement redirigées sur des requêtes HTTPS équivalentes pour maintenir la sécurité du site.

La version 0.9.6j de SSL est prise en charge.

Format

```
sp enable ssl-required
```

Codes de retour

Le TABLEAU H-87 liste les codes de retour de cette sous-commande.

TABLEAU H-87 Codes de retour de la sous-commande `sp enable ssl-required`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_FileError`	`18`	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande sp get ssl

Description : détermine si la redirection automatique visant à sécuriser HTTP est obligatoire ou facultative et si le serveur Web Apache utilise les fichiers de certificats d'usine ou fournis par l'utilisateur.

Format

`sp get ssl [{-H | noheader}] [{-D | --Delim <`*SÉPARATEUR*`>}]`

Le TABLEAU H-88 liste les arguments de cette sous-commande.

TABLEAU H-88 Arguments de la sous-commande `sp get ssl`

Argument	Description
`{-H | --noheader}`	Supprime les titres des colonnes.
`{ -D | --Delim }`	Délimite les colonnes avec le séparateur spécifié. Les titres sont également délimités s'ils n'ont pas été supprimés. Le séparateur peut être tout caractère ou chaîne.

Codes de retour

TABLEAU H-89 liste les codes de retour pour cette sous-commande.

TABLEAU H-89 Codes de retour de la sous-commande `sp get ssl`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commande sp set ssl

Description : vous permet d'utiliser les certificats SSL du site dans l'environnement SP. Cette commande permet de remplacer le certificat du serveur figurant dans l'image SP Value-Add par votre propre certificat généré en interne et de restaurer les paramètres définis en usine.

Format

```
sp set ssl [-f]
sp set ssl {-c | --certfile} <CHEMIN COMPLET DU FICHIER DU CERTIFICAT DU SERVEUR>
{-k | --keyfile} <CHEMIN COMPLET DU FICHIER DE LA CLÉ PRIVÉE>
```

Le TABLEAU H-90 liste les arguments de cette sous-commande.

TABLEAU H-90 Arguments de la sous-commande `sp set ssl`

Argument	Description
`[-f]`	Restaure les paramètres définis en usine.
`{-c | --certfile}`	Marque d'un indicateur les noms des fichiers à installer.
`{-k | --keyfile}`	Marque d'un indicateur les noms des fichiers à installer.

Codes de retour

Le TABLEAU H-91 liste les codes de retour pour cette sous-commande.

TABLEAU H-91 Codes de retour de la sous-commande `sp set ssl`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_FileError`	`18`	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Sous-commandes du SP relatives à la mise à jour

Les sous-commandes du TABLEAU H-92 gèrent la flash du SP.

TABLEAU H-92 Sous-commandes `SP Flash`

Sous-commande	Description
`sp update flash all`	Définit l'indicateur de mise à jour pour lancer une mise à jour complète de la flash à la prochaine réinitialisation du SP.
`sp update flash applications`	Copie le fichier `Value-Add` dans le composant Value-Add de la flash du SP.
`sp update diags`	Met à jour les diagnostics à une nouvelle version.

Sous-commande sp update flash all

Remarque – Avant d'utiliser cette commande, vous devez démarrer le Java Update Server. Pour les instructions à suivre pour démarrer le Java Update Server, voir « Mise à jour du package de base du SP », page 39.

Description : met à jour toute l'image flash du SP (noyau, système de fichiers de base et ajout de valeurs) dans le cadre d'une mise à jour majeure du logiciel du SP.

Cette sous-commande commence par vérifier que le programme java spUpdate est activé sur le serveur distant spécifié et que la version correcte du serveur de mise à jour est en cours d'exécution

Une fois la vérification faire, la sous-commande définit l'indicateur de mise à jour `update` pour lancer une mise à jour complète de la mémoire flash à la prochaine réinitialisation du SP. Lorsque le SP s'initialise, il se connecte avec le programme spUpdate, télécharge et installe la nouvelle image flash puis redémarre le SP en mode de fonctionnement normal. Il définit aussi l'adresse IP du serveur et un numéro de port de serveur optionnel dans les variables d'environnement.

Exécutez la commande `sp -V` depuis le SP pour vérifier la version de la nouvelle image flash.

- Si cette commande échoue pour l'image à valeur ajoutée, exécutez la sous-commande `sp update flash applications`.
- Si cette commande échoue pour l'image de base, mettez la flash à jour en utilisant le panneau de l'opérateur. Pour plus de détails sur le panneau de l'opérateur, voir le *Serveurs Sun Fire V20z et Sun Fire V40z — Guide de l'utilisateur* (819-2914).

Remarque – La sous-commande `sp update flash all` ne met pas à jour les données de `pstore`.

Format

```
sp update flash all { i | --serverip} <ipaddress xx.xx.xx.xx>
[{ p | --port} <port#>] [{-r|--remote} VERSION_DISTANTE ]
```

Le TABLEAU H-93 liste les arguments de cette sous-commande.

TABLEAU H-93 Arguments de la sous-commande `sp update flash all`

Argument	Description
`{-i | --serverip}`	Adresse IP du serveur distant sur lequel le serveur de mise à jour (application java) est en cours d'exécution. Le serveur de mise à jour contient les images flash.
`{-p | --port}`	*(facultatif)* Numéro du port du serveur distant sur lequel le programme java sp update écoute les requêtes de mise à jour de la flash du SP. Si ce numéro de port n'est pas indiqué, la commande essaie de se connecter au port par défaut. La valeur par défaut est 52 708 secondes.
`{-r | --remote}`	Identifiez la version à utiliser pour la mise à jour. Spécifiez une version (par exemple, V1.2.3.4) ou utilisez LATEST pour utiliser la dernière version disponible sur le serveur de mise à jour.

Codes de retour

Le TABLEAU H-94 liste les codes de retour pour cette sous-commande.

TABLEAU H-94 Codes de retour de la sous-commande `sp update flash all`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NotFound`	`5`	La version spécifiée est introuvable.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_UnknownError`	`15`	Erreur de type divers pas capturée par d'autres erreurs.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.

Mises à niveau inférieures

Si vous voulez mettre à niveau le processeur de service vers une version antérieure, vous devez suivre la procédure ci-dessous pour éviter tout problème lorsque le processeur de service essaie de démarrer.

1. **Exécutez sp reset to default-settings --all.**
2. **Après la réinitialisation du SP :**
   a. **Créez un nouvel utilisateur gestionnaire en vous connectant sous le nom setup.**
   b. **Exécutez sp update flash all.**
3. **Après la réinitialisation du SP :**
   a. **Exécutez sp reset to default-settings --all.**

   Après la réinitialisation du sp, créez un nouvel utilisateur gestionnaire et mettez à jour votre configuration comme requis. Si vous effectuez cette procédure sur plusieurs machines, utilisez la commande `sp autoconfigure` d'un processeur de service préconfiguré.

   Si la commande `sp update flash all` échoue pour l'image du composant Value Add, utilisez la commande sp update flash applications. Si cette commande échoue pour l'image de base, mettez la flash à jour en utilisant le panneau de l'opérateur. Pour toute information sur l'utilisation du panneau de l'opérateur, reportez-vous au *Guide de gestion des serveurs*.

Sous-commande sp update flash applications

Description : Le système de fichiers du SP est divisé en deux composants : Base et Value-Add. Le composant Base inclut le référentiel et le composant Value-Add inclut le logiciel d'application.

Cette commande copie le fichier `Value-Add` dans le composant Value-Add de la flash du SP. La nouvelle image Value-Add entre en vigueur image après avoir réinitialisé le SP.

Si la sous-commande `sp update flash applications` échoue et l'image Value-Add est corrompue, vous pouvez utiliser la commande similaire disponible dans l'image Base du SP.

Format

```
sp update flash applications [{-f|--filename} FICHIER]
[{-h|--help}] [{-i|--ipaddress} ADRESSE_DISTANTE]
[{-p|--port} PORT_DISTANT] [{-r|--remote} VERSION_DISTANTE]
```

Le TABLEAU H-95 liste les arguments de cette sous-commande.

TABLEAU H-95 Arguments de la sous-commande `sp update flash applications`

Argument	Description
`{-f | --filename}`	Spécifie le chemin complet du fichier.
`{-i | --ipaddress}`	Adresse IP du serveur sur lequel le serveur de mise à jour (application java) est en cours d'exécution.
`{-p | --port}`	*(facultatif)* Numéro du port du serveur distant sur lequel le programme java sp update écoute les requêtes de mise à jour de la flash du SP. Si ce numéro de port n'est pas indiqué, la commande essaie de se connecter au port par défaut. La valeur par défaut est 52 708 secondes.
`{-r | --remote}`	Identifiez la version à utiliser pour la mise à jour. Spécifiez une version (par exemple, V1.2.3.4) ou utilisez LATEST pour utiliser la dernière version disponible sur le serveur de mise à jour.

Codes de retour

Le TABLEAU H-96 liste les codes de retour pour cette sous-commande.

TABLEAU H-96 Codes de retour de la sous-commande `sp update flash applications`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_NotFound`	`5`	Entité (utilisateur, service, fichier, chemin ou autre) introuvable.
`NWSE_NoPermission`	`6`	Pas autorisé à effectuer cette opération.
`NWSE_NoMemory`	`8`	Mémoire insuffisante.
`NWSE_FileError`	`18`	Fichier ouvert, manquant ou erreur de lecture ou d'écriture.
`NWSE_ServiceNotAvailable`	`24`	Le service demandé n'est pas disponible.
`NWSE_DeviceError`	`25`	Impossible de lire ou d'écrire sur le périphérique.

Sous-commandes du SP relatives à la mise à jour des diagnostics

Description : met à jour la version courante des diagnostics si une mise à jour est disponible.

Bien que le SP fonctionne normalement sans accéder à un système de fichiers externe, un système de fichiers est requis pour activer plusieurs fonctions, dont les diagnostics. Le logiciel du SP utilise une version par défaut des diagnostics. Cependant, si une nouvelle version est proposée et stockée sur le Network Share Volume, vous devez pointer explicitement sur cette nouvelle version pour l'utiliser.

Format

`sp update diags {-p | --path} <CHEMIN_DU_DOSSIER_DIAGS>`

Le TABLEAU H-97 liste les arguments pour cette sous-commande.

TABLEAU H-97 Arguments de la sous-commande `sp update diags`

Argument	Description
{-p | --path}	Pointe sur l'emplacement des nouveaux diagnostics.

Codes de retour

Le TABLEAU H-98 liste les codes de retour pour cette sous-commande.

TABLEAU H-98 Codes de retour de la sous-commande `sp update diags`

Code de retour	ID	Description
`NWSE_Success`	`0`	La commande a réussi.
`NWSE_InvalidUsage`	`1`	Usage incorrect : utilisation d'un paramètre erroné, spécification d'options en conflit.
`NWSE_InvalidArgument`	`4`	Un ou plusieurs arguments étaient incorrects ou invalides.
`NWSE_UnknownError`	`15`	Erreur de type divers pas capturée par d'autres erreurs.

Index

A

Accès IPMI
  Activation 22
  Activation de l'accès in-band
    IPMI sur un serveur Linux 22
    Sur un serveur x86 Solaris 24
  Mise à niveau du noyau 27
Accès LAN IPMI
  Activation 25
  Activation de l'accès in-band
    IPMI sur un serveur Linux 25
    Sur un serveur x86 Solaris 26
  Activation de l'accès out-of-band sur un serveur Linux 26
Activation de l'accès
  IPMI 22
  LAN IPMI 25
Adresse IP
  Paramètre DHCP 14
  Paramètre statique 16
Adresse MAC, Détermination 47
ADS 53
  Exigences du serveur 56
Agent X pour SNMP 95
Alimentation 50
Authentification 19

B

BIOS, Paramètres pour redirection console 119
BMC, voir Contrôleur de gestion de carte de base
Boutons du panneau de l'opérateur
  Fonctions définies 9
  Illustration 8

C

Certificat SSL 58, 59
Clé d'hôte, Scripts 106
Clé publique pour l'utilisation de scripts 107
Codes des blocs d'initialisation
  Dans la ROM Flash 264
  Pour la ROM Flash 264
Commande
  ssh, Utilisation du protocole 126
  Tableau récapitulatif codes de retour 129
  Tableau récapitulatif types de commandes 127
Commande d'accès
  add public key 152
  add trust 147
  add user 156
  delete public keys 155
  delete trust 150
  delete user 157
  disable service 142
  enable service 143
  get map 138
  get public key users 154
  get services 145

get trusts 151
get users 158
Groupe get 132, 133, 134, 136, 137
map 139
Récapitulatif groupes de sous-commandes 131
Sous-commandes
Mappage 138
Relatives à la confiance 147
Relatives aux clés publiques 152
Relatives aux groupes 132, 136
Relatives aux services d'annuaire 142
Relatives aux utilisateurs 156
unmap 140
update password 159
update user 160
Commande d'inventaire
compare versions 178
get all 184
get hardware 179
get software 182, 183
Tableau récapitulatif sous-commandes 177
Commande diags
cancel tests 165
get modules 167
get state 168
get tests 169
run tests 171
start 173
Tableau récapitulatif sous-commandes 163
terminate 175
Commande du SP
add mount 273
add snmp-destination 284
create test events 255
delete event 238
delete mount 276
delete snmp-destination 285
disable dns 234
disable ssl-required 290
enable dns 235
enable ssl-required 291
get date 232
get dns 236
get events 239
get hostname 241
get ip 244
get jnet 247
get locatelight 250
get logfile 252
get mount 277
get port80 257
get smtp server 278
get smtp subscribers 280
get snmp proxy community 287
get snmp-destinations 287
get ssl 292
get status 266
get tdulog 267
load settings 265
reboot 269
Récapitulatif
Sous-commandes de mise à jour 295
Sous-commandes diverses du SP 255
Sous-commandes du SP relatives aux événements 237
Sous-commandes relatives à DNS 234
Sous-commandes relatives à IP 244
Sous-commandes relatives à l'adresse JNET 247
Sous-commandes relatives à SMTP 278
Sous-commandes relatives à SNMP 284
Sous-commandes relatives à SSL 290
Sous-commandes relatives au voyant de localisation 250
Sous-commandes relatives aux fichiers journaux 252
reset 270
set date 233
set hostname 242
set ip 245
set jnet 248
set locatelight 251
set logfile 253
set smtp server 279
set snmp proxy community 288
set ssl 293
Sous-commandes relatives à la date 232
Sous-commandes relatives au montage 273
Tableau récapitulatif
Groupes de sous-commandes 231
Sous-commandes relatives au nom de l'hôte 241
update diags 300
update flash all 295
update flash applications 298
update smtp subscriber 282

Commande IPMI
Commande get sel 192
disable channel 186
disable pef 188
enable channel 187
enable pef 189
get channels 190
get global enables 191
reset 197
set global enable 195
Tableau récapitulatif des sous-commandes 185
Commande relative aux capteurs
get 224
set 227
Tableau récapitulatif sous-commandes 223
Compte de configuration, Ouverture d'une session 19
Compte de gestionnaire initial, Création 19
Configuration
Automatique du SP 43
BIOS 50
Certificat SSL 58
Date et heure 57
E-mail 51
Notification d'événements SMTP 51
Processeur de service 14
Serveurs en guirlande 28
Service d'annuaire 53
Connecteur
Sun Fire V20z 5
Sun Fire V40z 4
Connexe, Documentation xxii
Console, Systems Management 48
Contrôleur de gestion de carte de base, IPMI 68
Création d'un compte de gestionnaire initial 19
Création de relations d'hôte de confiance, Scripts 107

D

Date et heure, Paramètres 57
Dépannage
IPMI 87
SNMP 101
Déroutement, Événement du serveur avec SNMP 96
Documentation connexe xxii

E

État 50
Alimentation 33
Système d'exploitation 50
Événement 64
Icône 66
Système 64

F

Fichier keytab 56
Fonction de la console SM 48
Fonction Serial Over LAN
Activation 122
Désactivation 123
Lancement et arrêt d'une session 123
Fonctions de la console Systems Management 48

G

Gestion des serveurs
Présentation des options 4
Schéma des options 7
getty, Utilisation pour redirection console 117
Groupe d'utilisateur, Définition 10
Groupe, Mappage 54
grub, Utilisation pour redirection console 115

H

Hôte, Génération d'une paire de clés 108

I

Icône 66
Intégration du protocole SNMP 90
Intelligent platform management interface, voir Interface IPMI
Interconnexion de serveurs, Schéma 28

Interface IPMI
Accès au canal LAN 70
Conformité 70
Contrôleur de gestion de carte de base 68
Dépannage 87
Fonctions de gestion 69
Interface LAN pour le BMC 84
IPMItool 78
Journal d'événements système, Affichage 86
Lights Out Management 78
Pilote de périphérique du noyau Linux 84
Présentation 67
Interface SNMP
Agent du SP 93
Agent proxy 94
Agent X 95
Conditions requises 92
Configuration 92
Dépannage 101
Déroutement d'événement du serveur 96
Destination des déroutements d'événement du serveur 97
Détails de la MIB 98
Intégration, Présentation 90
MIB 91
Navigateur de MIB de tierce partie 95
Nom de communauté, Définition 94
Option de journalisation, Définition 96
Présentation 89
Schéma de l'architecture 92
Tableau Événements du SP 99
Interfaces de gestion de serveurs, Liste 6
Interfaces prises en charge, Liste 6
IPMItool
Expressions et paramètres de la commande 80
Options de la commande 79
Source de téléchargement 78
Syntaxe de la commande 78

J

Journal d'événements système, IPMI 86

L

Lights Out Management, IPMI 78
LILO, Utilisation pour redirection console 116
LOM, voir Lights Out Management

M

Mappage de groupes de services d'annuaire 54
MIB pour SNMP 91
Mise à jour
Inférieure du SP 297
Logiciel du processeur de service 34
Mot de passe 19

N

Navigateur MIB 95
Network share volume
Contenu extrait 120
Structure 120
NIS 53
Nom d'utilisateur 19
Nom d'utilisateur et mot de passe, Règles 19
Nom de communauté pour SNMP 94
Notification d'événements SMTP 51
Noyau IPMI, Mise à niveau 27

O

Organisation de ce livre xxi
Ouverture d'une session avec un compte de configuration 19

P

Panneau arrière
Connecteurs du Sun Fire V20z 5
Connecteurs du Sun Fire V40z 4
Panneau de l'opérateur, Boutons 9
Paramètre de date ou d'heure 57
Pilote de plate-forme Newisys 32

Plate-forme
Adresse MAC 47
Opérations 50
Plate-forme, Commandes
Console 200
get console 204
get hostname 220, 221
get os state 209
get power state 216
get product-id 222
Récapitulatif des sous-commandes relatives à la console 200
set console 206
set power state 217
Sous-commandes de la plate-forme
Relatives à l'état de l'alimentation 216
Relatives à l'état du SE 208
Tableau récapitulatif des sous-commandes 199
POST, Tableau des codes 258
Présentation
Chapitres du livre xxi
Gestion des serveurs 4
Prise en charge linguistique 33
Processeur de service
Adresse MAC 47
Agent SNMP 93
Assignation des paramètres réseau, DHCP 14
Assignation des paramètres réseau, Statique 16
Configuration automatique 43
Configuration initiale 14
Mise à jour du logiciel du SP 34
Sécurisation au moyen de comptes 19
Processeur de service (commandes), Voir Commande du SP
Propagation des paramètres du SP 43

R

Récapitulatif types de commandes 127
Redémarrage 50
Redirection console sur une connexion série
getty, Utilisation 117
grub, Utilisation 115
LILO, Utilisation 116
Paramètres du BIOS, Configuration 119
Présentation 114
securetty, Utilisation 118
Règle régissant
Mots de passe 19
Noms d'utilisateurs 19

S

Schéma
Arborescence de la MIB 91
Connexions entre serveurs 28
LAN 28
Options de gestion de serveurs 7
Script, Utilisation
Accès SSH en utilisant des clés publiques 111
Accès SSH en utilisant des hôtes de confiance 110
Clé publique, Ajout 107
Configuration de plusieurs systèmes 105
Conseils pour des résultats optimaux 113
Création de relations d'hôte de confiance 107
Directives 112
Génération d'une paire de clés d'hôte 108
Génération de clés d'hôte 106
Présentation 103
Scripts à distance avec SSH 105
Shell, Présentation des scripts 103
Sortie des commandes 112
securetty, Utilisation pour redirection console 118
Séquences d'échappement, console distante 124
Service d'annuaire 53
Mappage de groupes 54
Shell, Utilisation de scripts 103
Simple Network Management Protocol, voir Interface SNMP
SSH, Accès en utilisant
Clés publiques 111
Hôtes de confiance 110
ssh, Protocole de commande 126
SSH, Scripts à distance 105
Sun Fire V20z
Panneau arrière, Présentation 5
Plate-forme 5
Sun Fire V40z
Panneau arrière, Présentation 4
Plate-forme 4

T

Tableau
Codes de POST du BIOS 258
Récapitulatif codes de retour 129
Tâche de gestion de systèmes 12
TDU (Troubleshooting Dump Utility) 267
Type d'utilisateur, Définition 10
Type, Icônes 66