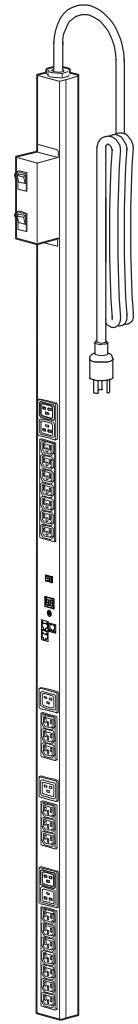
Guide d'utilisation

PDU en rack gérée
Unité de distribution de l'alimentation



GUIDE D'UTILISATION

PDU en rack gérée

Sommaire

Introduction

Caractéristiques du produit

La PDU gérée à monter en rack Dell® (PDU) est une unité de distribution de l'alimentation autonome, gérable en réseau. La PDU en rack permet une surveillance à distance en temps réel des charges connectées. Les alarmes configurées par l'utilisateur alertent sur les surcharges potentielles du circuit. La PDU en rack permet de contrôler totalement des sorties à l'aide de commandes à distance et de paramètres d'interface utilisateur.

Vous pouvez gérer une PDU en rack par l'intermédiaire de son interface Web, de son interface par lignes de commande ou du protocole simplifié de gestion de réseau (SNMP) :

- Accès à l'interface Web à l'aide du protocole HTTP (Hypertext Transfer Protocol) ou du protocole HTTPS (Hypertext Transfer Protocol avec Secure Sockets Layer [SSL]). Voir Connexion à l'interface Web.
- Accès à l'interface par lignes de commande par connexion série, Telnet ou Secure Shell (SSH). Voir À propos de l'interface par lignes de commande.
- Utilisation d'un navigateur SNMP et de la base de données de gestion (MIB) Dell pour gérer votre PDU en rack.

Les PDU en rack disposent des fonctionnalités supplémentaires suivantes :

- Pointe de charge et surveillance de la puissance et de la consommation d'énergie de toutes les charges connectées.
- Surveillance de la tension, du courant et de la puissance sur les phases.
- Surveillance de l'alimentation de chaque prise.
- Seuils d'alarme configurables permettant d'établir des alarmes de réseau et visuelles afin d'éviter les surcharges des circuits.

- Comptes d'accès utilisateur à quatre niveaux : Administrateur, Utilisateur de périphérique, Utilisateur en lecture seule et Utilisateur de sorties.
- Contrôle indépendant des sorties.
- Délais de mise sous tension configurables.
- Jusqu'à vingt-quatre comptes utilisateurs de sorties indépendants.
- Consignation des événements et des données. Le journal de consignation des événements est accessible par Telnet, Secure CoPy (SCP), protocole de transfert de fichiers FTP (File Transfer Protocol), connexion série ou navigateur Web (à l'aide du protocole HTTPS avec SSL ou du protocole HTTP). Le journal de consignation des données est accessible par navigateur Web ou par protocoles SCP ou FTP.
- Notifications par courriel des événements de la PDU en rack et des événements système.
- Traps SNMP, messages Syslog et notifications par courriel basés sur le niveau de gravité ou la catégorie des événements de la PDU en rack et des événements système.
- Protocoles de sécurité pour l'authentification et le codage.

La PDU en rack n'assure pas la protection contre les surtensions. Pour vous assurer que l'équipement connecté soit protégé contre les coupures de courant ou les surtensions, connectez la PDU en rack à un onduleur.

Priorités d'accès en connexion

Un seul utilisateur à la fois peut se connecter à la PDU en rack. Les priorités d'accès suivantes s'appliquent, en ordre décroissant :

- Accès local à l'interface par lignes de commande depuis un ordinateur relié directement en série à la PDU en rack.
- Accès Telnet ou Secure Shell (SSH) à l'interface par lignes de commande depuis un ordinateur distant.
- Accès Web.

Consultez SNMP pour des informations sur le contrôle d'accès SNMP à la PDU en rack.

Types de comptes utilisateurs

La PDU en rack a quatre niveaux d'accès (Administrateur, Utilisateur de périphérique, Utilisateur en lecture seule et Utilisateur de sorties) protégés par un mot de passe et un nom d'utilisateur.

- L'administrateur peut utiliser tous les menus de l'interface Web ainsi que toutes les commandes de l'interface par lignes de commande. Le nom d'utilisateur et le mot de passe par défaut sont tous les deux **admin**.
- Le niveau Utilisateur de périphérique permet d'accéder uniquement aux éléments suivants :
  - Dans l'interface Web, accès aux menus des onglets **Device Manager** (Gestionnaire d'appareil) et **Environment (Environnement)**, ainsi qu'aux journaux de consignation des événements et des données, accessibles sous les en-têtes **Events (Événements)** et **Data (Données)** du menu de navigation gauche de l'onglet **Logs (Journaux de consignation)**. Les journaux de consignation des événements et des données ne comprennent aucun bouton d'effacement du journal.
  - Dans l'interface par lignes de commande, accès aux fonctions et options équivalentes.

Le nom d'utilisateur et le mot de passe par défaut sont tous les deux **device**.

- Un utilisateur en lecture seule dispose de l'accès limité suivant :
  - Accès uniquement par l'intermédiaire de l'interface Web.
  - Accès aux mêmes onglets et menus que le niveau Utilisateur de périphérique, mais sans possibilité de modifier les configurations, de contrôler des périphériques, de supprimer des données, ni d'utiliser des options de transfert de fichiers. Les liens vers les options de configuration sont visibles mais désactivés. Les journaux de consignation des événements et des données ne comprennent aucun bouton d'effacement du journal.

  Le nom d'utilisateur et le mot de passe par défaut sont tous les deux **readonly**.

Pour définir les valeurs **User Name (Nom d'utilisateur)** et **Password (Mot de passe)** des trois types de comptes ci-dessus, consultez Configuration de l'accès utilisateur.

- Un utilisateur de sorties dispose de l'accès limité suivant :
  - Accès par l'interface Web et l'interface par lignes de commande.
  - Accès aux mêmes menus que le niveau Utilisateur de périphérique, mais avec une possibilité limitée de modifier les configurations, de contrôler des périphériques, de supprimer des données, ou d'utiliser des options de transfert de fichiers. Les liens vers les options de configuration sont visibles mais désactivés. Le niveau Utilisateur de sorties permet d'accéder à l'option de menu **Outlet Control** (Contrôle des sorties) qui permet à l'utilisateur de contrôler les sorties attribuées par l'administrateur. Les utilisateurs de sorties ne peuvent pas effacer les journaux de consignation des événements et des données.

  Le nom d'utilisateur et le mot de passe sont définis par l'administrateur pendant la procédure de création d'un nouvel utilisateur de sorties.

Pour commencer

Pour commencer à utiliser la PDU en rack :

1. Installez la PDU en rack en suivant les *instructions pour l'installation de l'unité de distribution de l'alimentation en rack* fournies avec la PDU.
2. Mettez l'appareil sous tension et connectez-vous à votre réseau. Suivez les indications des *instructions pour l'installation de l'unité de distribution de l'alimentation en rack*.
3. Définissez les paramètres réseau (voir Définition des paramètres réseau).
4. Commencez à utiliser la PDU en rack de l'une des manières suivantes :
   - Interface Web
   - Interface par lignes de commande
   - Panneau avant de la PDU en rack

Définition des paramètres réseau

Vous devez configurer les paramètres TCP/IP suivants pour que la PDU en rack puisse fonctionner en réseau :

- Adresse IP de la PDU en rack
- Masque de sous-réseau
- Passerelle par défaut.

En l'absence de passerelle par défaut disponible, utilisez l'adresse IP d'un ordinateur appartenant au même sous-réseau que la PDU en rack et qui soit généralement en fonctionnement. La PDU en rack utilise la passerelle par défaut pour tester le réseau lorsque le trafic est très faible.

N'utilisez pas l'adresse de retour en boucle (127.0.0.1) comme adresse de passerelle par défaut pour la PDU en rack. Ceci désactiverait la carte et nécessiterait de restaurer les paramètres TCP/IP par défaut en utilisant une connexion série locale.

Méthodes de configuration TCP/IP

Utilisez l'une des méthodes suivantes pour définir les paramètres TCP/IP requis par la PDU en rack :

- Configuration BOOTP & DHCP
- Interface par lignes de commande

Configuration BOOTP & DHCP

Le paramètre de configuration TCP/IP par défaut, **DHCP**, considère qu'un serveur DHCP correctement configuré est disponible pour fournir les paramètres TCP/IP aux PDU en rack. Vous pouvez également configurer ce paramètre pour BOOTP.

Un fichier de configuration utilisateur (.ini) peut servir de fichier de démarrage BOOTP ou DHCP. Pour plus d'informations, consultez Utilisation d'un fichier .ini.

BOOTP. Pour que la PDU en rack utilise un serveur BOOTP pour configurer ses paramètres TCP/IP, elle doit d'abord détecter un serveur BOOTP compatible RFC951 correctement configuré.

Dans le fichier BOOTPTAB du serveur BOOTP, entrez l'adresse MAC, l'adresse IP, le masque de sous-réseau et la passerelle par défaut de la PDU en rack et, si vous le souhaitez, un nom pour le fichier de démarrage. Pour connaître l'adresse MAC, regardez sous la PDU en rack ou consultez la fiche de contrôle qualité livrée avec l'unité.

Au redémarrage de la PDU en rack, le serveur BOOTP lui confère les paramètres TCP/IP.

- Si vous avez indiqué un nom de fichier d'amorçage, la PDU en rack tente de transférer ce fichier depuis le serveur BOOTP par protocole TFTP ou FTP. La PDU en rack intègre ainsi tous les paramètres spécifiés dans le fichier d'amorçage.
- Dans le cas contraire, vous pouvez configurer les autres paramètres de la PDU en rack à distance par l'intermédiaire de son Interface Web ou de l'Interface par lignes de commande.

Pour plus d'informations sur la création d'un fichier d'amorçage, reportez-vous à la documentation de votre serveur BOOTP.

DHCP. Vous pouvez utiliser un serveur DHCP compatible RFC2131/RFC2132 pour configurer les paramètres TCP/IP requis par la PDU en rack.

Cette section présente brièvement la communication de la PDU en rack avec un serveur DHCP. Pour plus de détails sur la manière dont un serveur DHCP peut configurer les paramètres réseau d'une PDU en rack, voir Options de réponse DHCP.

1. La PDU en rack transmet une requête DHCP utilisant les éléments d'auto-identification suivants :
   - Un identifiant de catégorie de fournisseur
   - Un identifiant client (par défaut, adresse MAC de la PDU en rack)
   - Un identifiant de catégorie d'utilisateur (par défaut, l'identification du microprogramme de l'application de la PDU en rack)
2. Un serveur DHCP correctement configuré renvoie une proposition DHCP contenant tous les paramètres requis par la PDU en rack pour établir une communication réseau. La proposition DHCP comprend également l'option Vendor Specific Information (Informations spécifiques au fournisseur) (option DHCP 43). La PDU en rack peut être configurée pour ignorer les propositions DHCP qui ne contiennent pas le cookie du fournisseur dans l'option DHCP 43 au format hexadécimal suivant (la PDU en rack ne nécessite pas ce cookie par défaut).

   ```
   Option 43 = 01 04 31 41 50 43
   ```

   où :
   - le premier octet (`01`) correspond au code,
   - le second octet (`04`) correspond à la longueur,
   - les octets restants (`31 41 50 43`) correspondent au cookie fournisseur.

Reportez-vous à la documentation de votre serveur DHCP pour obtenir de plus amples informations sur l'ajout de codes à l'option Vendor Specific Information.

Remarque : en cochant la case **Require vendor specific cookie to accept DHCP Address** (Exiger un cookie spécifique au fournisseur pour accepter l'adresse DHCP) dans l'interface Web, vous pouvez exiger que le serveur DHCP fournisse un cookie fournisseur avant de transmettre les informations des paramètres **Administration > Network** >**TCP/IP** > **ipv4 settings** (paramètres réseau TCP/IP > ipv4) de la PDU en rack.

Interface par lignes de commande

1. Connectez-vous à l'interface par lignes de commande. Voir Connexion à l'interface par lignes de commande.
2. Demandez à votre administrateur réseau l'adresse IP, le masque de sous-réseau et la passerelle par défaut de la PDU en rack.
3. Utilisez les trois commandes suivantes pour configurer les paramètres réseau (le texte en italiques indique une variable).
   a. `tcpip -i votre_adresse_IP`
   b. `tcpip -s votre_masque_de_sous-réseau`
   c. `tcpip -g votre_passerelle_par_défaut`

   Pour chaque variable, tapez une valeur numérique au format *xxx.xxx.xxx.xxx*.

   Par exemple, pour attribuer la valeur 156.205.14.141 à l'adresse IP, saisissez la commande suivante et appuyez sur la touche ENTRÉE :
   `tcpip -i 156.205.14.141`
4. Tapez **`exit`**. La PDU en rack redémarre pour appliquer les modifications.

Restauration suite à la perte du mot de passe

Vous pouvez accéder à l'interface par lignes de commande depuis un ordinateur local connecté à la PDU en rack ou à un autre dispositif par le biais du port série.

1. Sélectionnez un port série de l'ordinateur local et désactivez tout service exploitant ce port.
2. Connectez le câble série fourni au port choisi sur l'ordinateur et au port série de la PDU en rack.
3. Exécutez un programme d'émulation de terminal (tel que HyperTerminal®) et configurez le port sélectionné sur 9600 bits/s, 8 bits de données, sans parité, 1 bit d'arrêt et sans contrôle de flux.
4. Appuyez sur ENTRÉE, plusieurs fois si nécessaire, pour afficher l'invite **User Name (Nom d'utilisateur)**. Si l'invite **User Name** ne s'affiche pas, vérifiez les éléments suivants :
   - Le port série n'est pas utilisé par une autre application.
   - Les paramètres de terminal sont conformes à ceux indiqués à l'étape 3.
   - Le câble utilisé est conforme aux instructions de l'étape 2.
5. Appuyez sur le bouton **Reset** (Réinitialiser). Le voyant d'état clignote en orange et vert. Appuyez immédiatement une seconde fois sur le bouton **Reset** pendant que le voyant clignote pour restaurer temporairement les valeurs par défaut du nom d'utilisateur et du mot de passe.
6. Appuyez sur ENTRÉE autant de fois que nécessaire pour afficher à nouveau l'invite **User Name**, puis utilisez la valeur par défaut **dell** pour le nom d'utilisateur et le mot de passe (si vous n'êtes toujours pas connecté dans les 30 secondes suivant le réaffichage de la fenêtre **User name**, répétez l'étape 5 et connectez-vous à nouveau).

7. Dans l'interface par lignes de commande, tapez les commandes suivantes pour modifier les paramètres **User Name** et **Password**, qui sont redevenus **dell** :

   `user -an` ***`votre_nom_d'administrateur`***

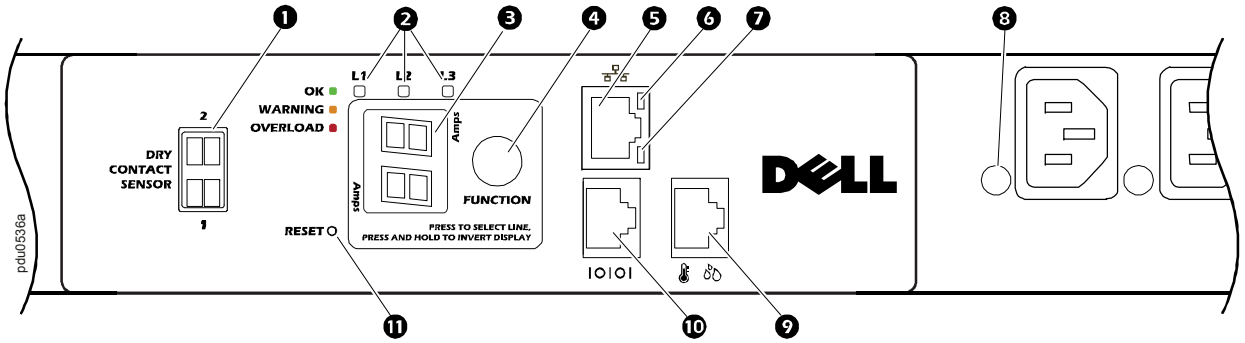
   `user -ap` ***`votre_mot_de_passe_administrateur`***

   Par exemple pour choisir **Don Adams** comme nom d'administrateur, tapez :

   `user -an Don Adams`

8. Tapez **`quit`** ou **`exit`** pour vous déconnecter, rebranchez les câbles série débranchés, puis redémarrez tous les services précédemment désactivés.

Panneau avant de la PDU en rack



Élément		Fonction
❶	Entrées à contact sec	Connecteur pour deux appareils à contact sec.
❷	Voyants de phase Remarque : les PDU en rack monophasées comportent un seul voyant.	Lorsqu'aucune alarme n'est présente, l'affichage indique la présence d'un courant de phase et un voyant de phase vert indique sur quelle phase. Le système contrôle successivement chacune des phases et affiche le courant de phase pendant trois secondes. Si une alarme est présente pour une phase, le voyant de phase concerné s'allume et reste allumé tant que la condition d'alarme subsiste. Le voyant s'allume en orange pour une alarme d'avertissement, en rouge pour une alarme critique. Si une alarme est présente sur plusieurs phases, le système contrôle automatiquement chaque phase en alarme et allume son voyant de phase pendant trois secondes.

Élément		Fonction
❸	Affichage DEL	Indique le courant de phase correspondant à la phase dont le voyant est allumé.
❹	Bouton Function	• Pour afficher manuellement le courant de chaque phase, appuyez sur ce bouton à plusieurs reprises. Le courant s'affiche pendant 30 secondes ou jusqu'à un nouvel appui sur le bouton (cette fonctionnalité n'est pas disponible pour les PDU en rack monophasées). • Pour afficher l'adresse IP, enfoncez et maintenez le bouton pendant cinq secondes jusqu'à ce que **IP** s'affiche, puis relâchez-le. L'adresse s'affiche sur l'écran DEL par séries de deux chiffres dont le cycle se répète. • Pour inverser l'affichage, enfoncez et maintenez le bouton pendant dix secondes jusqu'à ce que le schéma **AA** s'affiche. Maintenez le bouton enfoncé jusqu'à ce que l'orientation AA voulue s'affiche, puis relâchez-le.
❺	Connecteur 10/100 Base-T	Port de connexion de la PDU en rack au réseau.
❻	Voyant 10/100	Voir Voyant 10/100.
❼	Voyant d'état du réseau	Voir Voyant d'état du réseau.
❽	Voyant d'état de la sortie	S'allume en vert lorsque la sortie est alimentée (chaque sortie possède un voyant).
❾	Port du capteur de température/humidité	Port de connexion du capteur de température (G853N) ou d'un capteur de température/humidité (H621N) pour PDU en rack.

Élément		Fonction
⑩	Port série RJ-45	Port de connexion d'une PDU en rack à un programme d'émulation de terminal pour l'accès local à l'interface par lignes de commande. Utilisez le câble série fourni.
⑪	Bouton Reset	Pour redémarrer l'interface de la PDU en rack sans affecter les sorties, appuyez sur le bouton Reset et relâchez-le.

Voyant d'état du réseau

État	Description
Éteint	Vous êtes dans l'un des cas suivants : • La PDU en rack n'est pas alimentée. • La PDU en rack ne fonctionne pas correctement. Elle doit peut-être être réparée ou remplacée.
Vert fixe	Les paramètres TCP/IP de la PDU en rack sont valides.
Vert clignotant	Les paramètres TCP/IP de la PDU en rack ne sont pas valides.
Orange fixe	Détection d'une panne matérielle de la PDU en rack.
Orange clignotant	La PDU en rack effectue des requêtes BOOTP.
Orange et vert clignotant (alternativement)	Si le voyant clignote lentement, la PDU en rack émet des requêtes DHCP. S'il clignote rapidement, la PDU en rack est en cours de démarrage.

1. Si vous n'utilisez pas de serveur BOOTP ou DHCP, consultez Définition des paramètres réseau pour configurer les paramètres TCP/IP de la PDU en rack.
2. Pour utiliser un serveur DHCP, consultez Paramètres TCP/IP et de communication.

Voyant 10/100

État	Description
Éteint	Vous êtes dans l'un des cas suivants ou plusieurs : • La PDU en rack n'est pas alimentée. • Le câble reliant la PDU en rack au réseau est déconnecté ou défectueux. • L'appareil reliant la PDU en rack au réseau est hors tension. • La PDU en rack elle-même ne fonctionne pas correctement. Elle doit peut-être être réparée ou remplacée.
Vert fixe	La PDU en rack est connectée à un réseau fonctionnant à 10 mégabits par seconde (Mbps).
Orange fixe	La PDU en rack est connectée à un réseau fonctionnant à 100 Mbps.
Vert clignotant	La PDU en rack reçoit ou transmet des paquets de données à 10 Mbps.
Orange clignotant	La PDU en rack reçoit ou transmet des paquets de données à 100 Mbps.

Interface par lignes de commande

À propos de l'interface par lignes de commande

Vous pouvez utiliser l'interface par lignes de commande pour consulter l'état de la PDU en rack et la gérer. En outre l'interface par lignes de commande permet de créer des scripts pour un fonctionnement automatisé. Le niveau Administrateur permet l'accès complet à l'interface par lignes de commande, les niveaux Utilisateur de périphérique et Utilisateur de sorties permettent un accès limité, le niveau Utilisateur en lecture seule est totalement limité (pour plus de détails, voir Types de comptes utilisateurs).

Vous pouvez configurer tous les paramètres d'une PDU en rack (y compris ceux pour lesquels il n'existe pas de lignes de commande spécifiques) en utilisant l'interface par lignes de commande pour lui transférer un fichier INI. L'interface par lignes de commande utilise le protocole XMODEM pour effectuer le transfert. Toutefois XMODEM ne permet pas de lire le fichier INI actuel.

Connexion à l'interface par lignes de commande

Pour accéder à l'interface par lignes de commande, vous pouvez utiliser un ordinateur par le biais d'une connexion locale (série) ou d'une connexion à distance (Telnet ou SSH) au réseau de la PDU en rack.

Accès à distance à l'interface par lignes de commande

Vous pouvez accéder à l'interface par lignes de commande via Telnet ou SSH. Telnet est activé par défaut. L'activation de SSH provoque la désactivation de Telnet.

Pour activer ou désactiver ces méthodes d'accès, utilisez l'interface Web. Dans l'onglet **Administration**, sélectionnez **Network (Réseau)** dans la barre de menus supérieure, puis l'option d'**accès** sous **Console** dans le menu de navigation de gauche.

Telnet pour un accès de base. Telnet fournit une sécurité de base grâce à une authentification par nom d'utilisateur et mot de passe mais ne présente pas les avantages d'une haute sécurité par cryptage.

Pour accéder à l'interface par lignes de commande via Telnet :

1. À l'invite de commande sur un ordinateur connecté au même réseau que la PDU en rack, tapez **`telnet`** et l'adresse IP de la PDU en rack (par exemple **`telnet 139.225.6.133`**, lorsque la PDU en rack utilise le port Telnet 23 par défaut) et appuyez sur ENTRÉE.
   Si la PDU en rack utilise un numéro de port (de 5000 à 32768) autre que celui du port par défaut, vous devez ajouter le symbole deux-points ou un espace (selon votre client Telnet) à la suite de l'adresse IP (ou du nom de DNS), puis ce numéro de port. (Ces commandes sont celles généralement utilisées ; certains clients ne permettent pas de spécifier le port comme argument et d'autres peuvent nécessiter des commandes supplémentaires).
2. Entrez vos nom d'utilisateur et mot de passe (par défaut, **admin** et **admin** pour un administrateur ou **device** et **device** pour un utilisateur de périphérique).

Si vous avez oublié votre nom d'utilisateur ou votre mot de passe, consultez Restauration suite à la perte du mot de passe.

SSH pour un accès hautement sécurisé. Si vous utilisez le mode haute sécurité du protocole SSL pour l'interface Web, utilisez SSH pour accéder à l'interface par lignes de commande. SSH crypte les noms d'utilisateurs, les mots de passe et les données transmises. Que vous utilisiez l'interface par lignes de commande via SSH ou Telnet, l'interface, les comptes et les droits d'accès utilisateurs restent les mêmes ; mais pour utiliser SSH, vous devez d'abord le configurer et installer une application client SSH sur votre ordinateur.

Accès local à l'interface par lignes de commande

Pour accéder localement à l'interface par lignes de commande, utilisez un ordinateur connecté à la PDU en rack par un port série :

1. Sélectionnez un port série de l'ordinateur local et désactivez tout service utilisant ce port.
2. Connectez le câble série fourni du port choisi sur l'ordinateur au port série de la PDU en rack.
3. Exécutez un programme d'émulation de terminal (tel que HyperTerminal) et configurez le port sélectionné sur 9600 bits/s, 8 bits de données, sans parité, 1 bit d'arrêt et sans contrôle de flux.
4. Appuyez sur ENTRÉE puis, à l'invite, entrez votre nom d'utilisateur et votre mot de passe.

À propos de l'écran principal

Voici un exemple de l'écran principal, qui s'affiche lorsque vous vous connectez à l'interface par lignes de commande d'une PDU en rack :

```
Dell Corporation                          Network Management Card AOS  vx.x.x
(c)Copyright 2009 All Rights Reserved     RPDUD                        vx.x.x
-------------------------------------------------------------------------------
Name     : Test Lab                                    Date : 10/30/2009
Contact  : Don Adams                                   Time : 5:58:30
Location : Building 3                                  User : Administrator
Up Time  : 0 Days, 21 Hours, 21 Minutes                Stat : P+ N+ A+

cli>
```

Champs d'informations de l'écran principal :

- Deux champs identifient les versions du système d'exploitation (AOS) et du microprogramme de l'application (APP). Le nom du microprogramme de l'application identifie le type d'appareil connecté au réseau. Dans l'exémple précédent, le microprogramme de l'application de la PDU en rack est affiché.

  ```
  Network Management Card AOS  vx.x.x

  RPDUD vx.x.x
  ```

- Trois champs identifient le nom du système, la personne à contacter et l'emplacement de la PDU en rack (sur la console de contrôle, utilisez le menu **Système** pour définir ces valeurs).

  ```
  Name: Test Lab

  Contact: Don Adams

  Location: Building 3
  ```

- Un champ **Up Time** (temps d'utilisation) indique la durée de fonctionnement de la PDU en rack depuis son démarrage ou sa dernière réinitialisation.

  ```
  Up Time: 0 Days, 21 Hours, 21 Minutes
  ```

- Deux champs indiquent la date et l'heure de votre connexion.

  ```
  Date: 10/30/2009

  Time: 5:58:30
  ```

- Un champ **User** (Utilisateur) indique si vous vous êtes connecté en tant que compte **Administrateur** (« Administrator ») ou **Périphérique** (« Device ») (un **utilisateur en lecture seule** ne peut pas accéder à l'interface par lignes de commande).

  ```
  User : Administrator
  ```

- Un champ **Stat** indique l'état de la PDU en rack.

```
Stat : P+ N+ A+
```

P+	Le système d'exploitation Dell fonctionne correctement.

IPv4 uniquement	IPv6 uniquement	IPv4 et IPv6*	Description
N+	**N+**	**N4+ N6+**	Le réseau fonctionne correctement.
N?	**N6?**	**N4? N6?**	Un cycle de requêtes BOOTP est en cours.
N–	**N6–**	**N4– N6–**	La PDU en rack n'a pas réussi à se connecter au réseau.
N!	**N6!**	**N4! N6!**	Un autre périphérique utilise l'adresse IP de la PDU en rack.
* Les valeurs N4 et N6 peuvent être différentes : par exemple, il est possible d'avoir N4-N6+.			

A+	L'application fonctionne correctement.
A–	La somme de contrôle de l'application est incorrecte.
A?	L'application est en cours d'initialisation.
A!	L'application n'est pas compatible avec l'AOS.

Si P+ ne s'affiche pas, contactez Personnel d'assistance Dell.

Utilisation de l'interface par lignes de commande

L'interface par lignes de commande permet d'utiliser des commandes pour configurer la PDU en rack. Pour utiliser une commande, tapez cette commande et appuyez sur ENTRÉE. Les commandes et leurs arguments peuvent être saisis indifféremment en minuscules, en majuscules ou en mélange des deux. Les options sont sensibles à la casse.

Lorsque vous utilisez l'interface par lignes de commande, vous avez aussi différentes possibilités :

- Taper **`?`** et appuyer sur ENTRÉE permet d'afficher la liste des commandes disponibles en fonction de votre type de compte.
- Pour obtenir des informations sur le but et la syntaxe d'une commande donnée, tapez cette commande suivie d'un espace, puis du symbole **`?`** ou du mot **`help`**. Par exemple, pour afficher les options de configuration RADIUS, tapez :

  `radius ?`

  ou

  `radius help`

- Appuyez sur la touche flèche HAUT pour afficher la dernière commande saisie pendant la session. Les touches flèches HAUT et BAS permettent de parcourir jusqu'à dix commandes en liste.
- Tapez au moins un caractère d'une commande et appuyez sur la touche TAB pour parcourir la liste des commandes valides qui correspondent au texte que vous avez tapé dans la ligne de commande.
- Tapez **`exit`** ou **`quit`** pour fermer la connexion avec l'interface par lignes de commande.

Syntaxe des commandes

Élément	Description
-	Les options doivent être précédées d'un tiret.
< >	La définition d'une option doit être entourée par des crochets angulaires. Par exemple : `-dp <mot de passe du périphérique>`
[ ]	Si une commande accepte plusieurs options, ou si une option accepte des arguments mutuellement exclusifs, les valeurs peuvent être entourées par des crochets.
|	Une barre verticale entre des éléments entourés par des crochets indique que ces éléments sont mutuellement exclusifs. Vous devez utiliser l'un de ces éléments.

Exemmple d'une commande acceptant plusieurs options :

```
user [-an <nom d'administrateur>] [-ap <mot de passe administrateur>]
```

Dans cet exemple, la commande user accepte l'option **`-an`** qui définit le nom d'utilisateur avec droits d'administrateur, et l'option **`-ap`** qui définit le mot de passe Administrateur. Pour modifier le nom d'administrateur et son mot de passe en XYZ :

1. Tapez la commande « user » avec une option et l'argument **`XYZ`** :
   `user -ap XYZ`
2. Lorsque la première commande a été exécutée, tapez la commande « user » avec la deuxième option et l'argument **`XYZ`** :
   `user -an XYZ`

Exemple de commande dont une option accepte des arguments mutuellement exclusifs :

```
alarmcount -p [all | warning | critical]
```

Dans cet exemple, l'option -p accepte seulement trois arguments : all, warning ou critical (toutes les alarmes, alarmes d'avertissement, ou alarmes critiques). Par exemple, pour afficher le nombre d'alarmes critiques actives, tapez :
`alarmcount -p critical`

Cette commande échouera si vous tapez un argument autre que ceux spécifiés.

Codes de réponse aux commandes

Les codes de réponse aux commandes permettent de détecter des erreurs avec fiabilité par des opérations de script, sans que le texte du message d'erreur doive corresponde.

L'interface par lignes de commande fournit un rapport sur toutes les opérations commandées selon le format suivant :

E [0-9] [0-9] [0-9] : Message d'erreur

Code	Message	Code	Message
E000	Succès	E105	Préremplissage de commande
E001	Commande émise avec succès	E106	Données non disponibles
E002	Redémarrage nécessaire pour que les modifications prennent effet	E107	Communication série perdue avec la PDU en rack
E100	Échec de la commande		
E101	Commande inconnue		
E102	Erreur de paramètre		
E103	Erreur dans la ligne de commande		
E104	Refusé pour ce niveau d'utilisateur		

Description des commandes de la carte de gestion réseau

?

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description : Affiche la liste des commandes disponibles pour votre type de compte dans l'interface par lignes de commande. Pour afficher le texte de l'aide sur une commande spécifique, tapez cette commande suivie d'un point d'interrogation.

Exemple : Pour afficher la liste des options acceptées par la commande **`alarmcount`**, tapez :

```
alarmcount ?
```

about

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description : Affiche les informations relatives au matériel et au microprogramme. Ces informations sont utiles pour le dépannage et permetttent de déterminer si une mise à niveau du microprogramme est nécessaire.

alarmcount

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description :

Option	Arguments	Description
-p	all	Affiche le nombre d'alarmes actives signalées par la PDU en rack. Les informations sur ces alarmes figurent dans le journal de consignation des événements.
	warning	Affiche le nombre d'alarmes d'avertissement actives.
	critical	Affiche le nombre d'alarmes critiques actives.

Exemple : Pour afficher le nombre d'alarmes d'avertissement actives, tapez :

```
alarmcount -p warning
```

boot

Accès : Administrateur uniquement

Description : Définit comment la PDU en rack obtient ses paramètres réseau, notamment l'adresse IP, le masque de sous-réseau et la passerelle par défaut. Vous pouvez ensuite configurer les paramètres de serveur BOOTP ou DHCP.

Option	Argument	Description
-b <boot mode>	dhcp | bootp | manual	Définit comment les paramètres TCP/IP sont configurés au démarrage, à la réinitialisation ou au redémarrage de la PDU en rack. Consultez Paramètres TCP/IP et de communication pour des informations sur les paramètres de chacun des modes de démarrage.
-c	enable | disable	Uniquement pour les modes `dhcp` et `dhcpBootp`. Active ou désactive l'obligation que le serveur DHCP transmette le cookie fournisseur.
En général, il n'est pas nécessaire de modifier les valeurs par défaut suivantes de ces trois paramètres : -v <catégorie de fournisseur> : DELL -i <ID client> : adresse MAC de la PDU en rack, qui l'identifie de manière unique sur le réseau -u <catégorie d'utilisateur> : nom du module du microprogramme d'application.		

Exemple : Pour utiliser un serveur DHCP afin d'obtenir les paramètres réseau :

1. Tapez **`boot -b dhcp`**.
2. Activez l'obligation que le serveur DHCP transmette le cookie fournisseur :
   `boot -c enable`

cd

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description : Ouvre un dossier de l'arborescence de la PDU en rack.

Exemple°1 : Pour passer au dossier **`ssh`** afin de vérifier si un certificat de sécurité SSH a été téléchargé dans la PDU en rack :

1. Tapez **`cd ssh`** et appuyez sur ENTRÉE.
2. Tapez **`dir`** et appuyez sur ENTRÉE pour afficher la liste des fichiers contenus dans le dossier SSH.

Exemple°2 : Pour revenir au dossier principal du répertoire, tapez :

```
cd ..
```

console

Accès : Administrateur uniquement

Description : Définit le mode d'accès utilisateur à l'interface par lignes de commande : soit par Telnet (activé par défaut), soit par Secure Shell (SSH) qui ajoute une protection en transmettant les noms d'utilisateur, les mots de passe et les données sous forme cryptée. Vous pouvez changer le paramètre de port Telnet ou SSH pour ajouter une sécurité. Alternativement, vous pouvez aussi désactiver l'accès réseau à l'interface par lignes de commande.

Option	Argument	Description
-S	disable | telnet | ssh	Configure l'accès à l'interface par lignes de commande, ou en bloque l'accès avec la commande disable. L'activation de SSH active également SCP et désactive Telnet.
-pt	<numéro du port telnet>	Définit le port Telnet utilisé pour communiquer avec la PDU en rack (port 23 par défaut).
-ps	<numéro du port SSH>	Définit le port SSH utilisé pour communiquer avec la PDU en rack (port 22 par défaut).
-b	2400 | 9600 | 19200 | 38400	Configure la vitesse de transmission de la connexion par port série (9600 bits/s par défaut).

Exemple°1 : Pour activer l'accès SSH à l'interface par lignes de commande, tapez :

```
console -S ssh
```

Exemple°2 : Pour changer de port Telnet et utiliser le port 5000, tapez :

```
console -pt 5000
```

date

Accès : Administrateur uniquement

Définition : configure la date utilisée par la PDU en rack.

Pour une configuration où la date et l'heure de la PDU en rack sont définies par un serveur NTP, consultez Réglage de la date et de l'heure.

Option	Argument	Description
-d	<« chaîne de date »>	Entrez la date. Utilisez le format de date spécifié par la commande `date -f`.
-t	<00:00:00>	Définition de l'heure actuelle en heures, minutes et secondes. Utilisez le format horaire en 24 heures.
-f	mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd	Sélectionne le format numérique auquel toutes les dates seront affichées dans l'interface utilisateur. Chaque lettre (m pour mois, d pour jour et y pour année) représente un chiffre. Les jours et les mois calendaires à un seul chiffre sont affichés en deux chiffres commençant par un zéro.
-z	<décalage horaire>	Fixe le décalage par rapport à l'horaire GMT pour spécifier votre fuseau horaire. Cette option permet de vous synchroniser avec d'autres utilisateurs situés dans des fuseaux horaires différents.

Exemple°1 : Pour afficher la date au format aaaa-mm-jj, tapez :

```
date -f yyyy-mm-dd
```

Exemple°2 : Pour fixer la date au 30 octobre 2009, selon le format configuré dans l'exemple ci-dessus, tapez :

```
date -d "2009-10-30"
```

Exemple°3 : Pour fixer l'heure à 17 h, 21 min et 3 s, tapez :

```
date -t 17:21:03
```

delete

Accès : Administrateur uniquement

Description : Supprime un fichier du système de fichiers.

Argument	Description
<nom du fichier>	Tapez le nom du fichier à supprimer.

dir

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description : Affiche les fichiers et les dossiers enregistrés dans la PDU en rack.

dns

Accès : Administrateur uniquement

Définition : Configure les paramètres de DNS manuel (Domain Name System).

Paramètre	Argument	Description
-OM	enable | disable	Ignore le DNS manuel.
-p	<serveur DNS primaire>	Définit le serveur DNS primaire.
-s	<serveur DNS secondaire>	Définit le serveur DNS secondaire.
-d	<nom de domaine>	Définit le nom de domaine.
-n	<nom de domaine IPv6>	Définit le nom de domaine IPv6.
-h	<nom d'hôte>	Définit le nom d'hôte.

eventlog

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description : Affiche la date et l'heure auxquelles vous avez récupéré le journal de consignation des événements, l'état de la PDU en rack et l'état des capteurs connectés à la PDU en rack. Affiche les événements de périphérique les plus récents avec la date et l'heure auxquelles ils sont survenus. Utilisez les touches du clavier suivantes pour naviguer dans le journal de consignation des événements :

Touche	Description
ECHAP	Ferme le journal de consignation des événements et revient à l'interface par lignes de commande.
ENTRÉE	Actualise l'affichage du journal. Cette commande permet d'afficher les événements qui ont été enregistrés depuis que vous avez récupéré et affiché le journal.
ESPACE	Affiche la page suivante du journal de consignation des événements.
B	Affiche la page précédente du journal de consignation des événements. Cette commande n'est pas disponible à la page principale du journal.
D	Supprime le journal de consignation des événements. Suivez l'invite qui s'affiche pour confirmer ou refuser la suppression. Les événements supprimés ne peuvent plus être récupérés.

exit

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description : Ferme la session d'interface par lignes de commande.

format

Accès : Administrateur uniquement

Description : Reformate le système de fichiers de la PDU en rack et efface en totalité les certificats de sécurité, les clés de cryptage, les paramètres de configuration et les journaux de consignation des événements et des données.

Pour restaurer la configuration par défaut de la PDU en rack, utilisez la commande **`resetToDef`**.

FTP

Accès : Administrateur uniquement

Description : Active ou désactive l'accès au serveur FTP. En option, remplace le paramètre de numéro de port par le numéro d'un port inutilisé quelconque entre 5001 et 32768, afin de fournir une sécurité supplémentaire.

Option	Argument	Définition
-p	<numéro du port>	Définit le port TCP/IP utilisé par le serveur FTP pour communiquer avec la PDU en rack (port 21 par défaut). Le serveur FTP utilise à la fois le port du numéro spécifié et celui du numéro immédiatement inférieur.
-S	enable | disable	Active ou désactive l'accès au serveur FTP.

Exemple : Pour changer de port TCP/IP et utiliser le port 5001, tapez :

```
ftp -p 5001
```

help

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description : Affiche la liste des commandes disponibles pour votre type de compte dans l'interface par lignes de commande. Pour afficher le texte de l'aide sur une commande spécifique, tapez cette commande suivie de **`help`**.

Exemple°1 : Pour afficher la liste des commandes disponibles pour un Utilisateur de périphérique, tapez :

```
help
```

Exemple°2 : Pour afficher la liste des options acceptées par la commande **`alarmcount`**, tapez :

```
alarmcount help
```

netstat

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description : Affiche l'état du réseau et toutes les adresses IPv4 et IPv6 actives.

ntp

Accès : Administrateur

Définition : Affiche et configure les paramètres de protocole NTP (network time protocol).

Option	Argument	Définition
-OM	enable | disable	Ignore les paramètres manuels.
-p	<serveur NTP primaire>	Spécifie le serveur primaire.
-s	<serveur NTP secondaire>	Spécifie le serveur secondaire.

Exemple°1 : Pour activer l'instruction d'ignorer les paramètres manuels, tapez :

```
ntp -OM enable
```

Exemple°2 : Pour spécifier le serveur NTP primaire, tapez :

```
ntp -p 150.250.6.10
```

ping

Accès : Administrateur, Utilisateur de périphérique

Description. Détermine si le périphérique dont vous spécifiez l'adresse IP ou le nom DNS est connecté au réseau. Quatre demandes sont envoyées à cette adresse.

Argument	Description
<adresse IP ou nom DNS>	Tapez une adresse IP au format *xxx.xxx.xxx.xxx* ou le nom DNS configuré par le serveur DNS (serveur de noms de domaines).

Exemple : Pour déterminer si le périphérique ayant l'adresse IP 150.250.6.10 est connecté au réseau, tapez :

```
ping 150.250.6.10
```

portSpeed

Accès : Administrateur

Description :

Option	Arguments	Description
-s	auto | 10H | 10F | 100H | 100F	Fixe la vitesse de communication du port Ethernet. La commande `auto` permet aux périphériques Ethernet de négocier pour transmettre à la vitesse la plus rapide possible. Consultez Vitesse du port pour de plus amples informations sur les paramètres de vitesse du port.

Exemple : Pour configurer le port TCP/IP à une vitesse de communication de 100 Mbps en semi-duplex (communication dans un seul sens à la fois), tapez :

```
portspeed -s 100H
```

prompt

Accès : Administrateur, Utilisateur de périphérique

Description : Configure l'invite de l'interface par lignes de commande pour y inclure ou non le type de compte de l'utilisateur qui est en cours de session. Tous les utilisateurs peuvent modifier ce paramètre, ce qui met à jour tous les comptes utilisateur qui utiliseront alors la nouvelle configuration.

Option	Argument	Description
-s	long	L'invite inclut le type de compte utilisateur en cours de session.
	short	Paramètre par défaut. L'invite est constituée des quatre caractères suivants : `cli>`

Exemple : Pour inclure le type de compte de l'utilisateur en cours de session, tapez :

```
prompt -s long
```

quit

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description : Ferme la session de l'interface par lignes de commande (même fonctionnement que la commande « exit »).

radius

Accès : Administrateur uniquement

Description : Affiche les paramètres RADIUS existants, active ou désactive l'authentification RADIUS, et configure les paramètres d'authentification de base pour un ou deux serveurs RADIUS.

Pour le résumé de la configuration de serveur RADIUS et la liste des serveurs RADIUS pris en charge, consultez Configuration du serveur RADIUS.

D'autres paramètres d'authentification pour les serveurs RADIUS sont disponibles dans l'interface Web de la PDU en rack. Consultez RADIUS pour plus d'informations.

Pour des informations détaillées sur la configuration du serveur RADIUS, consultez Annexe B : Guide de sécurité.

Option	Argument	Description
-a	local | radiusLocal | radius	Configure l'authentification RADIUS : **`local`**—RADIUS est désactivé. L'authentification locale est activée. **`radiusLocal`**—RADIUS, puis authentification locale. Les authentifications RADIUS et locale sont activées. La première authentification demandée est celle du serveur RADIUS. Si le serveur RADIUS ne répond pas, l'authentification locale est utilisée. **`radius`**—RADIUS est activé. L'authentification locale est désactivée.

Option	Argument	Description
-p1 -p2	<IP du serveur>	Nom ou adresse IP du serveur RADIUS primaire ou secondaire. **REMARQUE :** les serveurs RADIUS utilisent le port 1812 par défaut pour authentifier les utilisateurs. Pour utiliser un port différent, ajoutez le signe deux points, suivi du nouveau numéro de port, à la suite du nom ou de l'adresse IP du serveur RADIUS.
-s1 -s2	<secret du serveur>	Secret partagé entre le serveur RADIUS primaire ou secondaire et la PDU en rack.
-t1 -t2	<délai de réponse du serveur>	Durée en secondes pendant laquelle la PDU en rack attend une réponse du serveur RADIUS primaire ou secondaire.

Exemple°1 :

Pour afficher les paramètres RADIUS existants de la PDU en rack, tapez **`radius`** et appuyez sur ENTRÉE.

Exemple°2 : Pour activer les authentifications RADIUS et locale, tapez :

```
radius -a radiusLocal
```

Exemple°3 : Pour configurer un délai de réponse de 10 secondes pour un serveur RADIUS secondaire, tapez :

```
radius -t2 10
```

reboot

Accès : Administrateur uniquement

Description : Redémarre l'interface de la PDU en rack.

resetToDef

Accès : Administrateur uniquement

Description :

Option	Arguments	Description
-p	all | keepip	Rétablit tous les paramètres par défaut, y compris les actions sur les événements, les paramètres de périphérique et, en option, les paramètres de configuration TCP/IP.

Exemple : Pour rétablir à leurs valeurs par défaut toutes les modifications de configuration sauf les paramètres TCP/IP de la PDU en rack, tapez :

```
resetToDef -p keepip
```

snmp, snmpv3

Accès : Administrateur uniquement

Description : Active ou désactive le protocole SNMP 1 ou SNMP 3.

Option	Arguments	Description
-S	enable | disable	Active ou affiche la version du protocole SNMP correspondant (1 ou 3).

Exemple : Pour activer SNMP version 1, tapez :

```
snmp -S enable
```

system

Accès : Administrateur uniquement

Description : Affiche et définit le nom système, la personne à contacter, l'emplacement et la durée de fonctionnement, ainsi que la date et l'heure, le nom de l'utilisateur connecté et l'état système à haut niveau (P, N et A, voir À propos de l'écran principal pour plus d'informations sur l'état du système).

Option	Argument	Description
-n	<nom système>	Définit le nom du périphérique, son emplacement, et le nom de la personne responsable de ce périphérique. **REMARQUE :** si vous entrez une valeur comprenant plus d'un mot, vous devez la mettre entre guillemets anglais.
-c	<personne à contacter>	
-l	<emplacement du système>	

Exemple°1 : Pour donner à l'emplacement du périphérique le nom **`Test Lab`**, tapez :

```
system -l "Test Lab"
```

Exemple°2 : Pour donner au système le nom **`Don Adams`**, tapez :

```
system -n "Don Adams"
```

tcpip

Accès : Administrateur uniquement

Description : Affiche et configure manuellement les paramètres réseau suivants de la PDU en rack :

Option	Argument	Description
-i	<adresse IP>	Tapez l'adresse IP de la PDU en rack, au format *xxx.xxx.xxx.xxx*
-s	<masque de sous-réseau>	Tapez le masque de sous-réseau de la PDU en rack.
-g	<passerelle>	Tapez l'adresse IP de la passerelle par défaut. **N'utilisez pas** l'adresse de retour en boucle (127.0.0.1) comme passerelle par défaut.
-d	<nom de domaine>	Tapez le nom DNS configuré par le serveur DNS.
-h	<nom d'hôte>	Tapez le nom d'hôte que la PDU en rack utilisera.

Exemple°1 : Pour afficher les paramètres réseau de la PDU en rack, tapez `tcpip` et appuyez sur ENTRÉE.

Exemple°2 : Pour configurer manuellement l'adresse IP `150.250.6.10` pour la PDU en rack, tapez :

```
tcpip -i 150.250.6.10
```

tcpip6

Accès : Administrateur uniquement

Description : Active IPv6, affiche et configure manuellement les paramètres réseau suivants de la PDU en rack :

Option	Argument	Description
-S	enable | disable	Active ou désactive IPv6.
-man	enable | disable	Active l'adressage manuel pour l'adresse IPv6 de la PDU en rack.
-auto	enable | disable	Active la configuration automatique de l'adresse IPv6 pour la PDU en rack.
-i	<adresse IPv6>	Définit l'adresse IPv6 de la PDU en rack.
-g	<passerelle IPv6>	Définit l'adresse IPv6 de la passerelle par défaut.
-d6	router | stateful | stateless | never	Définit le mode DHCPv6 avec la possibilité des paramètres suivants : contrôlé par le routeur, état complet (état conservé pour l'adresse et autres informations), sans état (état non conservé pour les informations autres que l'adresse), jamais.

Exemple°1 : Pour afficher les paramètres réseau de la PDU en rack, tapez **`tcpip6`** et appuyez sur ENTRÉE.

Exemple°2 : Pour configurer manuellement l'adresse IPv6 **`2001:0:0:0:0:FFD3:0:57ab`** pour la PDU en rack, tapez :

```
tcpip -i 2001:0:0:0:0:FFD3:0:57ab
```

user

Accès : Administrateur uniquement

Description : Configure le nom d'utilisateur, le mot de passe et le délai d'inactivité pour les comptes de type Administrateur, Utilisateur de périphérique et Utilisateur en lecture seule.

Pour plus d'informations sur les autorisations accordées à chaque type de compte, consultez Types de comptes utilisateurs.

Option	Argument	Description
-an -dn -rn	<nom d'administrateur> <nom du périphérique> <nom d'utilisateur en lecture seule>	Définit le nom d'utilisateur (sensible à la casse) pour chaque type de compte. La longueur maximum est de 10 caractères.
-ap -dp -rp	<mot de passe d'administrateur> <mot de passe du périphérique> <mot de passe d'utilisateur en lecture seule>	Définit le mot de passe (sensible à la casse) pour chaque type de compte. La longueur maximum est de 32 caractères. Un mot de passe vierge (aucun caractère) n'est pas autorisé.
-t	<minutes>	Fixe la durée d'attente (3 minutes par défaut) du système avant de déconnecter un utilisateur inactif.

Exemple°1 : Pour modifier le nom d'administrateur en XYZ, tapez :

```
user -an XYZ
```

Exemple°2 : Pour faire passer le délai de déconnexion en cas d'inactivité à 10 minutes, tapez :

```
user -t 10
```

web

Accès : Administrateur uniquement

Description : Active l'accès à l'interface Web en utilisant le protocole HTTP ou HTTPS.

Pour plus de sécurité, vous pouvez changer le paramètre de port HTTP ou HTTPS en choisissant un port inutilisé entre 5000 et 32768. Les utilisateurs devront alors insérer le signe deux points (« : ») dans le champ d'adresse de leur navigateur pour spécifier ce numéro de port. Par exemple, pour se connecter par le port numéro 5000 et l'adresse IP 152.214.12.114, tapez :

```
http://152.214.12.114:5000
```

Option	Argument	Définition
-S	disable | http | https	Configure l'accès à l'interface Web. Lorsque le protocole HTTPS est activé, les données sont cryptées pendant la transmission et authentifiées par un certificat numérique.
-ph	<n° de port HTTP>	Définit le port TCP/IP utilisé par le protocole HTTP pour communiquer avec la PDU en rack (port 80 par défaut).
-ps	<n° de port HTTPS>	Définit le port TCP/IP utilisé par le protocole HTTPS pour communiquer avec le PDU en rack (port 443 par défaut).

Exemple : Pour empêcher tout accès à l'interface Web, tapez :

```
web -S disable
```

xferINI

Accès : Administrateur uniquement

Description : Utilise le protocole XMODEM pour télécharger un fichier .ini pendant que vous êtes connecté à l'interface par lignes de commande par une connexion série. Lorsque le téléchargement est terminé :

- S'il y a des modifications du système ou du réseau, l'interface par lignes de commande redémarre et vous devrez vous connecter de nouveau.
- Si vous aviez sélectionné pour le transfert du fichier une vitesse de transfert différente de la vitesse par défaut définie pour la PDU en rack, vous devrez rétablir la vitesse par défaut afin de permettre de nouveau la communication avec la PDU en rack.

xferStatus

Accès : Administrateur uniquement

Description : Affiche le résultat du dernier transfert de fichier.

Consultez Contrôle des mises à niveau et des mises à jour pour la description des codes de résultat des transferts de fichiers.

Description des commandes de périphérique

devLowLoad

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de définir ou de consulter le seuil de faible charge en kilowatts pour le périphérique.

Exemple°1 : Pour consulter le seuil de faible charge, tapez :

```
cli> devLowLoad
E000: Success
0.5 kW
```

Exemple°2 : Pour fixer le seuil de faible charge à 1 kW, tapez :

```
cli> devLowLoad 1.0
E000: Success
```

devNearOver

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de définir ou de consulter le seuil proche de la surcharge en kilowatts pour le périphérique.

Exemple°1 : Pour consulter le seuil proche de la surcharge, tapez :

```
cli> devNearOver
E000: Success
20.5 kW
```

Exemple°2 : Pour fixer le seuil proche de la surcharge à 21,3 kW, tapez :

```
cli> devNearOver 21.3
E000: Success
```

devOverLoad

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de définir ou de consulter le seuil de surcharge en kilowatts pour le périphérique.

Exemple°1 : Pour consulter le seuil de surcharge, tapez :

```
cli> devOverLoad
E000: Success
25.0 kW
```

Exemple°2 : Pour fixer le seuil de surcharge à 25,5 kW, tapez :

```
cli> devOverLoad 25.5
E000: Success
```

devReading

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de consulter la puissance totale en kilowatts ou l'énergie totale en kilowatt-heures pour le périphérique.

Argument	Définition
power	Permet de consulter la puissance totale en kilowatts
energy	Permet de consulter l'énergie totale en kilowatts-heures

Exemple°1 : Pour consulter la puissance totale, tapez :

```
cli> devReading power
E000: Success
5.2 kW
```

Exemple°2 : Pour consulter l'énergie totale, tapez :

```
cli> devReading energy
E000: Success
200.1 kWh
```

devStartDly

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de régler ou de consulter le délai (en secondes) à ajouter au Délai de mise sous tension de chaque sortie une fois que la PDU en rack est alimentée. Valeurs autorisées : plage de 1 à 300 secondes ou jamais (ne jamais allumer).

Exemple°1 : Pour consulter le délai de démarrage à froid, tapez :

```
cli> devStartDly
E000: Success
5 seconds
```

Exemple°2 : Pour fixer le délai de démarrage à froid à six secondes, tapez :

```
cli> devStartDly 6
E000: Success
```

humLow

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de consulter ou de fixer le seuil de faible humidité en pourcentage de l'humidité relative.

Exemple°1 : Pour consulter le seuil de faible humidité, tapez :

```
cli> humLow
E000: Success
10 %RH
```

Exemple°2 : Pour fixer le seuil de faible humidité, tapez :

```
cli> humLow 12
E000: Success
```

humMin

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de consulter ou de fixer le seuil minimum d'humidité en pourcentage de l'humidité relative.

Exemple°1 : Pour consulter le seuil minimum d'humidité, tapez :

```
cli> humMin
E000: Success
6 %RH
```

Exemple°2 : Pour fixer le seuil minimum d'humidité, tapez :

```
cli> humMin 8
E000: Success
```

humReading

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description : Permet de consulter l'humidité détectée par le capteur.

Exemple : Pour consulter l'humidité détectée, tapez :

```
cli> humReading
E000: Success
25 %RH
```

inNormal

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de consulter l'état normal de chaque entrée à contact sec.

Exemple : Pour consulter l'état normal de chaque entrée à contact sec, tapez :

```
cli> inNormal
E000: Success
1: Open
2: Open
```

inReading

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de consulter l'état actuel de chaque entrée à contact sec.

Exemple : Pour consulter l'état de chaque entrée à contact sec, tapez :

```
cli> inReading
E000: Success
1: Open
2: Open
```

olAssignUsr

Accès : Administrateur

Description : Permet d'attribuer le contrôle de sorties à un utilisateur de sorties existant dans la base de données locale.

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.
<user>	Utilisateur existant dans la base de données locale (voir userAdd).

Exemple°1 : Pour attribuer un utilisateur nommé Bobby aux sorties 3, 5 à 7, et 10, tapez :

```
cli> olAssignUsr 3,5-7,10 bobby
E000: Success
```

Exemple°2 : Pour attribuer un utilisateur nommé Billy à toutes les sorties, tapez :

```
cli> olAssignUsr all billy
E000: Success
```

olCancelCmd

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : annule toutes les commandes en attente pour une sortie ou un groupe de sorties.

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.

Exemple : Pour annuler toutes les commandes pour la sortie 3, tapez :

```
cli> olCancelCmd 3
E000: Success
```

olDlyOff

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de mettre hors tension une sortie ou un groupe de sorties une fois le délai de mise hors tension écoulé (voir olOff).

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.

Exemple°1 : Pour mettre hors tension les sorties 3, 5 à 7, et 10, tapez :

```
cli> olDlyOff 3,5-7,10
E000: Success
```

Exemple°2 : Pour mettre toutes les sorties hors tension, tapez :

```
cli> olDlyOff all
E000: Success
```

olDlyOn

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de mettre sous tension une sortie ou un groupe de sorties une fois le délai de mise sous tension écoulé (voir olOnDelay).

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.

Exemple°1 : Pour mettre sous tension les sorties 3, 5 à 7, et 10, tapez :

```
cli> olDlyOn 3,5-7,10
E000: Success
```

Exemple°2 : Pour mettre sous tension la sortie configurée sous le nom Sortie1, tapez :

```
cli> olDlyOn Sortie1
E000: Success
```

olDlyReboot

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de couper puis rétablir l'alimentation d'une sortie ou d'un groupe de sorties. Les sorties spécifiées sont mises hors tension en fonction du délai de mise hors tension configuré (voir olOffDelay). Lorsque la plus longue durée de redémarrage (voir olRbootTime) des sorties sélectionnées est écoulée, celles-ci sont remises sous tension en fonction des délais de mise sous tension (voir olOnDelay) configurés pour elles.

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.

Exemple°1 : Pour couper puis rétablir l'alimentation des sorties 3, 5 à 7, et 10, tapez :

```
cli> olDlyReboot 3,5-7,10
E000: Success
```

Exemple°2 : Pour couper puis rétablir l'alimentation de la sortie configurée sous le nom Sortie1, tapez :

```
cli> olDlyReboot Sortie1
E000: Success
```

olGroups

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties.

Description : Répertorie les groupes de synchronisation de sorties définis pour la PDU en rack (voir Configuration et contrôle des groupes de sorties pour plus d'informations).

Exemple : Pour répertorier les groupes de synchronisation de sorties, tapez :

```
cli> olGroups
E000: Success
Outlet Group A:
159.215.6.141 -> Outlets: 2,4,5
159.215.6.143 -> Outlets: 2,8
Outlet Group B:
159.215.6.141 -> Outlets: 1
159.215.6.166 -> Outlets: 1
```

olLowLoad

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de fixer ou de consulter le seuil d'avertissement de charge faible de sorties.

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.
<puissance>	Nouveau seuil de la sortie (en watts).

Exemple°1 : Pour régler le seuil de faible charge sur 2 watts pour toutes les sorties, tapez :

```
cli> olLowLoad all 2
E000: Success
```

Exemple°2 : Pour consulter le seuil de faible charge pour les sorties 3 et 5 à 7, tapez :

```
cli> olLowLoad 3,5-7
E000: Success
3: BobbysServer: 2 W
5: BillysServer: 2 W
6: JoesServer: 2 W
7: JacksServer: 2 W
```

olName

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de définir ou de consulter le nom configuré pour une sortie.

Argument	Description
all	Toutes les sorties des appareils.
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.
<nouveau nom>	Nom d'une sortie spécifique. Utilisez uniquement des lettres et des chiffres.

Exemple : Pour configurer la sortie 3 sous le nom BobbysServer, tapez :

```
cli> olName 3 BobbysServer
E000: Success
3: BobbysServer
5: BillysServer
6: JoesServer
7: JacksServer
```

olNearOver

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de régler ou de consulter le seuil d'avertissement de proximité de surcharge de sorties.

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.
<puissance>	Nouveau seuil de la sortie (en watts).

Exemple°1 : Pour consulter le seuil de proximité de surcharge pour les sorties 3 et 5 à 7, tapez :

```
cli> olNearOver 3,5-7
E000: Success
3: BobbysServer: 5 W
5: BillysServer: 6 W
6: JoesServer: 5 W
7: JacksServer: 4 W
```

Exemple°2 : Pour régler le seuil de proximité de surcharge des sorties 3 et 5 à 7 sur six watts, tapez :

```
cli> olNearOver 3,5-7 6
E000: Success
3: BobbysServer: 6 W
5: BillysServer: 6 W
6: JoesServer: 6 W
7: JacksServer: 6 W
```

olOff

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de mettre hors tension sans délai une sortie ou un groupe de sorties.

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.

Exemple°1 : Pour mettre hors tension les sorties 3 et 5 à 7, tapez :

```
cli> olOff 3,5-7
E000: Success
```

olOffDelay

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de définir ou de consulter le délai pour la commande de mise hors tension avec délai (voir olDlyOff) et pour la commande de redémarrage avec délai (voir olDlyReboot).

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.
<durée>	Durée du délai dans la plage de 1 à 7200 secondes (2 heures).

Exemple°1 : Pour régler un délai de 9 secondes avant la mise hors tension des sorties 3 et 5 à 7, tapez :

```
cli> olOffDelay 3,5-7 9
E000: Success
```

Exemple°2 : Pour consulter le délai de la commande de mise hors tension avec délai des sorties 3 et 5 à 7, tapez :

```
cli> olOffDelay 3,5-7
E000: Success
3: BobbysServer: 9 sec
5: BillysServer: 9 sec
6: JoesServer: 9 sec
7: JacksServer: 9 sec
```

olOn

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de mettre sous tension sans délai une sortie ou un groupe de sorties.

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.

Exemple°1 : Pour mettre sous tension les sorties 3 et 5 à 7, tapez :

```
cli> olOn 3,5-7
E000: Success
```

olOnDelay

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de définir ou de consulter le délai pour la commande de mise sous tension avec délai (voir olDlyOn) et pour la commande de redémarrage avec délai (voir olDlyReboot).

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.
<durée>	Durée du délai dans la plage de 1 à 7200 secondes (2 heures).

Exemple°1 : Pour régler un délai de 6 secondes avant la mise sous tension des sorties 3 et 5 à 7, tapez :

```
cli> olOnDelay 3,5-7 6
E000: Success
```

Exemple°2 : Pour consulter le délai de la commande de mise sous tension avec délai des sorties 3 et 5 à 7, tapez :

```
cli> olOnDelay 3,5-7
E000: Success
3: BobbysServer: 6 sec
5: BillysServer: 6 sec
6: JoesServer: 6 sec
7: JacksServer: 6 sec
```

olOverLoad

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de régler ou de consulter le seuil d'avertissement de surcharge de sorties.

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.
<puissance>	Nouveau seuil de la sortie (en watts).

Exemple°1 : Pour consulter le seuil de surcharge pour les sorties 3 et 5 à 7, tapez :

```
cli> olOverLoad 3,5-7
E000: Success
3: BobbysServer: 7 W
5: BillysServer: 8 W
6: JoesServer: 7 W
7: JacksServer: 6 W
```

Exemple°2 : Pour régler le seuil de surcharge des sorties 3 et 5 à 7 sur sept watts, tapez :

```
cli> olOverLoad 3,5-7 7
E000: Success
3: BobbysServer: 7 W
5: BillysServer: 7 W
6: JoesServer: 7 W
7: JacksServer: 7 W
```

olRbootTime

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de définir ou de consulter la durée de maintien hors tension de sorties pour une commande de redémarrage avec délai (voir olDlyReboot).

Exemple°1 : Pour consulter la durée fixée pour le maintien hors tension des sorties 3 et 5 à 7 pendant un redémarrage, tapez :

```
cli> olRbootTime 3,5-7
E000: Success
3: BobbysServer: 4 sec
5: BillysServer: 5 sec
6: JoesServer: 7 sec
7: JacksServer: 2 sec
```

Exemple°2 : Pour définir la durée du maintien hors tension des sorties 3 et 5 à 7 pendant un redémarrage, tapez :

```
cli> olRebootTime 3,5-7 10
E000: Success
3: BobbysServer: 10 sec
5: BillysServer: 10 sec
6: JoesServer: 10 sec
7: JacksServer: 10 sec
```

olReading

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de consulter le courant, la puissance ou l'énergie d'une sortie ou d'un groupe de sorties.

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.
current | power | energy	Nouveau seuil de la sortie (en watts).

Exemple°1 : Pour consulter le courant des sorties 3 et 5 à 7, tapez :

```
cli> olReading 3,5-7 current
E000: Success
3: BobbysServer: 4 A
5: BillysServer: 5 A
6: JoesServer: 7 A
7: JacksServer: 2 A
```

Exemple°2 : Pour consulter la puissance de la sortie 3, tapez :

```
cli> olReading 3 power
E000: Success
3: BobbysServer: 40 W
```

Exemple°3 : Pour consulter l'énergie de la sortie JoesServer, tapez :

```
cli> olReading joesserver energy
E000: Success
6: JoesServer: 7,3 kWh
```

olReboot

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de couper puis de rétablir l'alimentation d'une sortie ou d'un groupe de sorties sans délai. Si plusieurs sorties sont spécifiées, cette procédure s'applique à toutes ces sorties en même temps.

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.

Exemple : Pour redémarrer les sorties 3 et 5 à 7, tapez :

```
cli> olReboot 3,5-7
E000: Success
```

olStatus

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Permet de consulter l'état des sorties spécifiées.

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.

Exemple : Pour consulter l'état des sorties 3 et 5 à 7, tapez :

```
cli> olStatus 3,5-7
E000: Success
3: BobbysServer: On
5: BillysServer: Off
6: JoesServer: Off
7: JacksServer: On
```

olUnasgnUsr

Accès : Administrateur

Description : Permet de supprimer le contrôle des sorties d'un utilisateur de sorties existant dans la base de données locale.

Argument	Description
all	Toutes les sorties des appareils.
<nom de la sortie>	Nom configuré pour une sortie spécifique (voir olName).
<n° de sortie>	Numéro unique ou plage de numéros séparés par un tiret, ou liste avec virgules séparatrices de numéros ou de plages de numéros de sorties.
<utilisateur>	Utilisateur existant dans la base de données locale (voir userList).

Exemple°1 : Pour supprimer le contrôle des sorties 3, 5 à 7, et 10 par l'utilisateur nommé Bobby, tapez :

```
cli> olUnasgnUsr 3,5-7,10 bobby
E000: Success
```

Exemple°2 : Pour supprimer le contrôle de toutes les sorties par l'utilisateur nommé Billy, tapez :

```
cli> olUnasgnUsr all billy
E000: Success
```

phLowLoad

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de fixer ou de consulter le seuil de faible charge des phases en kilowatts. Pour spécifier les phases, choisissez l'une des options suivantes. Tapez : **`all`** (pour toutes les phases), le numéro d'une phase, une plage de phases ou une liste de phases séparées par des virgules.

Exemple°1 : Pour fixer le seuil de faible charge sur 1 kW pour toutes les phases, tapez :

```
cli> phLowLoad all 1
E000: Success
```

Exemple°2 : Pour consulter le seuil de faible charge pour les phases 1 à 3, tapez :

```
cli> phLowLoad 1-3
E000: Success
1: 1 A
2: 1 A
3: 1 A
```

phNearOver

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de fixer ou de consulter le seuil proche de la surcharge des phases en kilowatts. Pour spécifier les phases, choisissez l'une des options suivantes. Tapez : **`all`** (pour toutes les phases), le numéro d'une phase, une plage de phases ou une liste de phases séparées par des virgules.

Exemple°1 : Pour fixer le seuil proche de la surcharge sur 10 kW pour toutes les phases, tapez :

```
cli> phNearOver all 10
E000: Success
```

Exemple°2 : Pour consulter le seuil proche de la surcharge pour les phases 1 à 3, tapez :

```
cli> phNearOver 1-3
E000: Success
1: 10 A
2: 10 A
3: 10 A
```

phOverLoad

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de fixer ou de consulter le seuil de surcharge des phases en kilowatts. Pour spécifier les phases, choisissez l'une des options suivantes. Tapez : **all** (pour toutes les phases), le numéro d'une phase, une plage de phases ou une liste de phases séparées par des virgules.

Exemple°1 : Pour fixer le seuil de surcharge sur 13 kW pour toutes les phases, tapez :

```
cli> phOverLoad all 13
E000: Success
```

Exemple°2 : Pour consulter le seuil de surcharge pour les phases 1 à 3, tapez :

```
cli> phOverLoad 1-3
E000: Success
1: 13 A
2: 13 A
3: 13 A
```

phReading

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de consulter le courant, la tension ou la puissance d'une phase. Permet de fixer ou de consulter le seuil proche de la surcharge des phases en kilowatts. Pour spécifier les phases, choisissez l'une des options suivantes. Tapez : **`all`** (pour toutes les phases), le numéro d'une phase, une plage de phases ou une liste de phases séparées par des virgules.

Exemple°1 : Pour consulter la mesure du courant de la phase 3, tapez :

```
cli> phReading 3 current
E000: Success
3: 4 A
```

Exemple°2 : Pour consulter la tension de chaque phase, tapez :

```
cli> phReading all voltage
E000: Success
1: 120 V
2: 120 V
3: 120 V
```

Exemple°3 : Pour consulter la puissance de la phase 2, tapez :

```
cli> phReading 2 power
E000: Success
2: 40 W
```

phRestrictn

Accès : Administrateur

Description : Permet de régler ou de consulter la fonction de restriction de surcharge afin d'empêcher la mise sous tension de sorties lorsque le seuil d'alarme de surcharge est dépassé. Les arguments acceptables sont **`none`** (aucune), **`near (proche)`** et **`over`** (dépassement). Pour spécifier les phases, choisissez l'une des options suivantes. Tapez : **`all`** (pour toutes les phases), le numéro d'une phase, une plage de phases ou une liste de phases séparées par des virgules.

Exemple°1 : Pour régler la restriction de surcharge de la phase trois sur aucune, tapez :

```
cli> phRestrictn 3 none
E000: Success
```

Exemple°2 : Pour consulter les restrictions de surcharge de toutes les phases, tapez :

```
cli> phRestrictn all
E000: Success
1: over
2: near
3: none
```

prodInfo

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description : Permet de consulter les informations relatives à la PDU en rack.

Exemple :

```
cli> prodInfo
E000: Success
AOS vX.X.X.X
Managed Rack PDU vX.X.X.X
Model:              DELL6xxx
Present Outlets:    12
Switched Outlets:   12
Metered Outlets:    0
Max Current:        20 A
Phases:             1
```

sensorName

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de définir ou de consulter le nom attribué au port du capteur de température/humidité de la PDU en rack.

Exemple°1 : Pour définir comme nom du port « Sensor1 », tapez :

```
cli> sensorName Sensor1
E000: Success
```

Exemple°2 : Pour afficher ensuite le nom du port du capteur, tapez :

```
cli> sensorName
E000: Success
Sensor1
```

tempHigh

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de fixer ou de consulter le seuil de température élevée en degrés Fahrenheit ou Celsius.

Exemple°1 : Pour régler le seuil de température élevée sur 70º Fahrenheit, tapez :

```
cli> tempHigh F 70
E000: Success
```

Exemple°2 : Pour consulter le seuil de température élevée en degrés Celsius, tapez :

```
cli> tempHigh C
E000: Success
21 C
```

Exemple°3 : Pour consulter le seuil de température élevée en degrés Fahrenheit, tapez :

```
cli> tempHigh F
E000: Success
70 F
```

tempMax

Accès : Administrateur, Utilisateur de périphérique

Description : Permet de fixer ou de consulter le seuil de température maximum en degrés Fahrenheit ou Celsius.

Exemple°1 : Pour fixer le seuil de température maximum sur 80º Fahrenheit, tapez :

```
cli> tempMax F 80
E000: Success
```

Exemple°2 : Pour fixer le seuil de température maximum en degrés Celsius, tapez :

```
cli> tempMax C
E000: Success
27 C
```

Exemple°3 : Pour consulter le seuil de température maximum en degrés Fahrenheit, tapez :

```
cli> tempMax F
E000: Success
80 F
```

tempReading

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description : Permet de consulter la température en degrés Fahrenheit ou Celsius détectée par le capteur.

Exemple : Pour consulter la température en degrés Fahrenheit, tapez :

```
cli> tempReading F
E000: Success
51,1 F
```

userAdd

Accès : Administrateur

Description : Permet d'ajouter un utilisateur de sorties à la base de données locale.

Exemple : Pour ajouter un utilisateur nommé Bobby, tapez :

```
cli> userAdd Bobby
E000: Success
```

userDelete

Accès : Administrateur

Description : Permet de supprimer un utilisateur de sorties dans la base de données locale.

Exemple : Pour supprimer un utilisateur nommé Bobby, tapez :

```
cli> userDelete Bobby
E000: Success
```

userList

Accès : Administrateur, Utilisateur de périphérique et Utilisateur de sorties, mais uniquement pour les sorties auxquelles l'utilisateur est attribué.

Description : Répertorie les utilisateurs et les sorties qui leur sont attribuées.

Exemple°1 : En vous connectant en tant qu'administrateur, tapez :

```
cli> userList
E000: Success
Local: admin: 1,2,3,4,5,6,7,8
Local: Bobby: 1,3
Local: Billy: 2,5
Local: Joe: 4,6
Local: Jack: 7,8
```

Exemple°2 : En vous connectant en tant que Billy, tapez :

```
cli> userList
E000: Success
Local: Billy: 2,5
```

userPasswd

Accès : Administrateur.

Description : Permet de définir le mot de passe d'un utilisateur de sorties.

Exemple : Pour définir le mot de passe de Bobby comme « abc123 », tapez :

```
cli> userPasswd Bobby abc123 abc123
E000: Success
```

whoami

Accès : Administrateur, Utilisateur de périphérique, Utilisateur de sorties

Description : Permet de consulter le nom d'utilisateur de l'utilisateur actif.

Exemple :

```
cli> whoami
E000: Success
admin
```

Interface Web

Navigateurs Web pris en charge

Vous pouvez utiliser le navigateur Microsoft® Internet Explorer® (IE) version 7.x ou supérieure (uniquement sur systèmes d'exploitation Windows®) ou Mozilla® Firefox® version 3.0.6 ou supérieure (sur tous les systèmes d'exploitation) pour accéder à la PDU en rack via son interface Web. Il est possible que d'autres navigateurs couramment utilisés conviennent, mais ceux-ci n'ont pas été soumis à des tests complets.

La PDU en rack n'est pas compatible avec un serveur proxy. Avant d'utiliser un navigateur Web pour accéder à son interface Web, vous devez procéder comme suit :

- Configurez votre navigateur Web de sorte qu'il désactive l'utilisation d'un serveur proxy pour la PDU en rack.
- Configurez le serveur proxy de sorte qu'il n'utilise pas l'adresse IP spécifique de la PDU en rack.

Connexion à l'interface Web

Présentation

Vous pouvez utiliser le nom DNS ou l'adresse IP système de la PDU en rack comme adresse URL de l'interface Web. Utilisez votre nom d'utilisateur et votre mot de passe (en respectant les majuscules) pour vous connecter. Le nom d'utilisateur et le mot de passe par défaut varient selon le type de compte :

- **admin/admin** pour le niveau Administrateur
- **device/device** pour le niveau Utilisateur de périphérique
- **readonly/readonly** pour le niveau Utilisateur en lecture seule

Pour les comptes Utilisateur de sorties, il n'existe pas de nom d'utilisateur ni de mot de passe par défaut. Un administrateur doit définir le nom d'utilisateur, le mot de passe et les autres caractéristiques du compte d'un utilisateur de sorties. Voir Configuration d'un utilisateur de sorties.

Si vous utilisez le protocole HTTPS (SSL/TLS) comme protocole d'accès, vos informations d'authentification sont comparées à celles que contient un certificat de serveur. Si le certificat a été créé avec l'Assistant de sécurité, et qu'une adresse IP a été spécifiée comme nom générique dans le certificat, vous devez utiliser cette adresse IP pour vous connecter à la PDU en rack. Si un nom DNS a été spécifié comme nom générique dans le certificat, vous devez utiliser ce nom DNS pour vous connecter.

Pour de plus amples informations sur la page Web qui apparaît lorsque vous vous connectez à l'interface Web, consultez À propos de l'onglet Home (Accueil).

Formats d'adresse URL

Tapez le nom DNS de la PDU en rack ou son adresse IP dans le champ d'adresse URL du navigateur Web et appuyez sur ENTRÉE. Lorsque vous spécifiez dans Internet Explorer un port de serveur Web qui n'est pas le port par défaut , l'URL doit contenir **`http://`** ou **`https://`**.

Messages d'erreur courants du navigateur au moment de la connexion.

Message d'erreur	Cause de l'erreur	Navigateur
« Vous n'êtes pas autorisé à afficher cette page » ou « Un utilisateur est actuellement connecté... »	Un autre utilisateur est connecté.	Internet Explorer, Firefox
« Impossible d'afficher cette page ».	L'accès par Internet est désactivé, ou l'URL n'est pas correcte.	Internet Explorer
« Connexion impossible ».		Firefox

Exemples de formats d'URL.

- Pour un nom DNS « Web1 » :
  - **`http://Web1`** si votre mode d'accès est HTTP.
  - **`https://Web1`** si votre mode d'accès est HTTPS.
- Pour une adresse IP système 139.225.6.133 et le port de serveur Web par défaut (80) :
  - **`http://139.225.6.133`** si votre mode d'accès est HTTP.
  - **`https://139.225.6.133`** si votre mode d'accès est HTTPS (HTTP avec SSL)
- Pour une adresse IP système 139.225.6.133 et un port de serveur Web autre que le port par défaut (5000) :
  - **`http://139.225.6.133:5000`** si votre mode d'accès est HTTP.
  - **`https://139.225.6.133:5000`** si votre mode d'accès est HTTPS (HTTP avec SSL).
- Pour une adresse IPv6 système de 2001:db8:1::2c0:b7ff:fe00:1100 et un port de serveur Web autre que le port par défaut (5000) :
  - **`http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000`** si votre mode d'accès est HTTP.

Fonctionnalités de l'interface Web

Lisez les informations qui suivent pour vous familiariser avec les fonctionnalités de base de l'interface Web de votre PDU en rack.

Onglets

Les onglets suivants sont disponibles :

- **Home** (Accueil) : s'affiche lorsque vous vous connectez. Permet de consultez les alarmes actives, l'état de la charge de la PDU en rack et les événements les plus récents concernant la PDU en rack. Pour plus d'informations, consultez À propos de l'onglet Home (Accueil).
- **Device Manager** (Gestionnaire d'appareils) : permet de consulter l'état de la charge, de configurer les seuils de charge et de consulter et gérer les mesures de pointe de charge de l'ensemble des appareils, phases et sorties connectés selon le cas. Permet aussi de gérer et contrôler les sorties. Pour plus d'informations, consultez À propos de l'onglet Device Manager (Gestionnaire d'appareils).
- **Environment** (Environnement) : permet de consulter les données des capteurs de température et d'humidité lorsqu'un capteur est connecté à la **PDU en rack**.
- **Logs** (Journaux de consignation) : permet de consulter les journaux de consignation des événements, des données et du système.
- **Administration** : permet de configurer les paramètres de sécurité, de connexion réseau, de notification, ainsi que les paramètres généraux.

Icônes d'état de l'appareil

Une ou plusieurs icônes avec infobulle indiquent l'état actuel du fonctionnement de la PDU en rack :

	**Critical** (Critique) : une alarme critique existe et nécessite une action immédiate.
	**Warning** (Avertissement) : une alarme nécessite votre attention et pourrait mettre en péril vos données ou votre équipement si le problème n'est pas corrigé.
	**No Alarms** (Aucune alarme) : aucune alarme n'est présente et la PDU en rack fonctionne normalement.

Dans le coin supérieur droit de chaque page, l'interface Web affiche les mêmes icônes que celles actuellement affichées dans la page d'accueil afin de signaler l'état de la PDU en rack :

- L'icône **Aucune alarme** si aucune alarme n'est présente.
- Une des autres icônes (**Critique** et **Avertissement**) en cas d'alarme, voire les deux, suivie du nombre d'alarmes actives à son niveau de gravité.

Pour revenir à l'onglet **Home (Accueil)** et consulter le récapitulatif de l'état de la PDU en rack, y compris les alarmes actives, cliquez sur une icône d'état instantané d'une page de l'interface.

Liens rapides

Dans le coin inférieur gauche de l'interface se trouvent trois liens configurables. Paramètres par défaut de ces liens :

- **Lien 1** : dell.com
- **Lien 2** : dell.com/home
- **Lien 3 :** dell.com/business

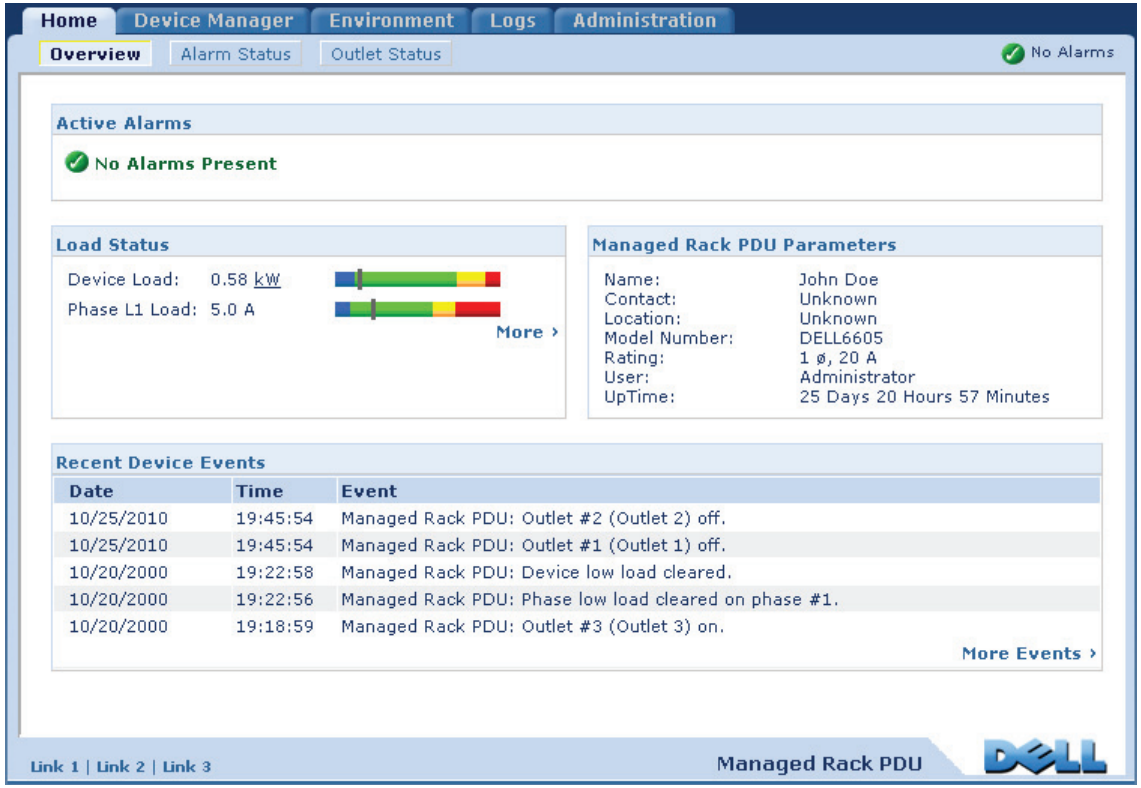
Pour reconfigurer les liens, consultez Configuration des liens.

Autres fonctions de l'interface Web

- L'adresse IP s'affiche dans le coin supérieur gauche.
- Un lien d'aide contextuelle (**Help**) et un lien de déconnexion (**Log off**) sont situés dans le coin supérieur droit.

À propos de l'onglet Home (Accueil)

Utilisez l'onglet Home pour consulter les alarmes actives, l'état de la charge et les événements les plus récents concernant la PDU en rack.

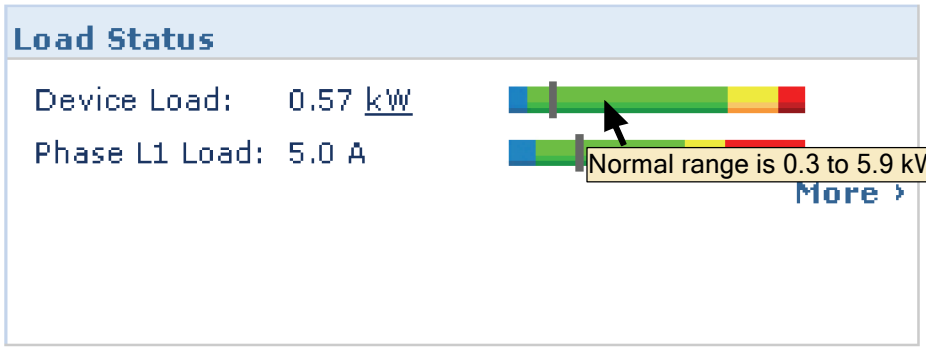


Écran Overview (Vue d'ensemble)

Chemin d'accès : Home > Overview

Le haut de la page Overview indique l'état des alarmes. Si une ou plusieurs alarmes sont présentes, le nombre et le type d'alarmes sont indiqués avec un lien vers l'écran **Alarm Status (État des alarmes)** , dans lequel vous pouvez consulter une description de chaque alarme. S'il n'y a aucune alarme, l'écran Overview affiche « No Alarms Present ».

Dans la zone **Load Status** (État de la charge), vous pouvez consulter la charge pour le périphérique (kW) et pour les phases (Amp), le cas échéant. Les compteurs vert, jaune et rouge indiquent l'état actuel de la charge : normal, proche de la surcharge ou surcharge. Notez que si un seuil de charge faible a été configuré, le compteur comprend également un segment bleu à gauche du vert. Placez le curseur au-dessus des couleurs pour consulter les seuils de charge fixés.



Cliquez sur **More** (Plus) pour aller à l'onglet **Device Manager** (Gestionnaire d'appareil) afin de fixer les seuils et de consulter et gérer les informations relatives aux pointes de charge.

Dans la zone des paramètres de l'appareil, consultez le nom d'utilisateur, la personne à contacter, l'emplacement, le courant nominal, le type de compte utilisateur accédant à la PDU en rack, ainsi que le temps de fonctionnement de la PDU en rack depuis le dernier redémarrage à la suite d'un cycle de mise sous tension ou d'un redémarrage de l'interface de gestion (pour plus d'informations, consultez Réinitialisation de la PDU en rack).

Dans la zone **Recent Device Events (Événements de périphérique récents)**, consultez en ordre chronologique inverse les événements les plus récents avec la date et l'heure auxquelles il sont survenus. Cinq événements au maximum s'affichent simultanément. Cliquez sur **More Events (Autres événements)** pour aller à l'onglet **Logs** (Journaux de consignation) afin de consulter la totalité du journal de consignation des événements.

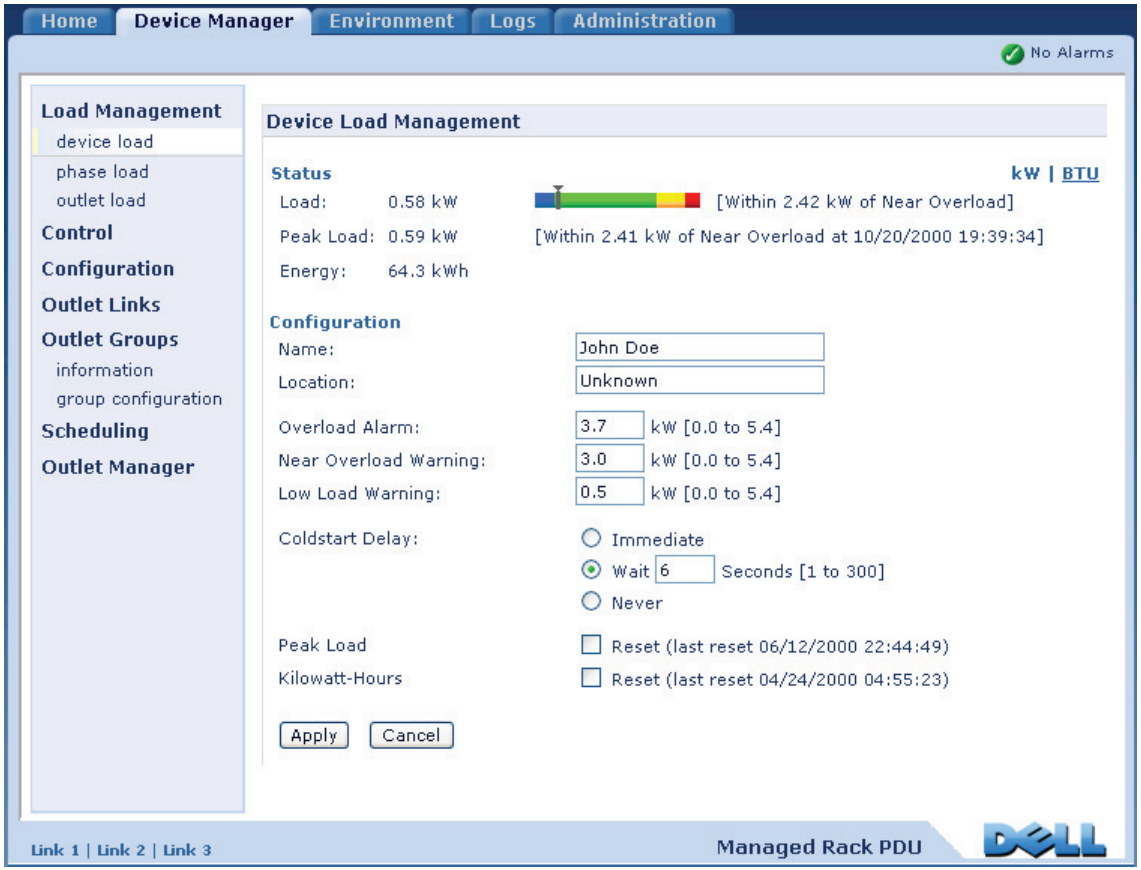
Écran Alarm Status (État des alarmes)

Chemin d'accès : Home > Alarm Status

L'écran **Alarm Status (État des alarmes)** fournit une description de toutes les alarmes présentes.

Pour plus de détails sur le dépassement d'un seuil de température ou d'humidité, cliquez sur l'onglet Environment.

Gestion de l'appareil



À propos de l'onglet Device Manager (Gestionnaire d'appareils)

Chemin d'accès : Device Manager

L'onglet **Device Manager** permet les opérations suivantes :

- Consulter l'état de la charge de la PDU en rack.
- Configurer les seuils de charge pour tous les appareils connectés et pour chaque phase concernée.
- Gérer et contrôler les sorties.
- Configurer un nom et un emplacement pour la PDU en rack.
- Consulter et gérer la mesure des pointes de charge.
- Cliquer sur des liens configurables par l'utilisateur pour ouvrir les pages Web des appareils spécifiques connectés à la PDU en rack.

Affichage de l'état de la charge et des pointes de charge

Chemin d'accès : Device Manager > *Load Management options*

L'aiguille du compteur vert, jaune et rouge indique l'état de la charge : normal, proche de la surcharge ou surcharge. Si un seuil de charge faible a été configuré, le compteur comprend également un segment bleu à gauche du vert. Lorsque vous consultez la charge de l'appareil (**Device Load**), le triangle au-dessus du compteur indique la pointe de charge.

Cliquez sur **kW | BTU** dans le coin supérieur droit pour afficher les valeurs de charge soit en kilowatts, soit en British Thermal Units (BTU).

Configuration des seuils de charge

Chemin d'accès : Device Manager > *Load Management options*

Pour configurer les seuils de charge :

1. Cliquez sur l'onglet **Device Manager** (Gestionnaire d'appareils).
2. Pour configurer les seuils de charge de l'appareil ou des phases, effectuez la sélection dans le menu Load Management (Gestion de la charge).
3. Réglez les seuils **Overload Alarm** (Alarme de surcharge), **Near Overload Warning** (Avertissement de proximité de surcharge) et **Low Load Warning** (Avertissement de charge faible).
4. Cliquez sur **Apply (Appliquer)**.

Configuration du nom et de l'emplacement de la PDU en rack

Chemin d'accès : Device Manager > Load Management > Device Load

Le nom et l'emplacement saisis s'affichent dans l'onglet **Home** (Accueil).

Vous pouvez définir le nom et l'emplacement par l'intermédiaire de l'onglet Device Manager (Gestionnaire d'appareils) ou Administration. Une modification de l'un des éléments affecte l'autre.

1. Cliquez sur l'onglet **Device Manager**, puis sur **device load** (charge du périphérique) dans le menu **Load Management** (Gestion de la charge).
2. Entrez un nom et un emplacement.
3. Cliquez sur **Apply**.

Réglage du délai de démarrage à froid

Chemin d'accès : Device Manager > Device Load

Le délai de démarrage à froid correspond au nombre de secondes ajoutées au délai de mise sous tension de chaque sortie une fois la PDU en rack alimentée. Les valeurs autorisées sont : de 1 à 300 secondes, **Immediate** (Immédiatement) ou **Never** (Jamais) (aucune mise sous tension).

1. Cliquez sur l'onglet **Device Manager**, puis sur **device load** (charge du périphérique) dans le menu **Load Management** (Gestion de la charge).
2. Sélectionnez le réglage du **Délai de démarrage à froid**.
3. Cliquez sur **Apply**.

Réinitialisation de la pointe de charge et des kWh

Chemin d'accès : Device Manager > Device Load

1. Cliquez sur l'onglet **Device Manager**, puis sur **device load** (charge du périphérique) dans le menu **Load Management** (Gestion de la charge).
2. Cochez les cases **Peak Load** (Pointe de charge) et **Kilowatt-Hours** selon les besoins.
3. Cliquez sur **Apply**.

Configuration et contrôle des groupes de sorties

Terminologie des groupes de sorties

Un *groupe de sorties* est constitué de sorties associées logiquement sur une même PDU en rack. Les sorties qui appartiennent à un groupe de sorties se mettent sous tension, hors tension et redémarrent de manière synchronisée :

- Un *groupe de sorties local* comprend deux sorties ou plus sur une PDU en rack. Seules les sorties de ce groupe sont synchronisées.
- Un *groupe de sorties global* comprend une ou plusieurs sorties sur une PDU en rack. Une sortie est configurée en tant que *sortie globale,* ce qui relie logiquement son groupe de sorties à d'autres groupes de sorties sur d'autres PDU en rack (jusqu'à 3 PDU). Toutes les sorties des groupes de sorties globaux ainsi associés sont synchronisées.
  - Pour les groupes de sorties globaux, le *groupe de sorties maître* est le groupe qui déclenche les actions.
  - Par rapport aux groupes de sorties globaux, un *groupe de sorties esclave* est un groupe de sorties qui est synchronisé avec un groupe de sorties maître.

Lorsque vous appliquez une action de contrôle de sortie sur des sorties qui sont membres d'un groupe de sorties, celles-ci sont synchronisées comme suit :

- Pour un groupe de sorties global, utilisez les délais et les durées de redémarrage configurés pour la sortie globale du groupe de sorties maître.
- Pour un groupe de sorties local, les sorties utilisent les délais et la durée de redémarrage de la sortie du groupe dont le numéro est le plus petit.

Objet et avantages des groupes de sorties

L'utilisation de groupes de sorties synchronisées sur des PDU en rack permet de s'assurer que les sorties se mettent hors tension, sous tension et redémarrent de manière synchronisée. La synchronisation des actions des groupes de contrôle par l'intermédiaire des groupes de sorties offre les avantages suivants.

- L'arrêt et le démarrage synchronisés de l'alimentation des serveurs à double alimentation permet d'éviter les signalements erronés de pannes de courant au cours d'un arrêt ou d'un redémarrage planifié du système.
- La synchronisation des sorties à l'aide de groupes de sorties fournit un délai d'arrêt et de redémarrage plus précis que le délai des prises individuelles.
- Une sortie globale est visible sur l'interface utilisateur de n'importe quelle PDU en rack à laquelle elle est associée.

Configuration requise pour les groupes de sorties

Pour configurer et utiliser des groupes de contrôle de sorties synchronisés :

- Vous avez besoin d'un réseau TCP/IP 10/100Base-T, équipé d'un concentrateur ou d'un commutateur Ethernet disposant d'une source d'alimentation indépendante des ordinateurs ou des autres appareils destinés à être synchronisés.
- Si des groupes de sorties doivent être synchronisés sur plusieurs PDU en rack, ces PDU en rack doivent répondre aux exigences suivantes :
  - Faire partie du même sous-réseau.
  - Utiliser des microprogrammes ayant le même numéro de version pour le module du système d'exploitation (AOS) et le module d'application.
- Vous avez besoin d'un ordinateur capable de lancer les opérations de contrôle synchronisé par l'intermédiaire de l'interface Web ou l'interface par lignes de commande des PDU en rack, ou via le protocole SNMP.
- Les groupes de sorties synchronisés doivent avoir la même adresse IP de multidiffusion. Assurez-vous que chaque commutateur Ethernet qui connecte les PDU en rack autorise le trafic réseau en multidiffusion pour cette adresse IP de multidiffusion.

Règles de configuration des groupes de sorties

Pour un système qui utilise des groupes de sorties, les règles suivantes s'appliquent :

- Une PDU en rack peut comprendre plusieurs groupes de sorties, mais une sortie ne peut appartenir qu'à un seul groupe de sorties.
- Un groupe de sorties local n'ayant aucune sortie globale doit comprendre deux sorties ou plus.
- Vous pouvez synchroniser un groupe de sorties global sur une PDU en rack avec un groupe de sorties global sur chacune de trois autres PDU en rack.
  - Dans un groupe de sorties global, une seule sortie peut être définie comme sortie globale pour l'associer aux groupes de sorties sur d'autres PDU en rack afin de les synchroniser. Ce groupe de sorties global peut être constitué de cette seule sortie globale, ou comprendre plusieurs sorties.
  - Pour associer les groupes de sorties sur une PDU en rack afin de les synchroniser, ces PDU en rack doivent avoir le même nom et la même adresse de multidiffusion, et fonctionner sous la même version de microprogramme de PDU en rack.
  - Dans un groupe de sorties global, le numéro de sortie physique de la sortie globale doit être identique à celui de la sortie globale de tout autre groupe de sorties auquel cette sortie est associée.
- Pour créer et configurer des groupes de sorties, vous devez utiliser l'interface Web ou exporter les paramètres du fichier de configuration (fichier .ini) d'une PDU en rack configurée. L'interface par lignes de commande permet de savoir si une sortie est membre d'un groupe de sorties et d'appliquer des actions de contrôle sur un groupe de sorties, mais pas de créer un groupe de sorties ni de le configurer.

Activation des groupes de sorties

Cliquez sur l'onglet **Device Manager** (Gestionnaire d'appareils) et sélectionnez **Group Configuration** (Configuration de groupe) dans le menu de navigation gauche **Outlet Groups** (Groupes de sorties). Configurez les paramètres suivants et cliquez sur **Apply**.

Activer la création de groupes de sorties.

Paramètre	Description
Device Level Outlet Group (Groupe de sorties, niveau appareil)	Pour créer un groupe de sorties, ce paramètre doit être activé. Ce paramètre est désactivé par défaut.

Activer le support pour les groupes de sorties globaux (groupes reliés).

Paramètre	Description
Multicast Name (Nom de multidiffusion)	Pour relier des groupes de sorties sur plusieurs PDU en rack, vous devez définir un nom de multidiffusion et une adresse IP de multidiffusion identiques sur chacune de ces PDU en rack.
Multicast IP (IP de multidiffusion)	**REMARQUE :** Quatre appareils au maximum peuvent être configurés avec le même nom de multidiffusion et la même adresse IP de multidiffusion.

Activer le codage et l'authentification des groupes de sorties.

Paramètre	Description
Authentication Phrase (Clé d'authentification)	Clé de 15 à 32 caractères ASCII qui confirme que l'appareil communique avec d'autres appareils, que le message n'a pas été modifié au cours de la transmission, et que le message a été communiqué en temps utile. La clé d'authentification indique qu'il n'a subi aucun retard et qu'il n'a pas été copié puis renvoyé ultérieurement à une heure inappropriée.
Clé de cryptage	Clé de 15 à 32 caractères ASCII qui garantit la confidentialité des données (à l'aide d'un cryptage).

Définition du port du groupe de sorties.

Paramètre	Description
Outlet Group Port (Port du groupe de sorties)	Numéro de port sur lequel l'appareil va communiquer avec d'autres appareils.

Les appareils qui tentent de se synchroniser avec des groupes de sorties présents sur d'autres appareils doivent tous avoir une clé d'authentification, une clé de cryptage et un numéro de port de groupe identiques. Ces valeurs ne sont pas visibles par l'utilisateur.

Création d'un groupe de sorties local

1. Dans l'onglet **Device Manager** (Gestionnaire d'appareils), sélectionnez **Information** dans le menu de navigation gauche **Outlet Groups** (Groupes de sorties).
2. Assurez-vous que les groupes de sorties sont activés (voir Activation des groupes de sorties).
3. Cliquez sur **Create Local Outlet Group** (Créer un groupe de sorties local).
4. Sous l'option **Select Local Outlets** (Sélectionner les sorties locales), sélectionnez chacune des sorties qui feront partie du groupe et attribuez un nom à ce groupe dans le champ **Outlet Group Name** (Nom du groupe de sorties). Vous devez sélectionner au moins deux sorties.

Création de plusieurs groupes de sorties globaux

Pour créer plusieurs groupes de sorties globaux reliés à des groupes de sorties sur d'autres PDU en rack :

1. Dans l'onglet **Device Manager** (Gestionnaire d'appareils), sélectionnez **Information** dans le menu de navigation gauche **Outlet Groups** (Groupes de sorties).
2. Assurez-vous que les groupes de sorties sont activés et que les paramètres de multidiffusion (nom et adresse IP) sont identiques pour toutes les PDU en rack à associer (voir Activation des groupes de sorties).
3. Cliquez sur **Create Global Outlet Groups** (Créer des groupes de sorties globaux).
4. Pour chaque groupe de sorties global que vous créez, sélectionnez une sortie en cochant sa case. Cliquez ensuite sur **Apply**. Par exemple, sélectionnez cinq sorties pour créer cinq groupes de sorties comprenant chacun une sortie globale.
5. Pour ajouter des sorties aux groupes de sorties globaux que vous avez créés, consultez Modification ou suppression d'un groupe de sorties.

Modification ou suppression d'un groupe de sorties

1. Dans l'onglet **Device Manager** (Gestionnaire d'appareils), sélectionnez **Information** dans le menu de navigation gauche **Outlet Groups** (Groupes de sorties).
2. Sous **Configured Outlet Groups** (Groupes de sorties configurés), cliquez sur le numéro ou le nom du groupe de sorties à modifier ou supprimer.

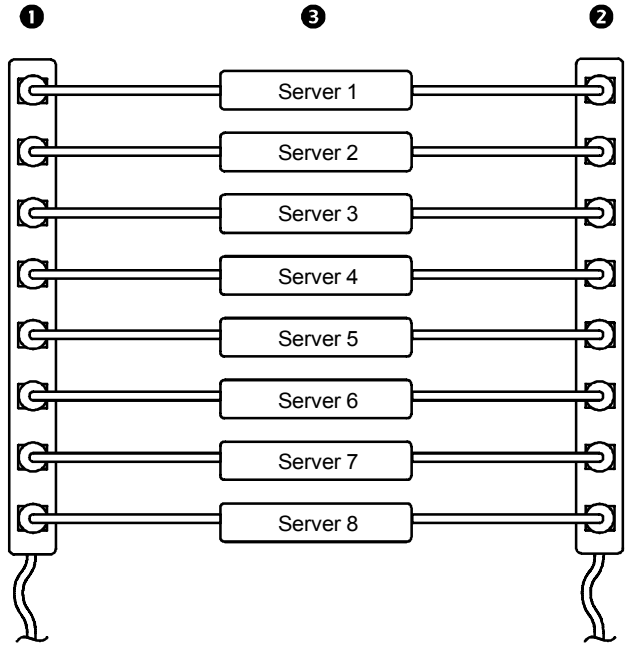
3. Lorsque vous modifiez un groupe de sorties, vous pouvez effectuer les opérations suivantes :
   - Renommer le groupe de sorties.
   - Ajouter ou supprimer des sorties en cochant ou en décochant les cases correspondantes.

   Vous ne pouvez pas supprimer une sortie d'un groupe de sorties contenant seulement deux sorties, sauf si la sortie restante est une sortie globale.

4. Pour supprimer le groupe de sorties, cliquez sur **Delete Outlet Group** (Supprimer le groupe de sorties).

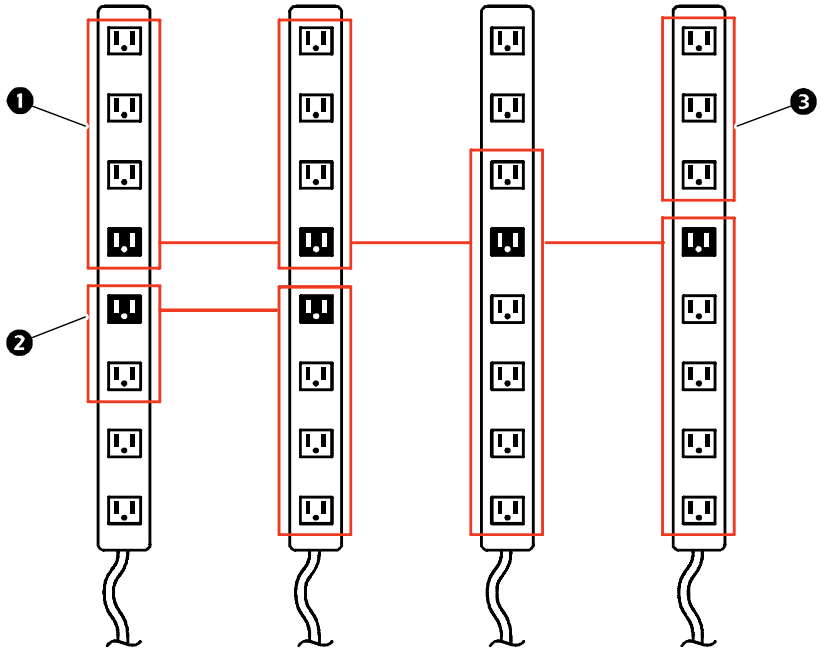
Configurations typiques de groupes de sorties

La configuration suivante montre deux PDU en rack, chacune comprenant huit groupes de sorties. Chaque groupe de sorties est constitué d'une seule sortie globale. Chaque groupe de sorties ❶ de la première PDU en rack est relié au groupe de sorties ❷ ayant le même emplacement sur la seconde PDU en rack. Un cordon d'alimentation d'un serveur à double alimentation ❸ est connecté à une sortie sur la première PDU en rack et l'autre cordon est connecté à la sortie correspondante sur la seconde PDU en rack, ce qui assure que la sortie des deux sources d'alimentation vers le serveur sera mise sous tension ou hors tension de manière synchronisée en réponse à une action de contrôle des sorties.



La configuration suivante montre trois ensembles de sorties synchronisées. Les sorties globales sont indiquées en noir. Les groupes de sorties sont encadrés par des rectangles rouges.

❶	Ces quatre groupes de sorties globaux synchronisent un total de 19 sorties.
❷	Ces deux groupes de sorties globaux synchronisent 6 sorties : 2 dans un groupe et 4 dans l'autre.
❸	Ce groupe de sorties local synchronise 3 sorties sur la même PDU en rack.



Vérification de l'installation et de la configuration de groupes de sorties globaux

Pour vous assurer que votre installation répond à la configuration requise pour des groupes de sorties et que les groupes de sorties sont correctement configurés, sélectionnez **Information** dans le menu de navigation gauche **Outlet Groups** (groupes de sorties) de l'interface Web pour afficher les groupes et leurs connexions :

- La section **Configured Outlet Groups** (Groupes de sorties configurés) affiche les éléments suivants :
  - Tous les groupes de sorties configurés sur la PDU en rack concernée.
  - Les sorties de chaque groupe classées par numéro de sortie.
  - Les groupes de sorties présents sur d'autres PDU en rack avec lesquelles un groupe de sorties global est synchronisé. Chaque PDU en rack est identifiée par son adresse IP et chaque sortie globale est affichée en gras.
- La section **Global Outlet Overview** (Présentation des sorties de groupe global) affiche les éléments suivants :
  - L'adresse IP de la PDU en rack actuelle.
  - L'adresse IP des PDU en rack comprenant des sorties globales disponibles pour être synchronisées avec des groupes de sorties sur d'autres PDU en rack.
  - Toutes les sorties globales configurées sur les PDU en rack, qu'elles soient ou non synchronisées avec des groupes de sorties sur la PDU en rack actuelle.

Paramètres de sortie pour les sorties et les groupes de sorties

Lancement d'une action de contrôle

Si vous appliquez une action de contrôle des sorties à des sorties ou des groupes de sorties, les délais suivants sont utilisés pour cette action :

- Pour une sortie individuelle (ne faisant pas partie d'un groupe de sorties), l'action utilise les délais et la durée de redémarrage configurés pour cette sortie.
- Pour un groupe de sorties global, l'action utilise les délais et la durée de redémarrage configurés pour la sortie globale.
- Pour un groupe de sorties local, l'action utilise les délais configurés pour la sortie du groupe dont le numéro est le plus petit.

Pour contrôler les sorties sur la PDU en rack :

1. Dans l'onglet **Device Manager** (Gestionnaire d'appareils), sélectionnez **Control** dans le menu de navigation gauche.
2. Cochez les cases de chaque sortie ou groupe de sorties à contrôler, ou cochez la case **All Outlets** (Toutes les sorties).
3. Sélectionnez une action de contrôle (**Control Action**) dans la liste et cliquez sur **Next >>** (Suivant). Dans la page de confirmation décrivant l'action, choisissez d'appliquer l'action ou de l'annuler.

Actions de contrôle possibles.

Option	Description
No Action (Aucune action, interface Web uniquement)	Ne rien faire.
On Immediate (Mise sous tension immédiate)	Mise sous tension des sorties sélectionnées.
On Delayed (Mise sous tension avec délai)	Mise sous tension de chaque sortie sélectionnée suivant son paramètre **Power On Delay** (Délai de mise sous tension).†
Off Immediate (Mise hors tension immédiate)	Mise hors tension des sorties sélectionnées.
Off Delayed (Mise hors tension avec délai)	Mise hors tension de chaque sortie sélectionnée selon son paramètre **Power Off Delay** (Délai de mise hors tension).†
Reboot Immediate (Redémarrage immédiat)	Mise hors tension de chaque sortie sélectionnée. Chacune de ces sorties est ensuite remise sous tension suivant son paramètre **Reboot Duration** (Durée de redémarrage).†
Reboot Delayed (Redémarrage avec délai)	Mise hors tension de chaque sortie sélectionnée suivant son paramètre **Power Off Delay** (Délai de mise hors tension). Attente jusqu'à ce que toutes les sorties soient hors tension (valeur **Reboot Duration** la plus haute) puis remise sous tension de chaque sortie suivant son paramètre **Power On Delay** (Délai de mise sous tension).†

† Si un groupe de sorties local est sélectionné, seuls sont utilisés les délais et la durée de redémarrage configurés de la sortie dont le numéro est le plus petit. Si un groupe de sorties global est sélectionné, seuls sont utilisés les délais et la durée de redémarrage configurés pour la sortie globale.

Option	Description
Cancel Pending Commands (Annuler les commandes en attente)	Annule toutes les commandes en attente pour les sorties sélectionnées et les maintient dans leur état actuel. **REMARQUE :** pour les groupes de sorties globaux, vous ne pouvez annuler une commande qu'à partir de l'interface du groupe de sorties maître. Cette action annule la commande pour le groupe de sorties maître et pour tous les groupes de sorties esclaves.
† Si un groupe de sorties local est sélectionné, seuls sont utilisés les délais et la durée de redémarrage configurés de la sortie dont le numéro est le plus petit. Si un groupe de sorties global est sélectionné, seuls sont utilisés les délais et la durée de redémarrage configurés pour la sortie globale.	

Configuration des paramètres et du nom de la sortie

Les paramètres suivants sont disponibles :

Paramètre	Description
Name (Nom)	Permet de définir le nom d'une ou de plusieurs sorties. Le nom s'affiche à côté du numéro de la sortie dans les écrans d'état.
External Link (Lien externe)	Permet de définir un lien HTTP ou HTTPS vers un site Web ou une adresse IP. • **http://www.dell.com** relie la sortie au site Web Dell. • **http://*adresse_ip_pdu*** (où ***adresse_ip_pdu*** est l'adresse IP de la PDU en rack) relie la sortie à l'interface Web de la PDU en rack ayant cette adresse IP, ce qui permet à d'autres utilisateurs de s'y connecter.
Power On Delay (Délai de mise sous tension)	Fixe le nombre de secondes pendant lesquelles la PDU en rack attend avant de mettre sous tension une sortie après qu'une commande est émise. **REMARQUE :** pour configurer une sortie hors tension en permanence, cochez la case **Never** (Jamais) à côté de **Power On Delay** (Délai de mise sous tension).
Power Off Delay (Délai de mise hors tension)	Fixe le nombre de secondes pendant lesquelles la PDU en rack attend avant de mettre hors tension une sortie après qu'une commande est émise. **REMARQUE :** pour configurer une sortie sous tension en permanence, cochez la case **Never** (Jamais) à côté de **Power Off Delay** (Délai de mise hors tension).
Reboot Duration (Durée de redémarrage)	Fixe le nombre de secondes pendant lesquelles une sortie reste hors tension avant de redémarrer.

Pour configurer les paramètres ou le nom des sorties, sélectionnez l'onglet **Device Manager** puis **Configuration** dans le menu de navigation gauche. Cliquez sur le bouton **Configure Multiple Outlets** (Configurer plusieurs sorties) dans la section **Outlet Configuration** (Configuration des sorties) ou cliquez sur le nom de la sortie.

- Configuration des paramètres de sortie pour plusieurs sorties :
  - Cochez les cases à côté des numéros des sorties que vous voulez modifier ou cochez la case **All Outlets** (Toutes les sorties).
  - Saisissez les valeurs **Name** (Nom) et **Link** (Lien) et cliquez sur le bouton **Apply** situé juste en dessous de la liste.
  - Saisissez les valeurs **Power On Delay** (Délai de mise sous tension), **Power Off Delay** (Délai de mise hors tension) ou **Reboot Duration** (Durée de redémarrage) et cliquez sur le bouton **Apply** situé juste en dessous de la liste.
- Configuration des paramètres de sortie pour une sortie unique :
  - Entrez les valeurs **Name** (Nom) et **Link** (Lien) et cliquez sur le bouton **Apply** situé juste en dessous de la liste.
  - Saisissez les valeurs **Power On Delay** (Délai de mise sous tension), **Power Off Delay** (Délai de mise hors tension) ou **Reboot Duration** (Durée de redémarrage) et cliquez sur le bouton **Apply** situé juste en dessous de la liste.

Planification des actions relatives aux sorties

Actions planifiables

Pour configurer les valeurs **Power On Delay** (Délai de mise sous tension), **Power Off Delay** (Délai de mise hors tension) et **Reboot Duration** (Durée de redémarrage) de chaque sortie, consultez Configuration des paramètres et du nom de la sortie. Bien que la planification des actions relatives aux sorties se fasse par l'intermédiaire de l'interface Web, vous pouvez fixer ces valeurs à l'aide de l'interface Web ou de l'interface par lignes de commande.

Pour pouvoir appliquer une action à un groupe de sorties, les groupes de sorties doivent être activés au début de l'action planifiée. Par exemple, si la mise hors tension avec délai (**Off Delayed**) est planifiée pour 16h00, le délai de mise hors tension (**Power Off Delay**) commence à 16h00. Même si vous activez les groupes de sorties pendant ce **délai de mise hors tension** avant que la mise hors tension des sorties soit planifiée, l'action s'appliquera uniquement à la sortie individuelle et non au groupe de sorties.

Pour les sorties sélectionnées, vous pouvez planifier le déclenchement des actions indiquées dans le tableau ci-dessous de différentes manières : quotidiennement, par intervalles de une, deux, quatre ou huit semaines, ou ponctuellement.

Option	Description
No action (Aucune action)	Ne rien faire.
On Immediate (Mise sous tension immédiate)	Mise sous tension des sorties sélectionnées.
On Delayed (Mise sous tension avec délai)	Mise sous tension de chaque sortie sélectionnée suivant son paramètre **Power On Delay** (Délai de mise sous tension).†
Off Immediate (Mise hors tension immédiate)	Mise hors tension des sorties sélectionnées.
Off Delayed (Mise hors tension avec délai)	Mise hors tension de chaque sortie sélectionnée selon son paramètre **Power Off Delay** (Délai de mise hors tension).†
Reboot Immediate (Redémarrage immédiat)	Mise hors tension de chaque sortie sélectionnée. Chacune de ces sorties est ensuite remise sous tension suivant son paramètre **Reboot Duration** (Durée de redémarrage).†
Reboot Delayed (Redémarrage avec délai)	Mise hors tension de chaque sortie sélectionnée suivant son paramètre **Power Off Delay** (Délai de mise hors tension). Attente jusqu'à ce que toutes les sorties soient hors tension (valeur **Reboot Duration** la plus haute) puis remise sous tension de chaque sortie suivant son paramètre **Power On Delay** (Délai de mise sous tension).†

† Si un groupe de sorties local est sélectionné, seuls sont utilisés les délais et la durée de redémarrage configurés de la sortie dont le numéro est le plus petit. Si un groupe de sorties global est sélectionné, seuls sont utilisés les délais et la durée de redémarrage configurés pour la sortie globale.

Planification d'un événement relatif aux sorties

1. Dans l'interface Web, sélectionnez l'onglet **Device Manager** puis **Scheduling** (Planification) dans le menu de navigation gauche.
2. Dans la page **Outlet Scheduling** (Planification des sorties), sélectionnez la fréquence de déclenchement de l'événement : **One-Time** (Ponctuel), **Daily** (Quotidien) ou **Weekly** (Hebdomadaire), puis cliquez sur le bouton **Next** (Suivant).

   Si vous sélectionnez **Weekly** (Hebdomadaire), vous pouvez planifier l'événement pour qu'il se déclenche une fois par semaine, ou une fois toutes les deux, quatre ou huit semaines.

3. Dans la page **Schedule a Daily Action** (Planifier une action quotidienne), dans la zone de texte **Name of event** (Nom de l'événement), remplacez le nom par défaut `Outlet Event` par un nom qui identifie le nouvel événement.
4. Utilisez les listes déroulantes pour sélectionner le type d'événement et le moment auquel il va se déclencher.

   Le format de date pour les événements ponctuels est *mm*/*jj*, le format de l'heure pour tous les événements est *hh*/*mm*, les heures à deux chiffres étant affichées au format 24 heures.

   - Un événement planifié quotidiennement ou à l'un des intervalles disponibles dans la sélection **Weekly** (Hebdomadaire) continue de survenir selon l'intervalle prévu jusqu'à ce que cet événement soit supprimé ou désactivé.
   - Un événement ponctuel ne peut survenir que dans les douze mois suivant la date à laquelle la planification est effectuée. Par exemple, le 26 décembre 2010, un événement ponctuel peut être planifié pour survenir à une date comprise entre cette date et le 26 décembre 2011.

5. Utilisez les cases à cocher pour sélectionner les sorties concernées par l'action. Vous pouvez sélectionner une ou plusieurs sorties individuelles ou bien **All Outlets** (Toutes les sorties).
6. Cliquez sur **Apply** pour confirmer la planification de l'événement, ou sur **Cancel** (Annuler) pour l'effacer.

Lorsque l'événement est confirmé, la page récapitulative s'affiche de nouveau, le nouvel événement apparaissant dans la liste des événements planifiés.

Modification, désactivation, activation ou suppression d'un événement de sortie planifié

1. Dans l'interface Web, sélectionnez l'onglet **Device Manager** puis **Scheduling** (Planification) dans le menu de navigation gauche.
2. Dans la liste des événements de la section **Scheduled Outlet Action** (Action de sortie planifiée) de la page **Scheduling** (Planification), cliquez sur le nom de l'événement.
3. Dans la page **Daily/Weekly scheduled action detail** (Détails de l'action quotidienne/hebdomadaire planifiée), vous pouvez effectuer les opérations suivantes :

– Modifier les détails de l'événement, par exemple son nom, sa date d'exécution planifiée et les sorties concernées.

– Sous **Status of event** (État de l'événement) en haut de la page, vous pouvez effectuer les tâches suivantes :

  • Désactiver l'événement en conservant les détails configurés pour pouvoir le réactiver ultérieurement. Un événement désactivé ne surviendra pas. Lorsqu'il est créé, un événement est activé par défaut.

  • Activer un événement s'il avait été désactivé par l'option **Disable**.

  • Supprimer l'événement pour le faire disparaître complètement du système. Un événement supprimé ne peut plus être récupéré.

4. Lorsque les modifications sont terminées dans cette page, cliquez sur **Apply** pour les confirmer ou sur **Cancel** pour annuler l'opération.

Menu Outlet Manager (Gestionnaire des sorties)

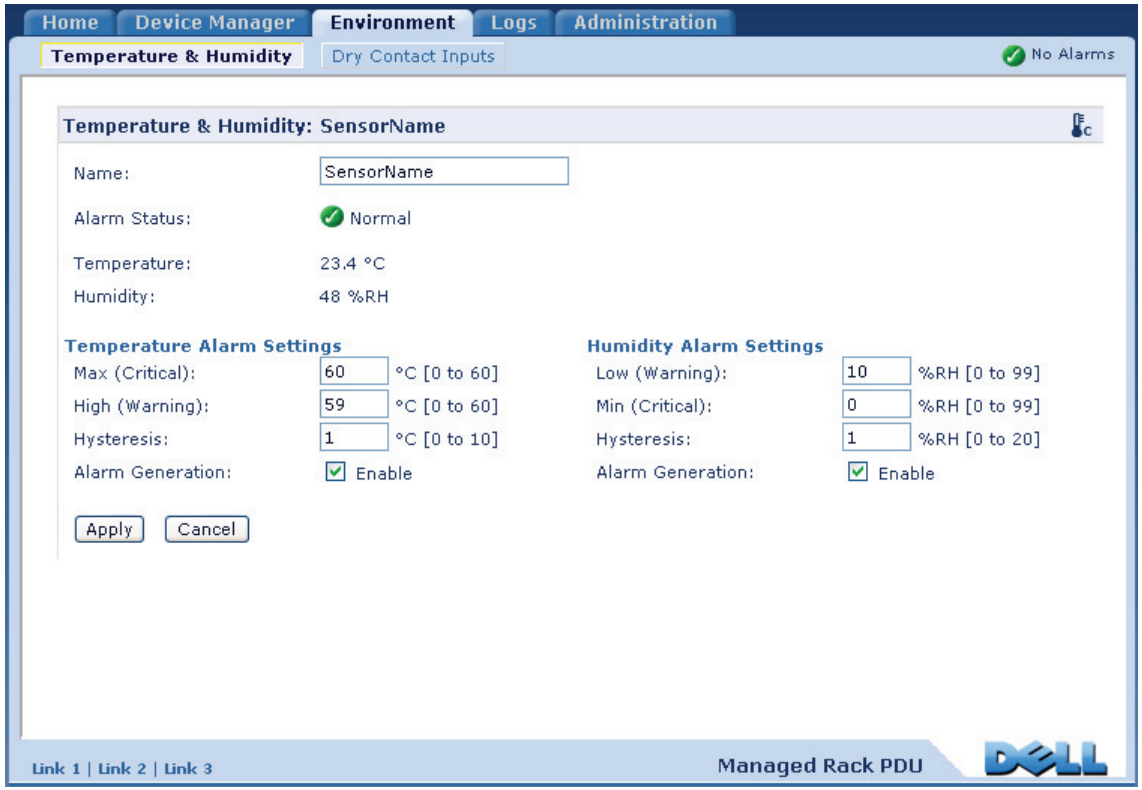
Ce menu permet de configurer les comptes d'utilisateurs de sorties. Des sorties individuelles peuvent être attribuées à un utilisateur disposant d'un compte Utilisateur de sorties. Un compte Utilisateur de sorties permet de contrôler uniquement les sorties attribuées. Seules les personnes disposant des droits Administrateur peuvent configurer les sorties. Le Gestionnaire d'appareils dispose de droits limités de configuration des sorties.

Configuration d'un utilisateur de sorties

1. Dans l'interface Web, sélectionnez l'onglet **Device Manager** puis **Outlet Manager** (Gestionnaire des sorties) dans le menu de navigation gauche.
2. Cliquez sur le bouton **Add New User** (Ajouter un utilisateur).
3. Renseignez les informations relatives aux options ci-dessous et cliquez sur **Apply** pour confirmer les modifications.

Option	Description
User Name (Nom d'utilisateur)	Permet de définir le nom de l'utilisateur de sorties. L'option « New User » (Nouvel utilisateur) est réservée et n'est pas accessible. **REMARQUE :** un nom d'utilisateur affiché en orange indique que le compte utilisateur a été désactivé.
Password (Mot de passe)	Permet de définir le mot de passe de l'utilisateur de sorties.
User Description (Description de l'utilisateur)	Permet de définir l'identification/la description de l'utilisateur de sorties.
Account Status (État du compte)	Permet d'activer, de désactiver ou de supprimer le compte d'un utilisateur de sorties.
Device outlet access (Accès aux sorties d'appareils)	Permet de sélectionner les sorties auxquelles l'utilisateur peut accéder.

Environnement



Configuration des capteurs de température et d'humidité

Chemin d'accès : Environment > Temperature & Humidity

Dans la page **Temperature & Humidity**, lorsqu'un capteur de température ou de température et d'humidité est connecté à la PDU à monter en rack, vous pouvez fixer les seuils de déclenchement des alarmes d'avertissement et des alarmes critiques (voir Icônes d'état de l'appareil pour plus de détails sur chaque type d'alarme).

Pour la température :

- Si le seuil de température élevée est atteint, le système génère une alarme d'avertissement.
- Si le seuil de température maximum est atteint, le système génère une alarme critique.

De même pour l'humidité :

- Si le seuil d'humidité basse est atteint, le système génère une alarme d'avertissement.
- Si le seuil d'humidité minimum est atteint, le système génère une alarme critique.

Cliquez sur le symbole du thermomètre dans le coin supérieur droit pour basculer entre Fahrenheit et Celsius.

Pour configurer les capteurs de température et d'humidité :

1. Entrez les valeurs des seuils minimum, maximum, haut et bas.
2. Entrez les valeurs d'**hystérésis** (voir Hystérésis pour plus de détails).
3. Activez le déclenchement d'alarmes comme vous le souhaitez.
4. Cliquez sur **Apply**.

Hystérésis. Cette valeur spécifie à quel niveau la température ou l'humidité doit revenir par rapport à un seuil pour arrêter son alarme de dépassement.

- Pour les seuils de température maximum et haute, le niveau à atteindre pour arrêter l'alarme est égal au seuil moins l'hystérésis.
- Pour les seuils d'humidité minimum et basse, le niveau à atteindre pour arrêter l'alarme est égal au seuil plus l'hystérésis.

Si la température ou l'humidité qui a dépassé un seuil a ensuite tendance à de légères variations, augmentez la valeur d'hystérésis pour éviter de multiples alarmes. Si la valeur d'hystérésis est trop basse, de telles variations peuvent provoquer puis arrêter des dépassements de seuil à répétition.

Exemple de montée de température suivie de variations : le seuil de température maximum est 85° F et l'hystérésis de la température est 3° F. La température monte au-dessus de 85 F, et franchit donc ce seuil. Ensuite la température redescend à 84° F puis remonte à 86° F plusieurs fois, mais cela ne provoque aucun événement d'arrêt de l'alarme ni de nouveau dépassement. Pour arrêter l'alarme de dépassement en cours, il faudrait que la température chute jusqu'à 82°F (soit 3°F en dessous du seuil).

Exemple de chute d'humidité suivie de variations : le seuil d'humidité minimum est 18 % et l'hystérésis d'humidité 8 %. L'humidité chute au-dessous de 18 % et dépasse donc son seuil. Ensuite elle monte à 24 % puis redescend à 13 % plusieurs fois, mais cela ne provoque aucun événement d'arrêt de l'alarme ni de nouveau dépassement. Pour arrêter l'alarme de dépassement en cours, il faudrait que l'humidité monte au-delà de 26 % (soit 8 % au-dessus du seuil).

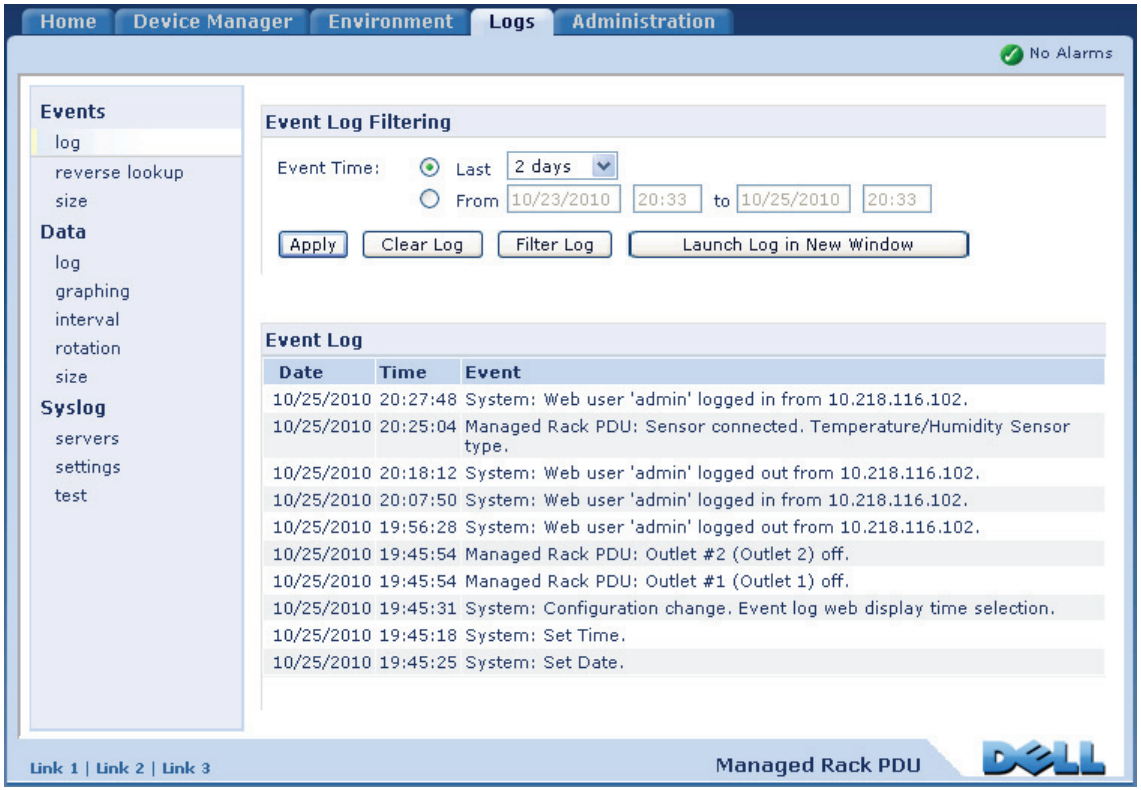
Configuration des entrées à contact sec

Chemin d'accès : Environment > Dry Contact Inputs

La page **Dry Contact Inputs** permet de consulter l'état actuel des contacts secs et de les configurer.

Paramètre	Description
Nom	Nom du contact en entrée. *Maximum* : 20 caractères.
État de l'alarme	**Normal** si le contact en entrée ne signale pas d'alarme, ou bien la gravité de l'alarme s'il signale une alarme.
État	État actuel du contact en entrée : **Closed (Fermé)** ou **Open (Ouvert)**.
Déclenchement d'alarme	Permet d'activer ou de désactiver le contact en entrée. S'il est désactivé, un contact ne génère aucune alarme même si sa position est anormale.
État normal	État normal (sans alarme) du contact en entrée : **Closed (Fermé)** ou **Open (Ouvert)**.

Journaux de consignation



Utilisation des journaux de consignation des événements et des données

Journal de consignation des événements

Chemin d'accès : Logs > Events > *options*

Vous pouvez consulter, filtrer ou supprimer le journal de consignation des événements. Par défaut, le journal affiche tous les événements enregistrés pendant les deux derniers jours, en ordre chronologique inverse.

Pour consulter les listes de tous les événements configurables ainsi que leur configuration actuelle, sélectionnez l'onglet **Administration**, **Notification** dans la barre de menus supérieure puis **by event** (par événement) sous **Event Actions** (Actions sur les événements) dans le menu de navigation gauche.

Voir Configuration par événement.

Affichage du journal de consignation des événements (Logs > Events > log) :

- Par défaut, le journal de consignation des événements s'affiche en page de l'interface Web. L'événement le plus récent est enregistré en page 1. Dans la barre de navigation au-dessous du journal :
  - Cliquez sur un numéro de page pour ouvrir une page spécifique du journal.
  - Cliquez sur **Previous** (Précédent) ou **Next** (Suivant) pour consulter les événements enregistrés immédiatement avant ou après ceux répertoriés dans la page ouverte.
  - Cliquez sur **<<** pour revenir à la première page ou sur **>>** pour afficher la dernière page du journal.

- Pour consulter les événements répertoriés dans une page, cliquez sur **Launch Log in New Window** (Ouvrir le journal dans une nouvelle fenêtre) dans la page du journal de consignation des événements pour afficher une vue en plein écran du journal.

Dans les options de votre navigateur, JavaScript® doit être activé pour pouvoir utiliser le bouton **Launch Log in New Window**.

Vous pouvez également utiliser les protocoles FTP ou Secure CoPy (SCP) pour consulter le journal de consignation des événements. Voir Utilisation du protocole FTP ou SCP pour récupérer les fichiers de journaux de consignation.

Filtrage du journal de consignation (Logs > Events > log) :

- **Filtrage du journal par date ou heure :** pour afficher la totalité du journal de consignation des événements ou pour modifier le nombre de jours ou de semaines pour lesquels le journal affiche les événements les plus récents, sélectionnez **Last** (Dernier). Sélectionnez un intervalle de temps dans le menu déroulant, puis cliquez sur **Apply** (Appliquer). La configuration du filtre est sauvegardée jusqu'à ce que la PDU en rack redémarre.
  Pour afficher les événements consignés pendant un intervalle de temps spécifique, sélectionnez **From** (Depuis). Spécifiez les heures (au format 24 heures) et les dates de début et de fin d'affichage des événements, puis cliquez sur **Apply**. La configuration du filtre est sauvegardée jusqu'à ce que la PDU en rack redémarre.
- **Filtrage du journal par événement** : pour spécifier les événements à afficher dans le journal, cliquez sur **Filter Log** (Filtrer le journal de consignation). Décochez la case d'option d'une catégorie d'événement ou d'un niveau de gravité d'une alarme pour les supprimer de l'affichage. Le texte dans le coin supérieur droit de la page du journal de consignation des événements indique si un filtre est actif.
  Si vous êtes connecté en tant qu'Administrateur, cliquez sur **Save As Default** (Enregistrer comme filtre par défaut) pour enregistrer ce filtre comme affichage du journal par défaut pour tous les utilisateurs. Si vous ne cliquez pas sur **Save As**

Default, le filtre reste actif jusqu'à ce que la PDU en rack redémarre.
Pour retirer un filtre actif, cliquez sur **Filter Log** puis sur **Clear Filter (Show All)** (Supprimer le filtre (Afficher tout)).

Les événements sont traités par le filtre en utilisant la logique **OU**.

- Les événements que vous ne sélectionnez pas dans la liste **Filter By Severity** (Filtrer par gravité) ne s'affichent jamais dans le journal de consignation des événements filtré, même si l'événement survient dans une catégorie sélectionnée dans la liste **Filter by Category** (Filtrer par catégorie).
- Les événements que vous ne sélectionnez pas dans la liste **Filter by Category** ne s'affichent jamais dans le journal de consignation des événements filtré, même si les périphériques de la catégorie concernée entrent dans une situation d'alarme sélectionnée dans la liste **Filter by Severity**.

Suppression du journal de consignation (Logs > Events > log) :

Pour supprimer tous les événements enregistrés dans le journal de consignation, cliquez sur le bouton **Clear Log** (Effacer le journal de consignation) de la page Web qui contient ce journal. Les événements supprimés ne peuvent plus être récupérés.

Pour désactiver la consignation des événements selon le niveau de gravité qui leur est attribué ou leur catégorie d'événements, consultez Configuration par événement.

Configuration de la recherche inversée (Logs > Events > reverse lookup) :

La recherche inversée est désactivée par défaut. Activez cette fonction sauf si vous n'avez aucun serveur DNS configuré ou si les performances de votre réseau sont faibles en raison d'un trafic important.

Lorsque la recherche inversée est activée et qu'un événement lié au réseau survient, l'adresse IP et le nom de domaine du périphérique réseau associé à l'événement sont consignés dans le journal de consignation des événements. Si aucun nom de domaine n'existe pour ce périphérique, seule son adresse IP est consignée avec l'événement. Comme les noms de domaines changent généralement moins souvent que les adresses IP, l'activation de la recherche inversée peut améliorer les possibilités d'identifier les adresses des périphériques réseau à l'origine des événements.

Modification de la taille du journal de consignation des événements (Logs > Events > size) :

Par défaut, le journal de consignation des événements conserve 400 événements. Vous pouvez modifier ce nombre. Lorsque vous modifiez la taille du journal de consignation des événements, toutes les entrées qu'il contient sont supprimées. Pour éviter toute perte de données du journal de consignation, utilisez le protocole FTP ou SCP pour récupérer le journal avant d'entrer une nouvelle valeur dans le champ **Event Log Size** (Taille du journal de consignation des événements).

Voir Utilisation du protocole FTP ou SCP pour récupérer les fichiers de journaux de consignation.

Lorsque le journal de consignation est plein, les entrées les plus anciennes sont supprimées.

Journal de consignation des données

Chemin d'accès : Logs > Data > *options*

Le journal de consignation des données enregistre le courant et la puissance de l'appareil et de ses phases (pour une PDU en rack triphasée, le cas échéant), ainsi que les données de température, d'humidité et de contacts secs selon l'intervalle de temps spécifié. Chaque entrée est répertoriée selon la date et l'heure auxquelles les données ont été enregistrées.

Affichage du journal de consignation des données (Logs > Data > log) :

- Par défaut, le journal de consignation des données s'affiche en page de l'interface Web. L'élément de données le plus récent est enregistré en page 1. Dans la barre de navigation au-dessous du journal :
  - Cliquez sur un numéro de page pour ouvrir une page spécifique du journal.
  - Cliquez sur **Previous** ou **Next** pour consulter les données enregistrées immédiatement avant ou après celles répertoriées dans la page ouverte.
  - Cliquez sur **<<** pour revenir à la première page du journal ou sur **>>** pour afficher la dernière page du journal.
- Pour consulter les données répertoriées dans une page, cliquez sur **Launch Log in New Window** (Ouvrir le journal dans une nouvelle fenêtre) dans la page du journal de consignation des données pour afficher une vue en plein écran du journal.

Dans les options de votre navigateur, JavaScript doit être activé pour pouvoir utiliser le bouton **Launch Log in New Window**.

Vous pouvez également utiliser les protocoles FTP ou SCP pour consulter le journal de consignation des données. Voir Utilisation du protocole FTP ou SCP pour récupérer les fichiers de journaux de consignation.

Filtrage du journal par date ou heure (Logs > Data > log) :

pour afficher la totalité du journal de consignation des données ou pour modifier le nombre de jours ou de semaines pour lesquels le journal affiche les événements les plus récents, sélectionnez **Last** (Dernier). Sélectionnez un intervalle de temps dans le menu déroulant, puis cliquez sur **Apply** (Appliquer). La configuration du filtre est sauvegardée jusqu'à ce que l'appareil redémarre.

Pour afficher les données consignées pendant un intervalle de temps spécifique, sélectionnez **From** (Depuis). Spécifiez les heures (au format 24 heures) et les dates de début et de fin d'affichage des données, puis cliquez sur **Apply** (Appliquer). La configuration du filtre est sauvegardée jusqu'à ce que l'appareil redémarre.

Suppression du journal de consignation des données :

Pour supprimer toutes les données enregistrées dans le journal de consignation, cliquez sur **Clear Data Log** (Effacer le journal de consignation des données) dans la page Web qui contient ce journal. Les données supprimées ne peuvent plus être récupérées.

Définition de la fréquence de collecte des données (Logs > Data > interval) :

Le paramètre **Log Interval** (Fréquence de consignation) permet de définir la fréquence d'échantillonnage et d'enregistrement des données dans le journal de consignation des données, et de consulter le calcul du nombre de jours de données que le journal de consignation peut enregistrer en fonction de l'intervalle choisi. Lorsque le journal de consignation est plein, les entrées les plus anciennes sont supprimées. Pour éviter la suppression automatique des données les plus anciennes, activez et configurez la rotation du journal de consignation des données, décrite dans la section suivante.

Configuration de la rotation du journal de consignation des données (Logs > Data > rotation) :

Permet de définir un dépôt du journal de consignation des données protégé par mot de passe sur un serveur FTP spécifié. Lorsque la rotation est activée, le contenu du journal de consignation des données est ajouté au fichier spécifié par nom et par emplacement. Ce fichier est mis à jour selon l'intervalle de téléchargement spécifié.

Paramètre	Description
Data Log Rotation (Rotation des journaux de consignation des données)	Activation ou désactivation (par défaut) de la rotation du journal de consignation des données.
FTP Server Address (Adresse du serveur FTP)	Emplacement du serveur FTP où le dépôt de données est enregistré.
User Name (Nom d'utilisateur)	Nom d'utilisateur requis pour envoyer les données au fichier de dépôt. Cet utilisateur doit aussi être configuré avec autorisation d'accès en lecture et en écriture au fichier de dépôt des données et au répertoire (dossier) dans lequel il est enregistré.
Password (Mot de passe)	Mot de passe requis pour envoyer les données au fichier de dépôt.
File Path (Chemin d'accès du fichier)	Chemin d'accès au fichier de dépôt.
Filename (Nom de fichier)	Nom du fichier de dépôt (fichier texte ASCII).
Delay *X* hours between uploads (Délai de *X* heures entre les téléchargements)	Nombre d'heures entre les téléchargements de données dans le fichier.

Paramètre	Description
Upload every *X* minutes (En cas d'échec, retenter le téléchargement toutes les *X* minutes)	Nombre de minutes entre chaque tentative de téléchargement de données dans le fichier après un échec du téléchargement.
Up to *X* times (Jusqu'à *X* fois)	Nombre maximum de tentatives de téléchargement après un échec initial.
Until Upload Succeeds (Jusqu'au succès du téléchargement)	Tentatives de téléchargement du fichier jusqu'à ce que le transfert soit terminé.

Pour modifier la taille le journal de consignation des données (Logs > Data > size) :

Par défaut, le journal de consignation des données conserve 1000 enregistrements. Vous pouvez modifier ce nombre. Lorsque vous modifiez la taille du journal de consignation des données, toutes les entrées qu'il contient sont supprimées. Pour éviter toute perte d'enregistrements, utilisez le protocole FTP ou SCP pour récupérer le journal avant d'entrer une nouvelle valeur dans le champ **Data Log Size** (Taille du journal de consignation des données).

Voir Utilisation du protocole FTP ou SCP pour récupérer les fichiers de journaux de consignation.

Lorsque le journal de consignation est plein, les entrées les plus anciennes sont supprimées.

Utilisation du protocole FTP ou SCP pour récupérer les fichiers de journaux de consignation

Le niveau Administrateur ou Utilisateur de périphérique permet d'utiliser FTP ou SCP pour récupérer un journal de consignation des événements (*event.txt*) ou des données (*data.txt*) au format texte séparé par des tabulations, qui peut être importé dans un tableur.

- Le fichier contient tous les événements ou toutes les données enregistrés depuis la dernière suppression du contenu du journal de consignation ; dans le cas du journal de consignation des données, celui-ci peut avoir été tronqué s'il avait atteint sa taille maximale.
- Le fichier contient des informations que le journal de consignation des événements ou des données n'affiche pas.
  - Version du format de fichier (premier champ)
  - Date et heure auxquelles le fichier a été récupéré
  - Valeurs de **Nom**, **Contact** et **Emplacement**, et adresse IP de la PDU en rack.
  - **Code d'événement** propre à chaque événement consigné (fichier *event.txt* uniquement).

La PDU en rack utilise une numérotation à quatre chiffres pour indiquer l'année des entrées du journal de consignation. Vous devrez peut-être sélectionner un format de date à quatre chiffres dans votre tableur pour afficher les quatre chiffres.

Si vous utilisez les protocoles de sécurité codés sur votre système, utilisez Secure CoPy (SCP) pour récupérer le journal de consignation.
Si vous utilisez des méthodes d'authentification non codées pour la sécurité de votre système, utilisez FTP pour récupérer le journal de consignation.

Voir Annexe B : Guide de sécurité pour des informations sur les protocoles et méthodes disponibles pour configurer le type de sécurité requis.

Utilisation du protocole SCP pour récupérer les fichiers. Pour utiliser SCP afin de récupérer le fichier *event.txt*, utilisez la commande suivante :

```
scp nom_d'utilisateur@nom_d'hôte_ou_adresse_ip:
event.txt ./event.txt
```

Pour utiliser SCP afin de récupérer le fichier *data.txt*, utilisez la commande suivante :

```
scp nom_d'utilisateur@nom_d'hôte_ou_adresse_ip:
data.txt ./data.txt
```

Utilisation du protocole FTP pour récupérer les fichiers. Pour utiliser FTP afin de récupérer le fichier *event.txt* ou *data.txt* :

1. À l'invite de commande, entrez **ftp**, puis l'adresse IP de la PDU en rack et appuyez sur ENTRÉE.

   Si le paramètre **Port** de l'option **FTP Server (Serveur FTP)** (configurée dans le menu **Network (Réseau)** de l'onglet **Administration**) n'est plus configuré sur la valeur par défaut (**21**), vous devez utiliser la valeur qui lui a été attribuée au niveau de la commande FTP. Pour les clients FTP sous Windows, utilisez la commande suivante (espaces inclus) : (avec certains clients FTP, insérez deux points (:) en remplacement d'un espace entre l'adresse IP et le numéro de port).

   ```
   ftp>open adresse_ip numéro_de_port
   ```

   Pour définir un port autre que le port par défaut afin d'augmenter la sécurité du serveur FTP, consultez Serveur FTP. Vous pouvez spécifier un port compris entre 5001 et 32768.

2. Utilisez le **nom d'utilisateur** et le **mot de passe** sensibles à la casse pour vous connecter comme Administrateur ou Utilisateur de périphérique. Pour le niveau Administrateur, le **mot de passe** et le **nom d'utilisateur** par défaut sont **admin**. Pour le niveau Utilisateur de périphérique, les valeurs par défaut sont **device** comme **nom d'utilisateur** et comme **mot de passe**.

3. Utilisez la commande **get** pour transmettre la version texte du journal de consignation sur votre disque local.

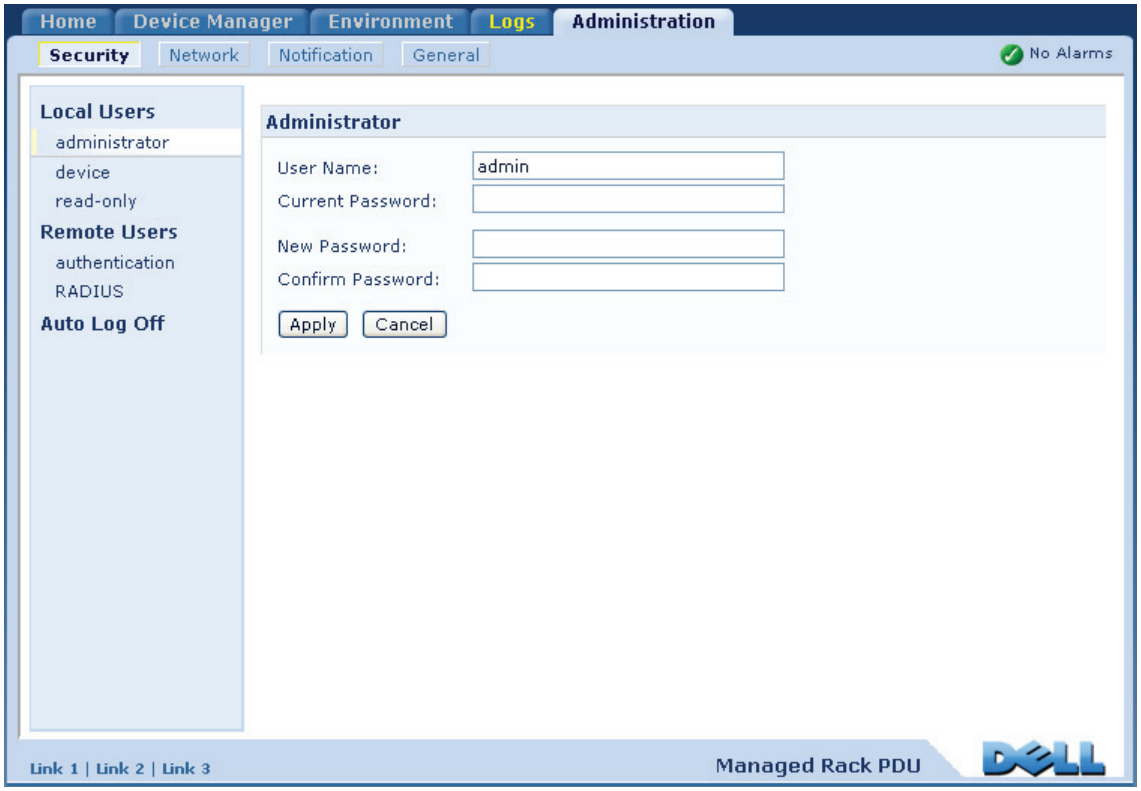
   `ftp>get event.txt`

   ou

   `ftp>get data.txt`

4. Entrez **`quit`** à l'invite **`ftp>`** pour quitter FTP.

Administration : Sécurité



Utilisateurs locaux

Configuration de l'accès utilisateur

Chemin d'accès : Administration > Security > Local Users > *options*

Le compte utilisateur Administrateur a toujours accès à la PDU en rack.

Les comptes Utilisateur de périphérique et Utilisateur en lecture seule sont activés par défaut. Pour désactiver les comptes Utilisateur de périphérique ou Utilisateur en lecture seule, sélectionnez le compte utilisateur dans le menu de navigation gauche, puis décochez la case **Activer**.

Définir le nom d'utilisateur et le mot de passe (sensibles à la casse) pour chaque type de compte se fait de la même manière. La longueur maximum d'un nom d'utilisateur est de 64 caractères, celle du mot de passe de 64 caractères. Un mot de passe vierge (aucun caractère) n'est pas autorisé.

Pour plus d'informations sur les autorisations accordées à chaque type de compte, consultez Types de comptes utilisateurs.

Pour les comptes Utilisateur de sorties, il n'existe pas de nom d'utilisateur ni de mot de passe par défaut. Un administrateur doit définir le nom d'utilisateur, le mot de passe et les autres caractéristiques du compte d'un utilisateur de sorties. Voir Configuration d'un utilisateur de sorties.

Type de compte	Nom d'utilisateur par défaut	Mot de passe par défaut	Accès autorisé
Administrateur	admin	admin	Interface Web et interface par lignes de commande
Utilisateur de périphérique	device	device	
Utilisateur en lecture seule	readonly	readonly	Interface Web uniquement

Utilisateurs distants

Authentification

Chemin d'accès : Administration > Security > Remote Users > Authentication Method

Cette option permet de sélectionner le mode de gestion de l'accès à distance à la PDU en rack.

Pour des informations sur l'authentification locale (sans utiliser l'authentification centralisée d'un serveur RADIUS), consultez Annexe B : Guide de sécurité.

La PDU en rack accepte les fonctions d'authentification et d'autorisation RADIUS (Remote Authentication Dial-In User Service).

- Lorsqu'un utilisateur accède à la PDU en rack ou à tout autre périphérique réseau sur lequel RADIUS est activé, une demande d'authentification est envoyée au serveur RADIUS pour déterminer le niveau d'autorisation de l'utilisateur.
- Les noms d'utilisateurs RADIUS utilisés avec la PDU en rack sont limités à 32 caractères.

Sélectionnez l'une des options suivantes :

- **Local Authentication Only** (Authentification locale uniquement) : RADIUS est désactivé. L'authentification locale est activée.
- **RADIUS, then Local Authentication** (Authentification RADIUS, puis locale) : les authentifications RADIUS et locale sont activées. La première authentification demandée est celle du serveur RADIUS. Si le serveur RADIUS ne répond pas, l'authentification locale est utilisée.

- **RADIUS Only** (RADIUS uniquement) : RADIUS est activé. L'authentification locale est désactivée.

Si **RADIUS Only** est sélectionné, et si le serveur RADIUS n'est pas disponible, s'il est incorrectement identifié ou incorrectement configuré, l'accès à distance est indisponible pour tous les utilisateurs. Vous devez vous connecter à l'interface par lignes de commande à l'aide d'une connexion série et modifier le paramètre **access** en lui donnant la valeur **local** ou **radiusLocal** pour rétablir l'accès. Par exemple, la commande pour modifier le paramètre d'accès sur **local** serait :

```
radius -a local
```

RADIUS

Chemin d'accès : Administration > Security > Remote Users > RADIUS

Cette option permet d'effectuer les actions suivantes :

- Répertorier les serveurs RADIUS (deux au maximum) disponibles pour la PDU en rack ainsi que leur délai de réponse.
- Cliquer sur un lien et configurer les paramètres pour une authentification par un nouveau serveur RADIUS.
- Cliquer sur un serveur RADIUS répertorié pour afficher et modifier ses paramètres.

Paramètre RADIUS	Définition
RADIUS Server (Serveur RADIUS)	Nom ou adresse IP du serveur RADIUS (IPv4 ou IPv6). Cliquez sur un lien pour configurer le serveur. **REMARQUE :** les serveurs RADIUS utilisent le port 1812 par défaut pour authentifier les utilisateurs. Pour utiliser un port différent, ajoutez le signe deux points, suivi du nouveau numéro de port, à la suite du nom ou de l'adresse IP du serveur RADIUS.
Secret	Secret partagé entre le serveur RADIUS et la PDU en rack.
Timeout (Délai de réponse)	Durée en secondes pendant laquelle la PDU en rack attend une réponse du serveur RADIUS.
Test Settings (Paramètres de test)	Entrez le nom d'utilisateur et le mot de passe Administrateur pour tester le chemin d'accès du serveur RADIUS que vous avez configuré.
Skip Test and Apply (Ignorer le test et appliquer)	Ne pas tester le chemin d'accès du serveur RADIUS.

Configuration du serveur RADIUS

Récapitulatif de la procédure de configuration

Vous devez configurer votre serveur RADIUS afin qu'il fonctionne avec la PDU en rack.

Pour des exemples de fichier des utilisateurs RADIUS disposant d'attributs fournisseur (Vendor Specific Attributes, VSA) et un exemple d'entrée dans le fichier dictionnaire sur le serveur RADIUS, consultez Annexe B : Guide de sécurité.

1. Ajoutez l'adresse IP de la PDU en rack à la liste des clients du serveur RADIUS (fichier).
2. Les utilisateurs doivent disposer d'attributions Service-Type sauf si des VSA (Vendor Specific Attributes) sont définis. Si aucune attribution Service-Type n'est configurée, les utilisateurs ne disposent que de l'accès en lecture seule (uniquement sur l'interface Web).

   Consultez votre documentation relative au serveur RADIUS pour des informations sur le fichier des utilisateurs RADIUS, et le Annexe B : Guide de sécurité pour voir un exemple.

3. Les VSA peuvent être utilisés au lieu des attributs Service-Type fournies par le serveur RADIUS. Les VSA nécessitent une entrée de dictionnaire et un fichier d'utilisateurs RADIUS. Dans le fichier de dictionnaire, définissez les noms des mots-clés ATTRIBUTE et VALUE, mais pas des valeurs numériques. Si vous modifiez les valeurs numériques, l'authentification et l'autorisation RADIUS vont échouer. Les VSA ont priorité sur les attributions RADIUS standard.

Configuration d'un serveur RADIUS sous UNIX® avec des mots de passe fantômes

Si des fichiers de mots de passe fantômes UNIX sont utilisés (/etc/passwd) avec les fichiers de dictionnaire RADIUS, vous pouvez utiliser les deux méthodes suivantes pour authentifier les utilisateurs :

- Si tous les utilisateurs UNIX disposent de privilèges administratifs, ajoutez les informations suivantes au fichier « user » RADIUS. Pour autoriser uniquement les comptes Utilisateur de périphérique, modifiez le paramètre DELL-Service-Type sur **`Device`**.

```
DEFAULT      Auth-Type = System
             DELL-Service-Type = Admin
```

- Ajoutez les noms d'utilisateurs et les attributs au fichier « user » RADIUS et confirmez le mot de passe par rapport à /etc/passwd. L'exemple suivant concerne les utilisateurs **`bconners`** et **`thawk`** :

```
bconners     Auth-Type = System
             DELL-Service-Type = Admin
thawk        Auth-Type = System
             DELL-Service-Type = Device
```

Serveurs RADIUS pris en charge

FreeRADIUS et Microsoft IAS 2003 sont pris en charge. Il est possible que d'autres applications RADIUS couramment utilisées conviennent, mais celles-ci n'ont pas été soumises à des tests complets.

Délai d'inactivité

Chemin d'accès : Administration > Security > Auto Log Off

Utilisez cette option pour configurer la durée d'attente (3 minutes par défaut) du système avant la déconnexion d'un utilisateur inactif. Si vous modifiez cette valeur, vous devez vous déconnecter pour que la modification prenne effet.

Cette minuterie continue si un utilisateur ferme la fenêtre du navigateur sans se déconnecter préalablement en cliquant sur **Log Off (Déconnexion)** dans le coin supérieur droit. Cet utilisateur étant toujours considéré comme connecté, aucun utilisateur ne peut se connecter avant l'expiration du délai spécifié en **Minutes of Inactivity (Minutes d'inactivité).** Par exemple, lorsque le paramètre **Minutes of Inactivity** a sa valeur par défaut, si un utilisateur ferme la fenêtre du navigateur sans se déconnecter, aucun utilisateur ne peut se connecter avant 3 minutes.

Administration : Notification

Actions sur les événements

Chemin d'accès : Administration > Notification > Event Actions > *options*

Types de notification

Vous pouvez configurer des actions sur les événements en réaction à un événement ou un groupe d'événements. Ces actions envoient une notification aux utilisateurs de différentes manières :

- Notification active et automatique. Les utilisateurs ou les services de surveillance spécifiés sont contactés directement.
  - Notification par e-mail
  - Traps SNMP
  - Notification Syslog
- Notification indirecte
  - Journal de consignation des événements. Si aucune notification directe n'est configurée, les utilisateurs doivent consulter le journal de consignation des événements pour savoir lesquels se sont produits.

    Vous pouvez aussi consigner au journal les données de performances à utiliser pour la surveillance du périphérique. Voir Journal de consignation des données pour obtenir des informations sur la configuration et l'utilisation de cette option de consignation des données.
  - Requêtes (SNTP et GET)

    Pour plus d'informations, consultez SNMP. Le protocole SNMP permet à un NMS d'exécuter des requêtes d'information. En SNMPv1, qui ne crypte pas les données avant la transmission, configurer le type d'accès SNMP le plus restreint (en lecture) permet d'utiliser des requêtes d'information sans risque d'autoriser des modifications de configuration à distance.

Configuration des actions sur les événements

Paramètres de notification. Pour les événements auxquels un événement d'arrêt est associé, vous pouvez aussi définir les paramètres suivants en configurant les événements individuellement ou par groupe, selon les explications indiquées dans les deux sections qui suivent. Pour accéder à ces paramètres, cliquez sur le nom du récepteur ou du destinataire.

Paramètre	Description
Delay *x* time before sending (Délai de *x* avant envoi)	Si l'événement persiste pendant le temps spécifié, une notification est envoyée. Si la condition disparaît avant l'expiration du délai, aucune notification n'est envoyée.
Repeat at an interval of *x* time (Répéter tou(te)s les *x*)	La notification est envoyée selon la période indiquée (ex. : toutes les 2 minutes).
Up to *x* times (Jusqu'à *x* fois)	Tant que l'événement est actif, la notification est répétée autant de fois qu'indiqué.
Until condition clears (Jusqu'à ce que la condition disparaisse)	La notification est envoyée en répétition jusqu'à ce que la condition disparaisse ou soit corrigée.

Configuration par événement. Pour définir les actions sur les événements pour un événement individuel :

1. Sélectionnez l'onglet **Administration**, **Notification** dans la barre de menu supérieure, puis **by event (par événement)** sous **Event Actions (Actions sur les événements)** dans le menu de navigation gauche.
2. Dans la liste d'événements, vérifiez les colonnes marquées pour savoir si l'action qui vous intéresse est déjà configurée (par défaut, la consignation au journal est configurée pour tous les événements).

3. Pour consulter ou modifier la configuration actuelle (par exemple la notification des destinataires par e-mail ou appel téléphonique, ou la notification des systèmes de gestion réseau (NMS) par traps SNMP, cliquez sur le nom de l'événement.

Si aucun serveur Syslog n'est configuré, les éléments qui concernent la configuration Syslog ne s'affichent pas.

Lorsque les détails de configuration d'un événement sont affichés, vous pouvez modifier cette configuration, activer ou désactiver la consignation des événements ou la notification Syslog, ou encore désactiver la notification pour des destinataires par messagerie ou des récepteurs de traps spécifiques, mais vous ne pouvez pas ajouter ou supprimer de destinataires ou de récepteurs. Pour ajouter ou supprimer des destinataires ou des récepteurs, consultez les sections suivantes :

- Identification de serveurs Syslog
- Destinataires des messages électroniques
- Récepteurs de traps

Configuration par groupe. Pour configurer simultanément un groupe d'événements :

1. Sélectionnez l'onglet **Administration**, **Notification** dans la barre de menu supérieure, puis **by group (par groupe)** sous **Event Actions (Actions sur les événements)** dans le menu de navigation gauche.
2. Choisissez comment grouper les événements à configurer :
   - Sélectionnez **Grouped by severity (Événements par gravité)**, puis sélectionnez tous les événements dans un ou plusieurs niveaux de gravité. Vous ne pouvez pas modifier la gravité d'un événement.
   - Sélectionnez **Grouped by category (Événements par catégorie)**, puis sélectionnez tous les événements dans une ou plusieurs catégories définies.

3. Cliquez sur **Next (Suivant) >>** pour changer de page afin d'effectuer les actions suivantes :

   a. Sélectionner les actions sur les événements pour le groupe d'événements.

   - Pour sélectionner une action autre que **Logging (Consignation)** (action par défaut), il faut d'abord qu'au moins un destinataire ou un récepteur concerné soit configuré.
   - Si vous sélectionnez **Logging (Consignation)** en ayant configuré un serveur Syslog, sélectionnez **Event Log (Journal de consignation des événements)** ou **Syslog** (voire les deux) dans la page suivante.

   b. Sélectionnez l'option de laisser activée la nouvelle action sur les événements configurée pour ce groupe d'événements, ou bien de la désactiver.

Notification directe active et automatique

Notification par e-mail

Présentation de la configuration. Utilisez le protocole SMTP (Simple Mail Transfer Protocol) pour envoyer des messages à quatre destinataires maximum lorsqu'un événement se produit.

Pour utiliser la fonction E-mail, vous devez configurer les paramètres suivants :

- L'adresse IP du serveur de noms de domaines (DNS) principal et, en option, du serveur secondaire.

  Voir DNS.

- L'adresse IP ou le nom DNS du **Serveur SMTP** et l'**Adresse de l'expéditeur (From Address)**.

  Voir SMTP.

- L'adresse de messagerie de quatre destinataires maximum.

  Voir Destinataires des messages électroniques.

Vous pouvez utiliser le paramètre **To Address (Adresse du destinataire)** de l'option **recipients (destinataires)** pour envoyer le message à un pager en mode texte.

SMTP.

Chemin d'accès : Administration > Notification > E-mail > server

Paramètre	Description
Local SMTP Server (Serveur SMTP local)	Adresse IPv4/ IPv6 ou nom DNS du serveur SMTP local. **REMARQUE :** cette définition est uniquement requise lorsque **SMTP Server** est paramétré en **Local**. Voir Destinataires des messages électroniques.
From Address (Adresse de l'expéditeur)	Contenu du champ **From (De)** des messages envoyés par la PDU en rack : • au format *utilisateur*@ [*adresse_IP*] (si une adresse IP est spécifiée en **Local SMTP Server**) • au format *utilisateur*@ [*domaine*] (si un DNS est configuré et que son nom DNS est spécifié en **Local SMTP Server**) dans les messages. **REMARQUE :** le serveur SMTP local peut nécessiter l'utilisation d'un compte utilisateur valide chez lui pour ce paramètre. Voir la documentation du serveur.

Destinataires des messages électroniques.

Chemin d'accès : Administration > Notification > E-mail > recipients

Identifiez un maximum de quatre destinataires de messages électroniques.

Paramètre	Description
To Address (Adresse du destinataire)	Nom d'utilisateur et de domaine du destinataire. Pour envoyer un message à un pager, utilisez l'adresse de messagerie du compte de passerelle du pager du destinataire concerné (par exemple : **`myacct100@skytel.com`**). La passerelle du pager génèrera la page. Pour contourner la recherche du serveur DNS de l'adresse IP du serveur de messagerie, indiquez l'adresse IP entre crochets au lieu du nom de domaine (ex. : utilisez jdupont@[xxx.xxx.x.xxx] au lieu de jdupont@societe.com. Cette indication est utile lorsque la recherche de serveur DNS ne fonctionne pas correctement. **REMARQUE :** le pager du destinataire doit être compatible avec une messagerie textuelle.

Paramètre	Description
E-mail Generation (Génération de message)	Active (par défaut) ou désactive l'envoi de message au destinataire.

Serveur SMTP	Sélectionnez l'une des options suivantes de routage des messages :
	• **Local** : par le serveur SMTP de la carte de gestion réseau. Ce paramètre (recommandé) assure l'envoi du message avant les 20 secondes de délai de temporisation de la PDU en rack, avec plusieurs nouvelles tentatives si nécessaire. Configurez aussi les éléments suivants :
	  • Activez le transfert au serveur SMTP de la PDU en rack pour qu'il puisse exécuter le routage des messages vers des serveurs SMTP externes. En général, les serveurs SMTP ne sont pas configurés pour transférer les messages. Consultez votre administrateur réseau (gestion du serveur SMTP) avant de modifier la configuration de votre serveur SMTP pour autoriser les transferts.
	  • Configurez un compte de messagerie spécial pour que la PDU en rack transfère les messages vers un compte de messagerie externe.
	• **Recipient (Destinataire)** : directement au serveur SMTP du destinataire. Avec ce paramètre, la PDU en rack tente d'envoyer le message une seule fois. Si le serveur SMTP distant est très actif, le délai de temporisation risque d'empêcher l'envoi de certains messages.
	Lorsque le destinataire utilise le serveur SMTP de la PDU en rack, ce paramètre n'a aucun effet.

Format	Le format long contient le nom, l'emplacement, le contact, l'adresse IP, le numéro de série du périphérique, la date et l'heure, le code d'événement et la description de l'événement. Le format court ne fournit que la description de l'événement.

Paramètre	Description
User Name - Password - Confirm Password (Nom d'utilisateur - Mot de passe - Confirmer le mot de passe)	Si votre serveur de messagerie requiert une authentification, entrez votre nom d'utilisateur et votre mot de passe ici. Cette authentification est simple et non SSI.

Test de messagerie.

Chemin d'accès : Administration>Notification>E-mail>test

Permet d'envoyer un message de test à un destinataire configuré.

Traps SNMP

Récepteurs de traps.

Chemin d'accès : Administration > Notification > SNMP Traps > trap receivers

Affiche les récepteurs de traps par IP/Nom d'hôte NMS. Vous pouvez configurer jusqu'à six récepteurs de traps.

- Pour configurer un nouveau récepteur de traps, cliquez sur **Add Trap Receiver (Ajouter un récepteur de traps)**.
- Pour modifier ou supprimer un récepteur de traps, cliquez d'abord sur son adresse IP ou son nom d'hôte pour accéder à ses paramètres (si vous supprimez un récepteur de traps, tous les paramètres de notification configurés en Event Actions (Actions sur les événements) pour ce récepteur de traps reprennent leur valeur par défaut).
- Pour spécifier le type de trap pour un récepteur de traps, sélectionnez le bouton d'option SNMPv1 ou SNMPv3. Pour qu'un NMS reçoive les deux types de traps, vous devez configurer deux récepteurs de traps pour lui (un pour chaque type).

Élément	Définition
Trap Generation (Génération de trap)	Active (par défaut) ou désactive la génération de traps pour ce récepteur de traps.
IP/Nom d'hôte NMS	Adresse IPv4/ IPv6 ou nom d'hôte du récepteur de traps. La valeur par défaut 0.0.0.0 laisse le récepteur de traps non défini.

Option SNMPv1.

Élément	Définition
Community Name (Nom de communauté)	Nom (**`public`** par défaut) utilisé comme identifiant lorsque des traps SNMPv1 sont envoyés à ce récepteur de traps.
Authenticate Traps (Authentifier les traps)	Lorsque cette option est activée (par défaut), le NMS identifié par le paramètre NMS IP/Host Name reçoit des traps d'authentification (traps générés en cas de tentatives non valides de connexion au périphérique). Décochez cette case pour désactiver cette possibilité.

Option SNMPv3. Sélectionnez l'identifiant du profil utilisateur pour ce récepteur de traps (pour afficher les paramètres des profils utilisateurs identifiés par les noms d'utilisateurs que vous pouvez sélectionner ici, cliquez sur **Network (Réseau)** dans la barre de menu supérieure et sur **user profiles (profils utilisateurs)** sous **SNMPv3** dans le menu de navigation gauche).

Voir SNMPv3 pour plus d'informations sur la création de profils utilisateurs et la sélection de méthodes d'authentification et de cryptage.

Test de traps SNMP

Chemin d'accès : Administration > Notification > SNMP Traps > test

Last Test Result (Résultat du dernier test). Résultat du plus récent test de trap SNMP. Un test de trap réussi confirme uniquement qu'un trap a été envoyé ; il ne confirme pas que ce trap a bien été reçu par le récepteur de trap sélectionné. Un test de trap est réussi si l'un des cas suivants est vrai :

- La version SNMP (SNMPv1 ou SNMPv3) configurée pour le récepteur de trap sélectionné est activée sur le périphérique.
- Le récepteur de trap est activé.
- Si un nom d'hôte est sélectionné en adresse **To (À)**, ce nom d'hôte peut être mis en correspondance avec une adresse IP valide.

To (À). Sélectionnez l'adresse IP ou le nom d'hôte auquel un test de trap SNMP sera envoyé. Si aucun récepteur de trap n'est configuré, un lien vers la page de configuration de **Trap Receiver (Récepteur de trap)** s'affiche.

Syslog

Chemin d'accès : Logs > Syslog > *options*

La PDU en rack peut envoyer des messages à quatre serveurs Syslog au maximum lorsqu'un événement se produit. Les serveurs Syslog enregistrent les événements qui se produisent sur les périphériques du réseau dans un journal de consignation qui fournit un enregistrement centralisé de ces événements.

Le présent guide d'utilisation ne décrit pas Syslog ni les valeurs de configuration de Syslog en détail. Pour de plus amples informations concernant Syslog, consultez **RFC3164**.

Identification de serveurs Syslog.

Chemin d'accès : Logs > Syslog > servers

Paramètre	Définition
Serveur Syslog	Utilise des adresses IPv4/IPv6 ou des noms d'hôtes pour identifier jusqu'à quatre serveurs devant recevoir les messages Syslog envoyés par la PDU en rack.
Port	Port UDP (user datagram protocol) que la PDU en rack utilisera pour envoyer des messages Syslog. La valeur par défaut est **514** (numéro du port UDP attribué à Syslog).
Protocole	Choisissez la langue à utiliser pour les messages Syslog.

Paramètres Syslog.

Chemin d'accès : Logs > Syslog > settings

Paramètre	Définition
Message Generation (Génération de messages)	Active (par défaut) ou désactive la fonction Syslog.
Facility Code (Code site)	Sélectionne le code attribué aux messages Syslog de la PDU en rack (**User**, par défaut). **REMARQUE : User** définit le mieux les messages Syslog envoyés par la PDU en rack. **Ne modifiez pas** cette sélection, sauf en cas de conseil en ce sens de la part de l'administrateur du réseau Syslog ou de votre administrateur réseau.
Severity Mapping (Mise en correspondance de gravité)	Fait correspondre chaque niveau de gravité des événements de la PDU en rack ou de l'environnement avec les priorités Syslog disponibles. Il ne devrait pas être nécessaire de modifier ces paramètres. Les définitions suivantes sont celles de RFC3164 : • **Urgence** : le système est inutilisable. • **Alerte** : une action doit intervenir immédiatement. • **Critique** : conditions critiques. • **Erreur** : conditions d'erreur. • **Avertissement** : conditions d'avertissement. • **Remarque** : conditions normales mais à surveiller. • **Info** : messages d'information. • **Débogage** : messages de débogage. Voici les paramètres par défaut correspondant aux paramètres **Local Priority** : • **Grave** correspond à **Critique**. • **Avertissement** correspond à **Avertissement**. • **Informatif** correspond à **Info**. **REMARQUE :** pour désactiver les messages Syslog, consultez la section Configuration des actions sur les événements.

Test Syslog et exemple de format.

Chemin d'accès : Logs > Syslog > test

Envoie un message de test aux serveurs Syslog configurés dans l'option **servers**.

1. Sélectionnez la gravité à attribuer au message de test.
2. Définissez le message de test selon les champs de message requis.

– Priorité (PRI) : priorité Syslog attribuée à l'événement objet du message, et code site des messages envoyés par la PDU en rack.

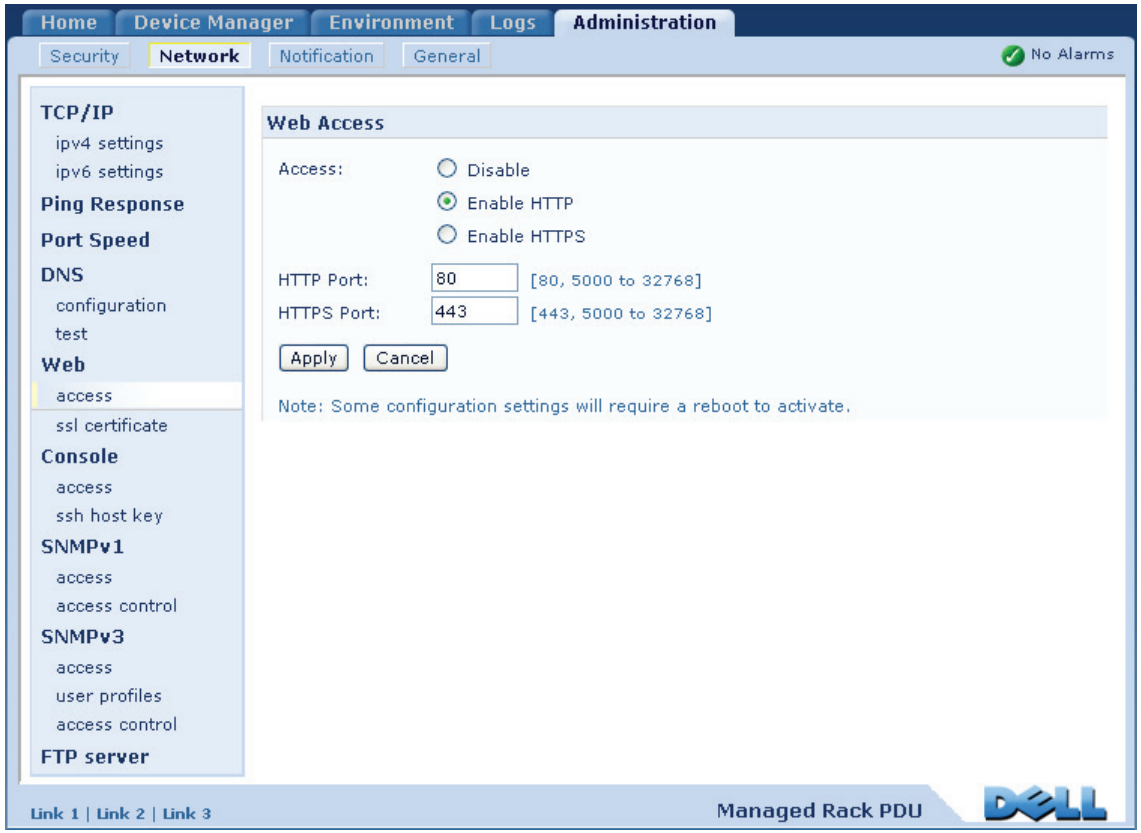
– En-tête : horodatage et adresse IP de la PDU en rack.

– Partie message (MSG) :

- Le champ TAG suivi du signe deux points et d'un espace identifie le type d'événement.
- Le champ CONTENT porte le texte de l'événement, suivi (en option) par un espace et le code de l'événement.

  Par exemple, **`Dell: Test Syslog`** est valide.

Administration : Fonctions réseau



Paramètres TCP/IP et de communication

Paramètres TCP/IP

Chemin d'accès : Administration > Network > TCP/IP

L'option **TCP/IP** du menu de navigation gauche, sélectionnée par défaut lorsque vous choisissez **Network** (Réseau) dans la barre de menu supérieure, affiche l'adresse IPv4, le masque de sous-réseau, la passerelle par défaut et l'adresse MAC actuels de la PDU en rack.

Pour des informations sur le protocole et les options DHCP, voir **RFC2131** et **RFC2132**.

Paramètre	Description
Activer	Cette case à cocher active ou de désactive IPv4.
Manual	Permet de configurer IPv4 manuellement en entrant l'adresse IP, le masque de sous-réseau et la passerelle par défaut.
1. En général, il n'est pas nécessaire de modifier les valeurs par défaut de ces trois paramètres des pages de configuration : •**Vendor Class (Catégorie de fournisseur)** : DELL •**Client ID (Identifiant client)** : adresse MAC de la PDU en rack, qui l'identifie de manière unique sur le réseau local (LAN). •**User Class (Catégorie d'utilisateur)** : nom du module du microprogramme d'application.	

Paramètre	Description
BOOTP	Un serveur BOOTP fournit les paramètres TCP/IP. Par intervalles de 32 secondes, la PDU en rack envoie une requête d'attribution réseau à n'importe quel serveur BOOTP : • Si la PDU en rack reçoit une réponse valide, elle démarre les services réseau. • Si la PDU en rack trouve un serveur BOOTP, mais que la requête à ce serveur échoue ou dépasse le délai d'attente, la PDU en rack abandonne ses requêtes de paramètres réseau jusqu'à son redémarrage. • Par défaut, s'il existe des paramètres réseau précédemment configurés et que la PDU en rack ne reçoit aucune réponse valide à cinq requêtes (requête initiale plus quatre tentatives ultérieures), elle utilise les paramètres précédemment configurés afin de rester accessible. Cliquez sur **Next>>** pour accéder à la page de configuration BOOTP afin de modifier le nombre de nouvelles tentatives ou l'action à effectuer si toutes les tentatives échouent [1] : • **Maximum retries (Nombre maximum de nouvelles tentatives)** : entrez le nombre de nouvelles tentatives à effectuer lorsqu'aucune réponse valide n'est reçue, ou zéro (0) pour un nombre illimité de tentatives. • **If retries fail (En cas d'échec des nouvelles tentatives)** : sélectionnez **Use prior settings** (valeur par défaut) ou **Stop BOOTP request** (Arrêter les requêtes BOOTP).

1. En général, il n'est pas nécessaire de modifier les valeurs par défaut de ces trois paramètres des pages de configuration :
   •**Vendor Class (Catégorie de fournisseur)** : DELL
   •**Client ID (Identifiant client)** : adresse MAC de la PDU en rack, qui l'identifie de manière unique sur le réseau local (LAN).
   •**User Class (Catégorie d'utilisateur)** : nom du module du microprogramme d'application.

Paramètre	Description
DHCP	Paramètre par défaut. Par intervalles de 32 secondes, la PDU en rack envoie une requête d'attribution réseau à n'importe quel serveur DHCP : • Si la PDU en rack reçoit une réponse valide, elle ne demande pas le cookie fournisseur au serveur DHCP pour accepter le bail et démarrer les services réseau. • Si la PDU en rack trouve un serveur DHCP, mais que la requête à ce serveur échoue ou expire, la PDU abandonne ses requêtes de paramètres réseau jusqu'à son redémarrage[1]. • **Require vendor specific cookie to accept DHCP Address (Cookie du fournisseur nécessaire pour accepter l'adresse DHCP)** : lorsque cette case est cochée, vous pouvez demander au serveur DHCP de fournir un cookie contenant des informations destinées à la PDU en rack.

1. En général, il n'est pas nécessaire de modifier les valeurs par défaut de ces trois paramètres des pages de configuration :
   •**Vendor Class (Catégorie de fournisseur)** : DELL
   •**Client ID (Identifiant client)** : adresse MAC de la PDU en rack, qui l'identifie de manière unique sur le réseau local (LAN).
   •**User Class (Catégorie d'utilisateur)** : nom du module du microprogramme d'application.

Options de réponse DHCP

Chaque réponse DHCP valide contient des options fournissant les paramètres TCP/IP que requiert la PDU en rack pour fonctionner en réseau, ainsi que des informations supplémentaires ayant une incidence sur le fonctionnement de la PDU en rack.

Informations spécifiques au fournisseur (option 43). La PDU en rack utilise cette option dans une réponse DHCP pour en définir la validité. Cette option contient une option spécifique au format TAG/LEN/DATA, appelée cookie Fournisseur. Ce paramètre est désactivé par défaut.

- **Vendor Cookie (Cookie Fournisseur). Tag 1, Len 4, Data « 1APC »**
  L'option 43 informe la PDU en rack qu'un serveur DHCP est configuré pour prendre en charge les PDU en rack Dell.
  Voici un exemple, au format hexadécimal, d'une option d'informations spécifiques au fournisseur contenant le cookie fournisseur :

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43
```

Options TCP/IP. La PDU en rack utilise les options suivantes dans une réponse DHCP valide pour définir ses paramètres TCP/IP. Toutes ces options, sauf la première, sont décrites dans **RFC2132**.

- **Adresse IP** (à partir du champ **yiaddr** de la réponse DHCP, décrit en **RFC2131)** : adresse IP attribuée à la PDU en rack par le serveur DHCP.
- **Subnet Mask (Masque de sous-réseau)** (option 1) : valeur du masque de sous-réseau requise par la PDU en rack pour fonctionner en réseau.
- **Router** (Routeur), c'est-à-dire la passerelle par défaut (option 3) : adresse de la passerelle par défaut requise par la PDU en rack pour fonctionner en réseau.
- **IP Address Lease Time** (Durée de bail d'adresse IP) (option 51) : durée du bail de l'adresse IP de la PDU en rack.
- **Renewal Time, T1** (Durée de renouvellement, T1) (option 58) : durée d'attente requise par la PDU en rack après l'attribution d'un bail d'adresse IP avant de demander que cette attribution soit renouvelée.

- **Rebinding Time, T2** (Durée de reliaison, T2) (option 59) : durée d'attente requise par la PDU en rack après l'attribution d'un bail d'adresse IP avant de pouvoir tenter de réassocier cette attribution.

Autres options. La PDU en rack utilise également ces options dans une réponse DHCP valide. Toutes ces options, sauf la dernière, sont décrites dans **RFC2132**.

- **Network Time Protocol Servers** (Serveurs du protocole de temps du réseau) (option 42) : jusqu'à deux serveurs NTP (primaire et secondaire) que peut utiliser la PDU en rack.
- **Time Offset** (Décalage de temps) (option 2) : décalage du sous-réseau de la PDU en rack en secondes par rapport à l'UTC (temps universel coordonné).
- **Domain Name Server** (Serveur de nom de domaine) (option 6) : jusqu'à deux serveurs DNS (primaire et secondaire) que peut utiliser la PDU en rack.
- **Host Name** (Nom d'hôte) (option 12) : nom d'hôte que la PDU en rack utilisera (32 caractères maximum).
- **Domain Name** (Nom de domaine) (option 15) : nom de domaine que la PDU en rack utilisera (64 caractères maximum).
- **Boot File Name** (Nom du fichier d'initialisation) (à partir du champ **file** (fichier) de la réponse DHCP, décrit en **RFC2131)** : chemin d'accès complet à un fichier de configuration utilisateur (fichier .ini) afin de le télécharger. Le champ **siaddr** de la réponse DHCP spécifie l'adresse IP du serveur depuis lequel la PDU en rack va télécharger le fichier .ini. Après le téléchargement, la PDU en rack utilise le fichier .ini comme fichier de démarrage pour reconfigurer ses paramètres.

Chemin d'accès : Administration > Network > TCP/IP > IPv6 settings

Paramètre	Description
Enable (Activer)	Cette case à cocher active ou désactive IPv6.
Manual (Manuel)	Permet de configurer IPv6 manuellement en entrant l'adresse IP et la passerelle par défaut.
Auto Configuration (Configuration automatique)	Lorsque la case Auto Configuration est cochée, le système obtient les préfixes d'adressage du routeur (si possible). Il utilise ces préfixes pour configurer automatiquement les adresses IPv6.

Paramètre	Description
DHCPv6 Mode (Mode DHCPv6)	**Router Controlled (Contrôlé par routeur) :** lorsque cette option est cochée, DHCPv6 est contrôlé par les indicateurs Managed (M) (Géré) et Other (O) (Autre) reçus dans les annonces de routage IPv6. Lorsqu'une annonce de routage est reçue, la carte de gestion réseau vérifie si l'indicateur est M ou O. La carte de gestion réseau interprète l'état des « bits » M (indicateur de configuration de l'adresse gérée) et O (indicateur d'autre configuration avec état) dans les cas suivants : • *Aucun n'est défini* : le réseau local n'a aucune infrastructure DHCPv6. La carte de gestion réseau utilise les annonces de routage et la configuration manuelle pour obtenir des adresses sans liaison locale et d'autres paramètres. • *M ou bien M et O sont définis* : dans cette situation, une configuration d'adresse DHCPv6 complète survient. DHCPv6 est utilisé pour obtenir des adresses ET d'autres paramètres de configuration. Ceci est appelé DHCPv6 avec état. Lorsque l'indicateur M a été reçu, la configuration d'adresse DHCPv6 reste en effet jusqu'à ce que l'interface concernée soit fermée. Ceci est vrai même si des paquets d'annonces de routage ultérieurs sont reçus dans lesquels l'indicateur M n'est pas défini. Si un indicateur O est reçu en premier, suivi par la réception ultérieure d'un indicateur M, la carte de gestion réseau effectue une configuration d'adresse complète dès la réception de l'indicateur M. • *Seul O est défini :* dans cette situation, la carte de gestion réseau envoie un paquet de requête d'informations DHCPv6. DHCPv6 sera utilisé pour configurer les « autres » paramètres (tels que l'emplacement des serveurs DNS), mais PAS pour fournir des adresses. Ceci est appelé DHCPv6 sans état. **Address and Other Information: (Adresse et autres informations :)** lorsque cette option est sélectionnée, DHCPv6 est utilisé pour obtenir des adresses ET d'autres paramètres de configuration. Ceci est appelé DHCPv6 avec état. **Non-Address Information Only: (Informations hors adresse uniquement :)** lorsque cette option est sélectionnée, DHCPv6 sera utilisé pour configurer les « autres » paramètres (tels que l'emplacement des serveurs DNS), mais PAS pour fournir des adresses. Ceci est appelé DHCPv6 sans état. **Never: (Jamais :)** cette option désactive DHCPv6.

Temps de réponse du ping

Chemin d'accès : Administration > Network > Ping Response

Cochez la case Enable de l'option **IPv4 Ping Response (Réponse du ping IPv4)** pour permettre à la carte de gestion réseau de répondre aux tests Ping du réseau. Décochez-la pour désactiver la réponse d'une carte de gestion réseau. Ceci ne s'applique pas à IPv6.

Vitesse du port

Chemin d'accès : Administration > Network > Port Speed

Le paramètre **Port Speed (Vitesse du port)** définit la vitesse de communication du port TCP/IP.

- En **Auto-negotiation (Négociation automatique)** (valeur par défaut), les périphériques Ethernet négocient les transmissions à la vitesse la plus élevée possible, mais si les vitesses prises en charge de deux périphériques ne correspondent pas, c'est la vitesse la plus lente qui est utilisée.
- Vous pouvez aussi choisir une vitesse de 10 Mbits/s ou 100 Mbits/s, chacune avec l'option semi-duplex (transmissions dans un sens à la fois) ou duplex (transmissions simultanées dans les deux sens sur le même canal).

DNS

Chemin d'accès : Administration > Network > DNS > *options*

Utilisez les options du menu **DNS** pour configurer le système de noms de domaine (DNS) et le tester :

- Sélectionnez **Primary DNS Server (Serveur DNS primaire)** ou **Secondary DNS Server (Serveur DNS secondaire)** pour spécifier les adresses IPv4 ou IPv6 du serveur DNS primaire ou du serveur secondaire en option. Pour que la PDU en rack puisse envoyer des courriels, vous devez au moins définir l'adresse IP du serveur DNS primaire.
  - La PDU en rack attend jusqu'à 15 secondes une réponse du serveur DNS primaire ou du serveur DNS secondaire (dans la mesure où un serveur DNS secondaire a été spécifié). Si la PDU en rack ne reçoit pas de réponse pendant ce délai, aucun e-mail ne peut être envoyé. Par conséquent, utilisez des serveurs DNS reliés au même segment du réseau que la PDU en rack ou à un segment adjacent (sans passer par un réseau étendu [WAN]).
  - Après avoir défini les adresses IP des serveurs DNS, vérifiez que le protocole DNS fonctionne correctement en entrant le nom DNS d'un ordinateur de votre réseau pour rechercher son adresse IP.
- **Host Name (Nom d'hôte)** : lorsque vous avez configuré un nom d'hôte dans cette zone et un nom de domaine dans le champ **Domain Name** , les utilisateurs peuvent entrer un nom d'hôte dans n'importe quel champ de l'interface de la PDU en rack (à l'exception des adresses électroniques) qui accepte un nom de domaine.
- **Domain Name (IPv4) (Nom de domaine (IPv4))** : vous devez configurer le nom de domaine uniquement ici. Dans tous les autres champs de l'interface de la PDU en rack (à l'exception des adresses électroniques) qui acceptent les noms de domaines, la PDU en rack ajoute ce nom de domaine lorsque seul un nom d'hôte est entré.
  - Pour ignorer tous les cas d'extension d'un nom d'hôte spécifié par l'ajout d'un nom de domaine, définissez le champ du nom de domaine sur sa valeur par défaut (`somedomain.com`) ou sur `0.0.0.0`.

  - Pour ignorer l'extension d'une entrée de nom d'hôte spécifique (par exemple à la définition d'un récepteur de traps), ajoutez un point final. La PDU en rack reconnaît un nom d'hôte comprenant un point final (tel que `monServeurSnmp.`) comme étant un nom de domaine complet et n'ajoute alors pas le nom de domaine.
- **Domain Name (IPv6) (Nom de domaine (IPv6))** : spécifiez ici le nom de domaine IPv6.
- Sélectionnez **test** pour envoyer une requête DNS permettant de tester la configuration de vos serveurs DNS :
  - En paramètre **Query Type (Type de requête)**, sélectionnez la méthode à employer pour la requête DNS :
    - **by Host (par hôte)** : nom URL du serveur
    - **by FQDN (par FQDN)** : nom de domaine complet
    - **by IP (par IP)** : adresse IP du serveur
    - **by MX (par MX)** : messagerie utilisée par le serveur
  - En **Query Question (Question de la requête)**, identifiez la valeur à attribuer au type de requête sélectionné :

Type de requête sélectionné	Question de la requête à utiliser
by Host	URL
by FQDN	Nom de domaine complet : `mon_serveur.`*mon_domaine*.
by IP	Adresse IP
by MX	Adresse de messagerie

  - Le résultat de la requête de test DNS s'affiche dans le champ **Last Query Response (Réponse à la dernière requête)**.

Web

Chemin d'accès : Administration > Network > Web > *options*

Option	Description

accès	Pour activer les modifications apportées aux choix ci-dessous, déconnectez-vous de la PDU en rack :
	• **Disable** (Désactiver) : désactive l'accès à l'interface Web (pour le réactiver, connectez-vous à l'interface par lignes de commande, puis tapez la commande **`http -S enable`**. Pour l'accès HTTPS, tapez **`https -S enable`**).
	• **Activer HTTP** (option par défaut) : active le protocole HTTP (Hypertext Transfer Protocol), qui fournit l'accès Web par nom d'utilisateur et mot de passe, mais sans coder les noms d'utilisateurs, les mots de passe ni les données pendant la transmission.
	• **Activer HTTPS** : active le protocole HTTPS (Hypertext Transfer Protocol avec Secure Sockets Layer [SSL]) Le protocole SSL code les noms d'utilisateurs, les mots de passe et les données pendant la transmission, et authentifie la PDU en rack par certificat numérique. Lorsque le protocole HTTPS est activé, votre navigateur affiche une petite icône représentant un cadenas.
	
	Pour choisir une méthode d'utilisation des certificats numériques, consultez « Creating and Installing Digital Certificates » (Création et installation de certificats numériques) en Annexe B : Guide de sécurité.
	
	HTTP Port : port TCP/IP (port 80 par défaut) utilisé pour communiquer par protocole HTTP avec la PDU en rack.
	
	HTTPS Port : port TCP/IP (port 443 par défaut) utilisé pour communiquer par protocole HTTPS avec la PDU en rack.
	
	Pour plus de sécurité, vous pouvez modifier le paramètre de ces ports sur un port inutilisé compris entre 5000 et 32768. Les utilisateurs doivent alors taper le signe deux points (:) dans le champ d'adresse du navigateur pour spécifier le numéro du port. Par exemple, pour se connecter par le port numéro 5000 et l'adresse IP 152.214.12.114 :
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`

Option	Description
ssl certificate (certificat SSL)	Ajout, remplacement ou suppression d'un certificat de sécurité. **État** : • **Not installed (Non installé)** : un certificat n'est pas installé, ou a été installé par FTP ou SCP à un emplacement incorrect. L'option **Add or Replace Certificate File** (Ajouter ou remplacer le fichier du certificat) installe le certificat à l'emplacement correct, à savoir **/ssl** sur la PDU en rack. • **Generating** (Création) : la PDU en rack génère un certificat car aucun certificat valide n'a été trouvé. • **Loading** (Chargement) : un certificat est en cours d'activation sur la PDU en rack. • **Valid certificate** (Certificat valide) : un certificat valide a été installé ou a été généré par la PDU en rack. Cliquez sur ce lien pour afficher le contenu du certificat. **Si vous installez un certificat non valide, ou si aucun certificat n'est chargé lorsque vous activez le protocole SSL, la** PDU en rack **génère un certificat par défaut mais ce processus peut retarder l'accès à l'interface jusqu'à une minute.** Vous pouvez utiliser le certificat par défaut pour les protocoles de sécurité codés de base, mais dans ce cas un message d'alerte de sécurité s'affiche chaque fois que vous vous connectez. **Add or Replace Certificate File** (Ajouter ou remplacer le fichier du certificat) : entrez le fichier de certificat créé avec l'Assistant de sécurité ou naviguez jusqu'à ce fichier. Pour choisir une méthode d'utilisation des certificats numériques créés par l'Assistant de sécurité ou générés par la PDU en rack, consultez « Création et installation de certificats numériques) » en Annexe B : Guide de sécurité. **Remove** (Supprimer) : supprimer le certificat actif.

Console

Chemin d'accès : Administration > Network > Console > *options*

Option	Description

access	Les options suivantes sont proposées pour l'accès par Telnet ou Secure Shell (SSH) :
	• **Disable** (Désactiver) : désactive tout accès à l'interface par lignes de commande.
	• **Enable Telnet** (Activer Telnet) (option par défaut) : le protocole Telnet transmet les noms d'utilisateurs, les mots de passe et les données sans codage.
	• **Enable SSH** (Activer SSH) : le protocole SSH transmet les noms d'utilisateurs, les mots de passe et les données sous forme codée, offrant une protection contre les tentatives d'interception, de contrefaçon ou d'altération des données au cours de leur transmission.
	Configurez les ports que ces protocoles devront utiliser :
	• **Telnet Port** : port Telnet utilisé pour communiquer avec la PDU en rack (port 23 par défaut). Pour plus de sécurité, vous pouvez modifier le paramètre du port sur un port inutilisé compris entre 5000 et 32768. Les utilisateurs doivent alors taper le signe deux points (:) ou un espace, selon les exigences de votre programme client Telnet, pour spécifier la valeur du port autre que la valeur par défaut. Par exemple pour le port 5000 et l'adresse IP 152.214.12.114, votre client Telnet exige l'une des commandes suivantes :
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• **SSH Port** : port SSH utilisé pour communiquer avec la PDU en rack (port 22 par défaut). Pour plus de sécurité, vous pouvez modifier le paramètre du port sur un port inutilisé compris entre 5000 et 32768. Consultez la documentation de votre client SSH pour connaître le format de ligne de commande requis pour spécifier un port autre que le port par défaut.

Option	Description
ssh host key (clé de l'hôte SSH)	**Status** indique l'état de la clé d'hôte (clé privée) : • **SSH Disabled: No host key in use (SSH désactivé : aucune clé d'hôte utilisée) :** lorsqu'il est désactivé, le protocole SSH ne peut pas utiliser de clé d'hôte. • **Generating** (Création) : la PDU en rack crée une clé d'hôte car aucune clé d'hôte valide n'a été trouvée. • **Loading** (Chargement) : une clé d'hôte est en cours d'activation sur la PDU en rack. • **Valid** : une des clés d'hôtes suivantes se trouve dans le répertoire **/ssh** (emplacement requis sur la PDU en rack) : •Clé d'hôte de 1024 ou 2048 bits créée par l'Assistant de sécurité. •Clé d'hôte RSA de 2048 bits générée par la PDU en rack. **Add or Replace** (Ajouter ou Remplacer) : permet de naviguer jusqu'à un fichier de clé d'hôte créé par l'Assistant de sécurité et de le télécharger. Pour utiliser l'Assistant de sécurité, consultez Annexe B : Guide de sécurité. **REMARQUE :** pour réduire le temps nécessaire pour activer le protocole SSH, créez une clé d'hôte à l'avance et téléchargez-la. **Si vous activez le protocole SSH sans qu'aucune clé d'hôte ne soit chargée, la** PDU en rack **prend jusqu'à une minute pour en créer une, délai au cours duquel le serveur SSH est inaccessible.** **Remove** (Supprimer) : supprime la clé d'hôte active.

Pour utiliser le protocole SSH, un client SSH doit être installé. La plupart des plateformes Linux et UNIX comprennent un client SSH, mais pas les systèmes d'exploitation Microsoft Windows. Les clients sont disponibles auprès de plusieurs fournisseurs.

SNMP

Tous les noms d'utilisateur, les mots de passe et les noms de communauté pour SNMP sont transmis sur le réseau sous forme de simple texte. Si votre réseau nécessite un codage de haute sécurité, désactivez l'accès SNMP ou paramétrez-le en lecture seule pour chaque communauté (une communauté disposant de l'accès en lecture peut recevoir des informations d'état et utiliser les traps SNMP).

Pour des informations détaillées sur l'amélioration et la gestion de la sécurité de votre système, consultez Annexe B : Guide de sécurité.

SNMPv1

Chemin d'accès : Administration > Network > SNMPv1 > *options*

Option	Description
access	**Enable SNMPv1 Access (Activer l'accès SNMPv1) :** active SNMP version 1 comme méthode de communication avec cet appareil.
access control (contrôle d'accès)	Vous pouvez configurer jusqu'à quatre entrées de contrôle d'accès pour spécifier les systèmes de gestion réseau (NMS) ayant accès à ce périphérique. Par défaut, la page d'ouverture du contrôle d'accès attribue une entrée à chacune des quatre communautés SNMPv1 disponibles. Vous pouvez toutefois modifier ces paramètres pour attribuer plus d'une entrée à une communauté afin de permettre l'accès par plusieurs adresses, noms d'hôtes ou masques d'adresse IP IPv4 et IPv6 spécifiques. Pour modifier les paramètres de contrôle d'accès pour une communauté, cliquez sur le nom de la communauté. • Si l'entrée du contrôle d'accès par défaut d'une communauté est inchangée, cette communauté a accès à ce périphérique depuis n'importe quel emplacement sur le réseau. • Si vous configurez plusieurs entrées de contrôle d'accès pour un seul nom de communauté, la limite de quatre entrées impose qu'une des autres communautés ou plusieurs n'aient aucune entrée de contrôle d'accès. Si aucune entrée de contrôle d'accès n'est répertoriée pour une communauté, celle-ci n'a pas accès à ce périphérique. **Community Name (Nom de communauté) :** nom que doit utiliser un système NMS pour accéder à la communauté. La longueur maximum est de 15 caractères ASCII et les noms par défaut des communautés sont **`public`**, **`private`**, **`public2`** et **`private2`**. **NMS IP/Host Name (IP/Nom d'hôte NMS) :** adresse IPv4 ou IPv6, masque de l'adresse IP ou nom d'hôte qui contrôle l'accès par les NMS. Un nom d'hôte ou une adresse IP spécifique (telle que 149.225.12.1) permet uniquement l'accès du NMS à cet emplacement précis. Les adresses IP contenant 255 limitent l'accès de la manière suivante : • 149.225.12.**255** : accès uniquement par un NMS sur le segment 149.225.12. • 149.225.**255.255** : accès uniquement par un NMS sur le segment 149.225. • 149.**255.255.255** : accès uniquement par un NMS sur le segment 149. • 0.0.0.0 (paramètre par défaut) que l'on peut aussi exprimer sous la forme 255.255.255.255 : accès par tous les NMS sur tous les segments. **Access Type** (Type d'accès) : actions qu'un NMS peut effectuer par l'intermédiaire de la communauté. • **Read** (Lecture) : commandes GET uniquement, à tout moment. • **Write** (Écriture) : commandes GET à tout moment, commandes SET lorsqu'aucun utilisateur n'est connecté à l'interface Web ni à l'interface par lignes de commande. • **Write+** : commandes GET et SET à tout moment. • **Disable** (Désactiver) : aucune commande GET ni SET, à aucun moment.

SNMPv3

Chemin d'accès : Administration > Network > SNMPv3 > *options*

Pour les destinataires de GET, de SET et d'interruptions SNMP, SNMPv3 utilise un système de profils pour identifier les utilisateurs. Un utilisateur SNMPv3 doit avoir un profil utilisateur assigné dans le logiciel MIB pour effectuer des GET et des SET, naviguer dans la MIB et recevoir des traps.

Pour utiliser SNMPv3, vous devez avoir un programme MIB compatible SNMPv3.

La PDU en rack prend en charge l'authentification SHA ou MD5 et le codage AES ou DES.

Option	Description
access	**SNMPv3 Access :** permet d'activer SNMPv3 comme méthode de communication avec ce périphérique.

Option	Description
user profiles (profils utilisateur)	Répertorie par défaut les paramètres de quatre profils utilisateurs, configurés avec les noms d'utilisateurs **dell snmp profile1** à **dell snmp profile4** et sans authentification ni confidentialité (pas de codage). Pour modifier les paramètres suivants d'un profil utilisateur, cliquez sur un nom d'utilisateur dans la liste. **User Name (Nom d'utilisateur) :** identifiant du profil utilisateur. SNMP version 3 mappe les commandes GET, SET et les traps vers un profil utilisateur en vérifiant la correspondance entre le nom d'utilisateur du profil et celui présent dans le paquet de données transmis. Un nom d'utilisateur peut contenir jusqu'à 32 caractères ASCII. **Authentication Passphrase (Clé d'authentification) :** clé de 15 à 32 caractères ASCII (par défaut **`dell auth passphrase`**) qui permet de vérifier que le NMS en communication avec le périphérique par protocole SNMPv3 est bien le NMS qu'il dit être, que le message n'a pas été modifié au cours de la transmission, et que le message a été communiqué en temps utile, indiquant qu'il n'a subi aucun retard et qu'il n'a pas été copié puis renvoyé ultérieurement à une heure inappropriée. **Privacy Passphrase (Clé privée) :** clé de 15 à 32 caractères ASCII (par défaut **`dell crypt passphrase`**) qui garantit la confidentialité des données (par l'intermédiaire d'un codage) envoyées par un NMS à ce périphérique ou reçues depuis ce périphérique par protocole SNMPv3. **Authentication Protocol (Protocole d'authentification) :** l'implémentation Dell du protocole SNMPv3 prend en charge les authentifications SHA et MD5. L'authentification n'interviendra que si un protocole d'authentification est sélectionné. **Privacy Protocol (Protocole de confidentialité) :** l'implémentation Dell du protocole SNMPv3 prend en charge les protocoles AES et DES comme protocoles de codage et de décodage des données. La confidentialité des données transmises nécessite qu'un protocole de confidentialité soit sélectionné et qu'une clé de confidentialité soit fournie dans la requête provenant du NMS. Lorsqu'un protocole de confidentialité est activé mais que le NMS ne fournit pas de clé de confidentialité, la requête SNMP n'est pas codée. **Remarque :** vous ne pouvez pas sélectionner le protocole de confidentialité si aucun protocole d'authentification n'est sélectionné.

Option	Description
access control (contrôle d'accès)	Vous pouvez configurer jusqu'à quatre entrées de contrôle d'accès pour spécifier les NMS ayant accès à ce périphérique. Par défaut, la page d'ouverture du contrôle d'accès attribue une entrée à chacun des quatre profils utilisateurs. Vous pouvez toutefois modifier ces paramètres pour attribuer plus d'une entrée à un profil utilisateur afin de permettre l'accès par plusieurs adresses IP, noms d'hôtes ou masques d'adresse IP spécifiques. • Si l'entrée de contrôle d'accès par défaut d'un profil utilisateur est inchangée, tous les NMS utilisant ce profil ont accès à ce périphérique. • Si vous configurez plusieurs entrées de contrôle d'accès pour un seul profil utilisateur, la limite de quatre entrées impose qu'un des autres profils utilisateurs ou plusieurs n'aient aucune entrée de contrôle d'accès. Si aucune entrée de contrôle d'accès n'est répertoriée pour un profil utilisateur, aucun NMS utilisant ce profil n'a accès à ce périphérique. Pour modifier les paramètres de contrôle d'accès pour un profil utilisateur, cliquez sur son nom d'utilisateur. **Access:** cochez la case **Enable** pour activer la contrôle d'accès spécifié par les paramètres de cette entrée de contrôle d'accès. **User Name (Nom d'utilisateur) :** sélectionnez dans la liste déroulante le profil utilisateur auquel ce contrôle d'accès va s'appliquer. Les choix possibles sont les quatre noms d'utilisateurs que vous configurez par l'intermédiaire de l'option **profils utilisateurs** du menu de navigation gauche. **NMS IP/Host Name (IP/Nom d'hôte NMS) :** adresse IP, masque de l'adresse IP ou nom d'hôte qui contrôle l'accès par les NMS. Un nom d'hôte ou une adresse IP spécifique (telle que 149.225.12.1) permet uniquement l'accès du NMS à cet emplacement précis. Un masque d'adresse IP contenant la valeur 255 limite l'accès de la manière suivante : • 149.225.12.**255** : accès uniquement par un NMS sur le segment 149.225.12. • 149.225.**255.255** : accès uniquement par un NMS sur le segment 149.225. • 149.**255.255.255** : accès uniquement par un NMS sur le segment 149. • 0.0.0.0 (paramètre par défaut) que l'on peut aussi exprimer sous la forme 255.255.255.255 : accès par tous les NMS sur tous les segments.

Serveur FTP

Chemin d'accès : Administration > Network > FTP Server

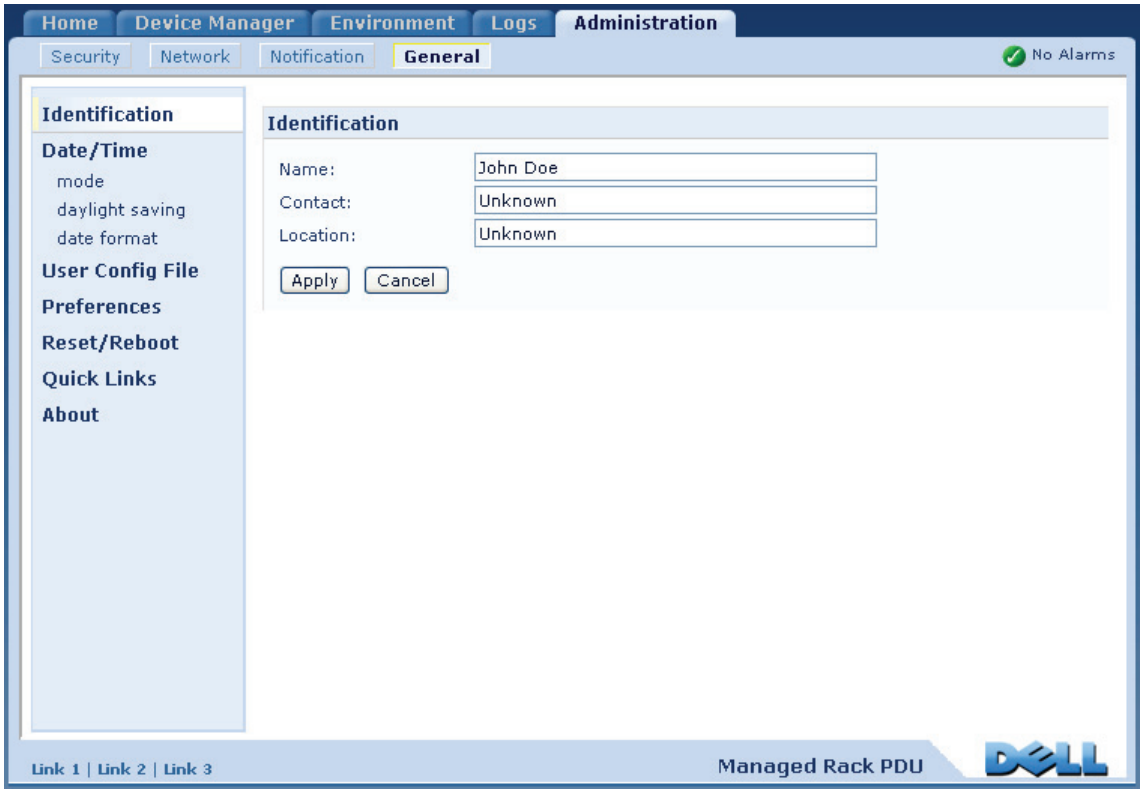
Les paramètres de **Serveur FTP** permettent d'activer (par défaut) ou de désactiver l'accès au serveur FTP et de spécifier le port TCP/IP (port 21 par défaut) que le serveur FTP utilise pour communiquer avec la PDU en rack. Le serveur FTP utilise à la fois le port du numéro spécifié et celui du numéro immédiatement inférieur.

Vous pouvez remplacer le paramètre **Port** par le numéro d'un port inutilisé quelconque entre 5001 et 32768, afin de fournir une sécurité supplémentaire. Les utilisateurs doivent alors utiliser le signe deux points (:) pour spécifier le numéro de port autre que par défaut. Par exemple, pour le port 5001 et l'adresse IP 152.214.12.114, la commande serait **`ftp 152.214.12.114:5001`**.

FTP permet de transférer les fichiers sans codage. Pour une plus haute sécurité, désactivez le serveur FTP et transférez les fichiers avec le protocole SCP. Sélectionner et configurer Secure Shell (SSH) active automatiquement le protocole SCP.

Pour des informations détaillées sur l'amélioration et la gestion de la sécurité de votre système, consultez Annexe B : Guide de sécurité.

Administration : Options Généralités



Identification

Chemin d'accès : Administration > General > Identification

Permet de définir le **Nom** (nom du périphérique), l'**Emplacement** (emplacement physique) et le **Contact** (personne responsable du périphérique) utilisés par l'agent SNMP de la PDU en rack. Ces paramètres sont les valeurs de **sysName**, **sysContact** et **sysLocation** utilisées pour les OID (identifications d'objets) MIB-II.

Pour plus d'informations sur les OID MIB-II, consultez la base de données de gestion (MIB) Dell.

Réglage de la date et de l'heure

Méthode

Chemin d'accès : Administration > General > Date & Time > mode

Permet de configurer la date et l'heure utilisées par la PDU en rack Vous pouvez modifier les paramètres actuels manuellement ou par l'intermédiaire d'un serveur NTP (Network Time Protocol) :

- **Mode manuel** : utilisez l'une de ces méthodes :
  - Entrez la date et l'heure de la PDU en rack.
  - Cochez la case **Apply Local Computer Time (Appliquer l'heure système locale)** pour que les paramètres de date et d'heure correspondent à ceux de l'ordinateur que vous utilisez.
- **Synchronize with NTP Server (Synchroniser avec le serveur NTP)** : un serveur NTP définit la date et l'heure pour la PDU en rack.

Paramètre	Définition
Primary NTP Server (Serveur NTP primaire)	Entrez l'adresse IP ou le nom de domaine du serveur NTP primaire.
Secondary NTP Server (Serveur NTP secondaire)	Entrez l'adresse IP ou le nom de domaine du serveur NTP secondaire, le cas échéant.
Time Zone (Fuseau horaire)	Permet de sélectionner un fuseau horaire. Le nombre d'heures qui précède chaque fuseau horaire dans la liste correspond au décalage par rapport au temps universel coordonné (UTC), anciennement intitulé Heure du méridien de Greenwich (GMT).
Update Interval (Fréquence de mise à jour)	Définit à quelle fréquence (en heures) la PDU en rack accède au serveur NTP pour effectuer une mise à jour. *Minimum* : 1; *Maximum* : 8760 (1 an).
Update Using NTP Now (Mettre à jour avec NTP)	Permet de lancer une mise à jour immédiate de la date et de l'heure par l'intermédiaire du serveur NTP.

Heure d'été

Chemin d'accès : Administration > General > Date & Time > daylight saving

Permet d'activer l'heure d'été habituelle des États-Unis (DST), ou d'activer et de configurer une heure d'été personnalisée correspondant à celle de votre zone géographique. L'heure DST est désactivée par défaut.

Personnalisation de l'heure d'été traditionnelle des États-Unis (DST) :

- Si l'heure DST locale débute ou finit toujours à la quatrième occurrence d'un jour de semaine spécifique d'un mois (par exemple le quatrième dimanche), sélectionnez **Fourth/Last (Quatrième/Dernier)**. Dans les années qui suivent, si ce mois comprend éventuellement un cinquième dimanche, le paramètre d'heure change tout de même le quatrième dimanche.
- Si l'heure DST locale débute ou finit toujours à la dernière occurrence d'un jour de semaine spécifique d'un mois, que cette occurence soit la quatrième ou la cinquième, sélectionnez **Fifth/Last (Cinquième/Dernier)**.

Format

Chemin d'accès : Administration > General > Date & Time > date format

Sélectionne le format numérique auquel toutes les dates seront affichées dans l'interface utilisateur. Chaque lettre de ces formats (m pour mois, d pour jour et y pour année) représente un chiffre. Les jours et les mois calendaires à un seul chiffre sont affichés en deux chiffres commençant par un zéro.

Utilisation d'un fichier .ini

Chemin d'accès : Administration > General > User Config File

Permet d'utiliser les paramètres d'une PDU en rack pour en configurer une autre. Récupérez le fichier config.ini de la PDU en rack configurée, personnalisez ce fichier (par exemple en modifiant l'adresse IP) et téléchargez-le sur la nouvelle PDU en rack. Le nom du fichier peut contenir jusqu'à 64 caractères et doit avoir l'extension .ini.

État	Progression du téléchargement. Le téléchargement réussit même si le fichier contient des erreurs ; dans ce cas, un événement système signale les erreurs dans le journal de consignation des événements.
Télécharger	Naviguez jusqu'au fichier personnalisé et téléchargez-le afin que la PDU en rack l'utilise pour effectuer sa propre configuration.

Pour récupérer le fichier d'une PDU en rack configurée et le personnaliser, consultez Exportation des paramètres de configuration.

Au lieu de télécharger le fichier vers une seule PDU en rack, vous pouvez l'exporter vers plusieurs PDU en rack en utilisant un sript FTP ou SCP.

Journal de consignation des événements et unités de température

Chemin d'accès : Administration > General > Preferences

Code couleur du journal de consignation des événements

Cette option est désactivée par défaut. Cochez la case de l'option **Event Log Color Coding (Code couleur du journal de consignation des événements)** pour activer le codage couleur du texte d'alarme enregistré dans le journal de consignation des événements. Les entrées d'événements système et de modifications de la configuration ne changent pas de couleur.

Couleur du texte	Gravité de l'alarme
Rouge	**Critique** : une alarme critique existe et nécessite une action immédiate.
Orange	**Avertissement** : une alarme nécessite votre attention et pourrait mettre en péril vos données ou votre équipement si le problème n'est pas corrigé.
Vert	**Alarme arrêtée** : les conditions ayant déclenché l'alarme se sont améliorées.
Noir	**Normal :** aucune alarme. La PDU en rack et tous les périphériques connectés fonctionnent normalement.

Modification de l'échelle de température par défaut

Sélectionnez l'échelle de température (Fahrenheit ou Celsius) dans laquelle s'afficheront les mesures de température dans cette interface utilisateur.

Réinitialisation de la PDU en rack

Chemin d'accès : Administration > General > Reset/Reboot

Action	Définition
Reboot Management Interface (Redémarrer l'interface de gestion)	Redémarre l'interface de la PDU en rack.
Reset All (Réinitialiser tout)[1]	Décochez la case **Exclude TCP/IP** pour réinitialiser tous les paramètres de configuration ; cochez la case **Exclude TCP/IP** pour réinitialiser tous les paramètres sauf le paramètre TCP/IP.
Reset Only (Réinitialiser uniquement)[1]	**TCP/IP settings (Paramètres TCP/IP)** : cette option permet de définir la configuration TCP/IP sur **DHCP & BOOTP** (paramètre par défaut), qui requiert que la PDU en rack reçoive ses paramètres TCP/IP d'un serveur DHCP ou BOOTP. Voir Paramètres TCP/IP et de communication.
	Event configuration (Configuration de l'événement) : toutes les modifications de configuration des événements, par événement et par groupe, sont rétablies à leurs paramètres par défaut.
	RPDU to Defaults (Restauration des valeurs par défaut de la PDU en rack) : rétablit les valeurs par défaut uniquement pour les paramètres de laPDU en rack, mais pas pour les paramètres réseau.
1. La réinitialisation peut prendre jusqu'à 1 minute.	

Configuration des liens

Chemin d'accès : Administration > General > Quick Links

Sélectionnez l'onglet **Administration** puis **General** dans la barre de menu supérieure, et **Quick Links (Liens rapides)** dans le menu de navigation gauche afin de consulter et de modifier les liens URL affichés en bas à gauche de chaque page de l'interface.

Par défaut, ces liens donnent accès aux pages Web suivantes :

- **Link 1** : dell.com
- **Link 2** : dell.com/home
- **Link 3 :** dell.com/business

Pour reconfigurer les liens ci-dessous, cliquez sur le nom du lien dans la colonne **Display (Affichage)** :

- **Display (Affichage)** : nom abrégé du lien affiché sur chaque page de l'interface.
- **Name (Nom)** : nom qui identifie entièrement la cible ou l'objet du lien
- **Address (Adresse)** : sous forme d'URL, par exemple l'URL d'un autre périphérique ou serveur.

À propos de la PDU en rack

Chemin d'accès : Administration > General > About

Les informations sur le matériel sont utiles pour résoudre des problèmes concernant la PDU en rack. Le numéro de série et l'adresse MAC figurent également sur la PDU en rack elle-même.

Les informations relatives au microprogramme du module d'application, au système d'exploitation Dell (AOS), et au contrôleur de démarrage indiquent le nom, la version du microprogramme et la date et l'heure de création de chaque module du microprogramme. Ces informations sont également utiles pour un dépannage.

Management Uptime (Autonomie de gestion) indique depuis combien de temps l'interface fonctionne de manière continue.

Exportation des paramètres de configuration

Récupération et exportation du fichier .ini

Récapitulatif de la procédure

Un Administrateur peut récupérer le fichier .ini d'une PDU en rack et l'exporter vers une autre PDU en rack ou plusieurs PDU en rack.

1. Configurez une PDU en rack avec les paramètres que vous souhaitez exporter.
2. Récupérez le fichier .ini de cette PDU en rack.
3. Personnalisez le fichier en modifiant au moins les paramètres TCP/IP.
4. Utilisez un protocole de transfert de fichiers pris en charge par la PDU en rack pour transférer une copie du fichier vers une autre PDU en rack ou plusieurs. Pour un transfert vers plusieurs PDU en rack, utilisez un script FTP ou SCP

Chaque PDU en rack destinataire utilise le fichier pour reconfigurer ses propres paramètres, puis le supprime.

Contenu du fichier .ini

Le fichier config.ini que vous récupérez d'une PDU en rack contient les informations suivantes :

- des *en-têtes de section* et des *mots-clés* (uniquement ceux pris en charge par le périphérique duquel provient le fichier récupéré) *:* les en-têtes de section sont des noms de catégories entre crochets ([ ]). Les mots-clés, sous chaque en-tête de section, sont des étiquettes qui décrivent les paramètres spécifiques de la PDU en rack. Chaque mot-clé est suivi du signe « égal » et d'une valeur (valeur par défaut ou valeur configurée).

- le mot-clé pour **`Override`** : avec sa valeur par défaut, ce mot-clé interdit l'exportation d'un ou de plusieurs mots-clés et de leurs valeurs spécifiques vers le périphérique concerné. Par exemple dans la section **`[NetworkTCP/IP]`**, la valeur par défaut en **`Override`** (l'adresse MAC de la PDU en rack) bloque l'exportation des valeurs **`SystemIP`**, **`SubnetMask`**, **`DefaultGateway`** et **`BootMode`**.

Procédures détaillées

Récupération. Pour configurer et récupérer un fichier .ini à exporter :

1. Si possible, utilisez l'interface d'une PDU en rack pour la configurer avec les paramètres à exporter. Modifier directement le fichier .ini risque d'introduire des erreurs.
2. Pour utiliser le protocole FTP afin de récupérer le fichier config.ini de la PDU en rack configurée :
   a. Ouvrez une connexion avec la PDU en rack en utilisant son adresse IP :

      `ftp> open` ***`adresse_ip`***

   b. Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.
   c. Récupérez le fichier config.ini contenant les paramètres de la PDU en rack :

      `ftp> get` ***`config.ini`***

      Le fichier est alors copié dans le dossier depuis lequel vous avez lancé le protocole FTP.

Personnalisation. Avant d'exporter le fichier, vous devez le personnaliser.

1. Pour cela, utilisez un éditeur de texte.
   - Les en-têtes de section, les mots-clés et les valeurs prédéfinies ne sont pas sensibles à la casse, mais les valeurs de chaîne que vous définissez le sont.
   - Utilisez des guillemets accolés pour indiquer une absence de valeur. Par exemple, **`LinkURL1=""`** indique que l'URL est volontairement non définie.
   - Mettez entre guillemets toute valeur qui contient un espace à sa gauche ou à sa droite, ou qui est déjà entre guillemets.
   - Pour exporter des événements planifiés, configurez les valeurs directement dans le fichier .ini.
   - Pour exporter une heure système avec la plus grande précision possible, si les PDU en rack destinataires peuvent accéder à un serveur NTP, configurez le paramètre **`NTPEnable`** sur **`enabled`** (activé) :

     `NTPEnable=enabled`

     Vous pouvez aussi réduire le temps de transmission en exportant la section **`[SystemDate/Time]`** dans un fichier .ini séparé.
   - Pour ajouter des commentaires, commencez chaque ligne de commentaire par un point-virgule (`;`).
2. Copiez le fichier personnalisé dans le même dossier sous un nom différent :
   - Le nom du fichier peut contenir jusqu'à 64 caractères et doit avoir l'extension .ini.
   - Conservez le fichier personnalisé initial pour utilisation future. **Le fichier que vous conservez constitue le seul enregistrement de vos commentaires.**

Transfert du fichier vers une seule PDU en rack. Pour transférer le fichier .ini vers une autre PDU en rack, procédez selon l'une des méthodes suivantes :

- À partir de l'interface Web de la PDU en rack destinataire, sélectionnez l'onglet **Administration** puis **General** dans la barre de menu supérieure, et enfin **User Config File (Fichier de configuration utilisateur)** dans le menu de navigation gauche. Entrez le chemin complet, ou utilisez la commande **Parcourir...**.
- Utilisez un protocole de transfert de fichiers pris en charge par les PDU en rack (FTP, Client FTP, SCP ou TFTP). Les exemples suivants utilisent le protocole FTP :
  a. Depuis le dossier contenant la copie du fichier .ini personnalisé, utilisez FTP pour vous connecter à la PDU en rack vers laquelle vous exportez le fichier .ini :

     ```
     ftp> open adresse_ip
     ```

  b. Exportez le fichier .ini personnalisé vers le répertoire racine de la PDU en rack de destination :

     ```
     ftp> put nom_fichier.ini
     ```

Exportation du fichier vers plusieurs PDU en rack. Pour exporter le fichier .ini vers plusieurs PDU en rack, utilisez FTP ou SCP en rédigeant un script qui incorpore et répète les étapes utilisées pour exporter ce fichier vers une seule PDU en rack.

Événements de téléchargement et messages d'erreur

Événement et messages d'erreurs correspondants

L'événement suivant survient quand la PDU en rack destinataire achève l'utilisation du fichier .ini pour mettre à jour ses paramètres.

`Configuration file upload complete, with` *`number`* `valid values`

Si un mot-clé, un nom de section ou une valeur est non valide, le téléchargement par la PDU en rack destinataire réussit et un texte supplémentaire sur l'événement signale l'erreur.

Texte sur l'événement	Description
Configuration file warning (Avertissement au niveau du fichier de configuration) : Invalid keyword on line *number* (mot clé non valide à la ligne *numéro*). Configuration file warning (Avertissement au niveau du fichier de configuration) : Invalid value on line *number* (valeur non valide à la ligne *numéro*).	Toute ligne contenant un mot-clé ou une valeur non valide est ignorée.
Configuration file warning (Avertissement au niveau du fichier de configuration) : Invalid section on line *number.* (section non valide à la ligne *numéro*).	Si un nom de section est non valide, toutes les paires de mots-clés/valeurs de cette section sont ignorées.

Texte sur l'événement	Description
Configuration file warning (Avertissement au niveau du fichier de configuration) : Keyword found outside of a section on line *number* (un mot clé se trouve hors de la section à la ligne *numéro*).	Un mot-clé entré au début du fichier (c'est-à-dire avant tout en-tête de section) est ignoré.
Configuration file warning (Avertissement au niveau du fichier de configuration) : Configuration file exceeds maximum size (le fichier de configuration dépasse la taille maximale).	Un fichier trop volumineux provoque un téléchargement incomplet. Réduisez la taille du fichier, ou divisez-le en deux fichiers et tentez de nouveau le téléchargement.

Messages dans le fichier config.ini

Une PDU en rack depuis laquelle vous téléchargez le fichier config.ini file doit être détectée avec succès pour que sa configuration soit prise en compte. Si la PDU en rack est absente ou n'est pas détectée, le fichier config.ini contient un message sous le nom de section approprié, au lieu des mots-clés et des valeurs. Par exemple :

```
Rack PDU not discovered
```

Si vous n'aviez pas l'intention d'exporter la configuration de la PDU en rack comme partie de l'importation du fichier .ini file, ignorez ces messages.

Erreurs générées par les valeurs ignorées

Le mot-clé **`Override`** et sa valeur vont générer des messages d'erreur dans le journal de consignation des événements lorsqu'il bloque l'exportation des valeurs.

Consultez Contenu du fichier .ini pour des informations sur les valeurs qui sont ignorées.

Les valeurs ignorées étant spécifiques à chaque périphérique et inappropriées pour l'exportation vers d'autres PDU en rack, ignorez ces messages d'erreur. Pour éviter ces messages d'erreur, supprimez les lignes contenant le mot-clé **`Override`** et celles contenant les valeurs qu'elles ignorent. Ne supprimez pas et ne modifiez pas la ligne contenant l'en-tête de section.

Transferts de fichiers

Mise à niveau du microprogramme

Avantages de la mise à niveau du microprogramme

Lorsque vous effectuez la mise à niveau du microprogramme de la PDU en rack :

- Vous obtenez les corrections et améliorations les plus récentes.
- De nouvelles fonctions sont immédiatement disponibles.

En maintenant à jour les versions du microprogramme sur tout votre réseau, toutes les PDU en rack prendront bien en charge les mêmes fonctions de la même manière.

Fichiers de microprogramme

Une version de microprogramme comprend trois modules : un module Operating System (AOS), un module d'application et un module de contrôleur de démarrage (bootmon). Chaque module contient un ou plusieurs contrôle(s) par redondance cyclique (CRC) pour éviter que ses données soient corrompues pendant le transfert.

Les fichiers des modules Operating System (AOS), d'application et de contrôleur de démarrage utilisés avec la PDU en rack possèdent le même format de base :

dell_version-matériel_type_version_microprogramme.bin

- **dell** : indique qu'il s'agit d'un fichier Dell.
- ***version-matériel*** **:** **hw0***x* identifie la version du matériel sur lequel ce fichier binaire est utilisable.
- ***type*** **:** identifie si le fichier est le module Operating System (AOS), le module d'application ou le module de contrôleur de démarrage de la PDU en rack.
- ***version*** **:** numéro de version du fichier.
- **bin** : indique qu'il s'agit d'un fichier binaire.

Consultez À propos de la PDU en rack pour vérifier le numéro de version de chaque module de microprogramme sur une PDU en rack.

Méthodes de transfert des fichiers de microprogramme

Pour mettre à niveau le microprogramme d'une PDU en rack, utilisez l'une des méthodes suivantes :

- À partir d'un ordinateur relié au réseau et fonctionnant sous un système d'exploitation pris en charge, utilisez le protocole FTP ou SCP pour transférer les modules AOS et d'application individuels.
- Pour une PDU en rack se trouvant hors réseau, utilisez XMODEM par l'intermédiaire d'une connexion série pour transférer les modules de microprogramme depuis votre ordinateur vers la PDU en rack.

lorsque vous transférez des modules de microprogramme individuels, **vous devez** transférer le module Operating System (AOS) vers la PDU en rack avant de transférer le module d'application.

Utilisation du protocole FTP ou SCP pour mettre à niveau une PDU en rack

FTP. Pour utiliser FTP afin de mettre à niveau une PDU en rack sur le réseau, procédez comme suit :

- La PDU en rack doit être connectée au réseau, et son adresse IP système, son masque de sous-réseau et sa passerelle par défaut doivent être configurés.
- Le serveur FTP doit être activé au niveau de la PDU en rack.
- Les fichiers de microprogramme doivent avoir été téléchargés depuis le site Dell.com.

Pour transférer les fichiers :

1. Sur un ordinateur relié au réseau, ouvrez une fenêtre d'invite de commande. Accédez au répertoire qui contient les fichiers du microprogramme, ainsi que la liste des fichiers :

   ```
   C:\>cd\dell
   C:\dell>dir
   ```

   Pour les fichiers répertoriés, *xxx* représente le numéro de version du microprogramme :

   - **dell_hw05_aos_*xxx*.bin**
   - **dell_hw05_application_*xxx*.bin**

2. Ouvrez une session client FTP :

   ```
   C:\dell>ftp
   ```

3. Tapez **open** et l'adresse IP de la PDU en rack puis appuyez sur ENTRÉE. Si le paramètre **port** du serveur FTP n'est plus configuré sur la valeur par défaut (**21**), vous devez utiliser la valeur qui lui a été attribuée au niveau de la commande FTP.
   - Pour les clients Windows FTP, séparez le numéro d'un port autre que le port par défaut et l'adresse IP par un espace. Par exemple :
     ftp> open 150.250.6.10 21000
   - Certains clients FTP requièrent le signe deux points (:) au lieu d'un espace avant le numéro de port.
4. Connectez-vous en tant qu'Administrateur : **admin** est la valeur par défaut pour le nom d'utilisateur et le mot de passe.
5. Mettez à niveau l'AOS (dans notre exemple, *xxx* représente le numéro de version du microprogramme) :

   ```
   ftp> bin
   ftp> put dell_hw05_aos_xxx.bin
   ```

6. Lorsque le protocole FTP confirme le transfert, tapez **quit** (quitter) pour fermer la session.
7. Attendez 20 secondes et répétez les étapes 2 à 5. À l'étape 5, utilisez le nom de fichier du module d'application.

SCP. Pour utiliser Secure CoPy (SCP) pour mettre à niveau le microprogramme de la PDU en rack :

1. identifiez et situez les modules de microprogramme décrits dans les précédentes instructions relatives au protocole FTP.
2. Utilisez une ligne de commande SCP pour transférer le module du microprogramme d'AOS vers la PDU en rack. L'exemple suivant utilise *xxx* pour représenter le numéro de version du module AOS :

   ```
   scp dell_hw05_aos_xxx.bin
   dell@158.205.6.185:dell_hw05_aos_xxx.bin
   ```

3. Utilisez une ligne de commande SCP similaire, contenant le nom du module d'application, pour transférer le module de microprogramme d'application vers la PDU en rack.

Mise à niveau de plusieurs PDU en rack

Utilisez FTP ou SCP pour mettre à niveau plusieurs PDU en rack. Pour mettre à niveau plusieurs PDU en rack à l'aide d'un client FTP ou du protocole SCP, écrivez un script qui permette d'effectuer automatiquement la procédure.

Utilisation du protocole XMODEM pour mettre à niveau une PDU en rack

Pour utiliser XMODEM pour mettre à niveau une PDU en rack hors réseau, vous devez d'abord télécharger les fichiers du microprogramme depuis le site Dell.com.

Pour transférer les fichiers :

1. Sélectionnez un port série au niveau de l'ordinateur local et désactivez tout service utilisant ce port.
2. Connectez le câble série fourni au port choisi sur l'ordinateur et au port série de la PDU en rack.
3. Exécutez un programme d'émulation de terminal (tel que HyperTerminal) et configurez le port sélectionné sur 57600 bits/s, 8 bits de données, sans parité, 1 bit d'arrêt et sans contrôle de flux.
4. Appuyez sur le bouton RESET [Réinitialisation] de la PDU en rack puis immédiatement deux fois sur la touche ENTRÉE, ou jusqu'à ce que l'invite du contrôleur de démarrage affiche : **`BM>`**
5. Saisissez **`XMODEM`** et appuyez sur ENTRÉE.
6. Dans le menu du programme d'émulation de terminal, sélectionnez XMODEM puis le fichier de microprogramme AOS binaire à transférer avec XMODEM. Lorsque le transfert XMODEM est terminé, l'invite du contrôleur de démarrage s'affiche de nouveau.
7. Pour installer le module d'application, répétez les étapes 5 et 6. À l'étape 6, utilisez le nom de fichier du module d'application.
8. Tapez **`reset`** ou appuyez sur le bouton Reset pour redémarrer la PDU en rack.

Pour plus d'informations sur le format utilisé pour les modules de microprogrammes, consultez Fichiers de microprogramme.

Contrôle des mises à niveau et des mises à jour

Vérification du succès ou de l'échec du transfert

Pour vérifier si une mise à niveau de microprogramme a réussi, utilisez la commande **`xferStatus`** dans l'interface par lignes de commande pour consulter le résultat du dernier transfert, ou une commande SNMP GET pour l'OID **mfiletransferStatusLastTransferResult**.

Codes des résultats du dernier transfert

Code	Description
Successful	Le transfert du fichier a réussi.
Result not available	Aucun transfert de fichier n'a été enregistré.
Failure unknown	Le dernier transfert de fichier a échoué pour un motif inconnu.
Server inaccessible	Le serveur TFTP ou FTP n'a pas pu être détecté sur le réseau.
Server access denied	L'accès au serveur TFTP ou FTP a été refusé.
File not found	Le serveur TFTP ou FTP n'a pas pu localiser le fichier spécifié.
File type unknown	Le fichier a été téléchargé mais son contenu n'a pu être identifié.
File corrupt	Le fichier a été téléchargé mais au moins un contrôle par redondance cyclique (CRC) est erroné.

Vérification des numéros de version des microprogrammes installés

Utilisez l'interface Web pour vérifier les versions des modules de microprogrammes mis à niveau en sélectionnant l'onglet **Administration** puis **General** dans la barre de menu supérieure, et **About (À propos de)** dans le menu de navigation gauche, ou bien utilisez une commande SNMP GET pour l'OID **sysDescr** MIB II. Dans l'interface par lignes de commande, utilisez la commande **`about`**.

Dépannage

PDU en rack - Problème d'accès

Problème	Solution
Impossible d'exécuter la commande ping sur la PDU en rack	Si le témoin d'état de la PDU en rack est vert, essayez un test Ping sur un nœud différent du même segment de réseau que celui de la PDU en rack. En cas d'échec, le problème ne vient pas de la PDU en rack. Si le témoin d'état n'est pas vert ou si le test ping réussit, procédez aux vérifications suivantes : • Vérifiez toutes les connexions réseau. • Vérifiez les adresses IP de la PDU en rack et du NMS. • Si le NMS se trouve sur un réseau (ou un sous-réseau) physique différent de celui de la PDU en rack, vérifiez l'adresse IP de la passerelle par défaut (ou du routeur). • Vérifiez le nombre de chiffres du masque de sous-réseau de la PDU en rack.
Impossible d'allouer le port de communication par l'intermédiaire d'un programme de terminal	Avant de pouvoir utiliser un programme de terminal pour configurer la PDU en rack, vous devez fermer tous les services, programmes ou applications qui utilisent le port de communication.
Impossible d'accéder à l'interface par lignes de commande par l'intermédiaire d'une connexion série	Assurez-vous que vous n'avez pas modifié la vitesse de transmission. Essayez 2400, 9600, 19200 ou 38400.

Problème	Solution
Impossible d'accéder à distance à l'interface par lignes de commande	• Assurez-vous que vous utilisez la méthode d'accès correcte, Telnet ou Secure Shell (SSH). Un Administrateur peut activer ces méthode d'accès. Par défaut, le protocole Telnet est activé. L'activation de SSH provoque la désactivation automatique de Telnet. • Pour SSH, la PDU en rack peut être en train de créer une clé d'hôte. La PDU en rack peut prendre jusqu'à une minute pour créer la clé d'hôte ; pendant ce temps, SSH est inaccessible.
Impossible d'accéder à l'interface Web	• Vérifiez que l'accès HTTP ou HTTPS est activé. • Assurez-vous que vous spécifiez l'URL correcte (cohérente avec le système de sécurité utilisé par la PDU en rack). Le protocole SSL requiert de taper **https**, et non pas **http**, au début de l'URL. • Vérifiez que vous pouvez effectuer un test Ping sur la PDU en rack. • Vérifiez que vous utilisez un navigateur Web pris en charge par la PDU en rack. Voir Navigateurs Web pris en charge. • Si la PDU en rack vient juste de redémarrer et que la sécurité SSL est en cours de configuration, il se peut que la PDU en rack soit en train de créer un certificat de serveur. La PDU en rack peut prendre jusqu'à une minute pour créer ce certificat ; pendant ce temps, le serveur SSH est inaccessible.

Annexe A : Liste des commandes acceptées

Description des commandes de la carte de gestion réseau

```
?
about
alarmcount
    [-p [all | warning | critical]]
boot
    [-b <dhcpBootp | dhcp | bootp | manual>]
    [-a <remainDhcpBootp | gotoDhcpOrBootp>]
    [-o <stop | prevSettings>]
    [-f <nombre de tentatives sans succès>]
    [-c <cookie dhcp> [enable | disable]]
    [-s <nombre de tentatives suivies d'abandon>]
    [-v <catégorie de fournisseur>]
    [-i <id client>]
    [-u <catégorie d'utilisateur>]
cd
console
    [-S<disable | telnet | ssh>]
    [-pt <n° de port telnet>]
    [-ps <n° de port SSH>]
    [-b <2400 | 9600 | 19200 | 38400>]
date
    [-d <“chaîne de date”>]
    [-t <00:00:00>]
    [-f [mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd]]
delete
dir
dns
    [-OM <enable | disable>]
    [-p <serveur DNS primaire>]
    [-s <serveur DNS secondaire>]
    [-d <nom de domaine>]
    [-n <nom de domaine IPv6>]
    [-h <nom d'hôte>]
eventlog
exit
format
```

ftp
    [-p <numéro du port>]
    [-S <enable | disable>]
help
netstat
ntp
    [-OM <enable | disable>]
    [-p <serveur NTP primaire>]
    [-s <serveur NTP secondaire>]
ping
    [<adresse IP ou nom DNS>]
portspeed
    [-s [auto | 10H | 10F | 100H | 100F]]
prompt
    [-s [long | short]]
quit
radius
    [-a <accès> [local | radiusLocal | radius]]
    [-p# <IP du serveur>]
    [-s# <secret du serveur>]
    [-t# <délai de temporisation du serveur>]
reboot
resetToDef
    [-p <all | keepip>]
snmp, snmpv3
    [-S <enable | disable>]
system
    [-n <nom système>]
    [-c <personne à contacter>]
    [-l <emplacement du système>]
tcpip
    [-i <adresse IP>]
    [-s <masque de sous-réseau>]
    [-g <passerelle>]
    [-d <nom de domaine>]
    [-h <nom d'hôte>]
tcpip6
    [-S <enable | disable>]
    [-man <enable | disable>]
    [-auto <enable | disable>]
    [-i <adresse IPv6>]
    [-g <passerelle IPv6>]
    [-d6 <router | stateful | stateless | never>]

user
[-an <nom d'administrateur>]
[-dn <nom d'utilisateur du périphérique>]
[-rn <nom d'utilisateur en lecture seule>]
[-ap <mot de passe administrateur>]
[-dp <mot de passe utilisateur de périphérique>]
[-rp <mot de passe utilisateur en lecture seule>]
[-t <délai d'inactivité en minutes>]

web
[-S <disable | http | https>]
[-ph <numéro de port http>]
[-ps <numéro de port https>]

xferINI

xferStatus

Description des commandes du périphérique

devLowLoad
[<puissance>]

devNearOver
[<puissance>]

devOverLoad
[<puissance>]

devReading
[<“power” | “energy”>]

devStartDly

humLow
[<humidité>]

humMin
[<humidité>]

humReading

inNormal

inReading

olAssignUsr
[<“all” | nom de la sortie | numéro de la sortie > <utilisateur>]

olCancelCmd
[<“all” | nom de la sortie | numéro de la sortie >]

olDlyOff
[<“all” | nom de la sortie | numéro de la sortie >]

olDlyOn
[<“all” | nom de la sortie | numéro de la sortie >]

olDlyReboot
[<“all” | nom de la sortie | numéro de la sortie >]

olGroups

olLowLoad
[<“all” | nom de la sortie | numéro de la sortie > <puissance>]
olName
[<“all” | numéro de la sortie > <nouveau nom>]
olNearOver
[<“all” | nom de la sortie | numéro de la sortie > <puissance>]
olOff
[<“all” | nom de la sortie | numéro de la sortie >]
olOffDelay
[<“all” | nom de la sortie | numéro de la sortie > <durée>]
olOn
[<“all” | nom de la sortie | numéro de la sortie >]
olOnDelay
[<“all” | nom de la sortie | numéro de la sortie > <durée>]
olOverLoad
[<“all” | nom de la sortie | numéro de la sortie > <puissance>]
olRbootTime
[<“all” | nom de la sortie | numéro de la sortie > <durée>]
olReading
[<“all” | nom de la sortie | numéro de la sortie > <current | power | energy>]
olReboot
[<“all” | nom de la sortie | numéro de la sortie >]
olStatus
[<“all” | nom de la sortie | numéro de la sortie >]
olUnasgnUsr
[<“all” | nom de la sortie | numéro de la sortie > <utilisateur>]
phLowLoad
[<“all” | numéro de phase> <courant>]
phNearOver
[<“all” | numéro de phase> <courant>]
phOverLoad
[<“all” | numéro de phase> <courant>]
phReading
[<“all” | numéro de phase> <“current” | “voltage” | “power”>]
phRestrictn
[<“all” | numéro de phase> <none | near | over>]
prodInfo
tempHigh
[<“F” | “C”> <température>]
tempMax
[<“F” | “C”> <température>]
tempReading
[<“F” | “C”>]

userAdd
    [<nouvel utilisateur>]
userDelete
    [<utilisateur>]
userList
userPasswd
    [<utilisateur> <nouveau mot de passe> <nouveau mot de passe>]
whoami

Annexe B : Guide de sécurité

Contenu et objet de cette annexe

Cette annexe répertorie les fonctions de sécurité de la version 5.*x.x* du microprogramme des PDU en rack Dell®, qui permet à ces PDU en rack de fonctionner à distance sur le réseau.

Cette annexe détaille les fonctions et protocoles ci-dessous, indique comment sélectionner ceux qui sont appropriés à votre propre situation et la manière de les configurer et de les utiliser dans un système de sécurité global :

- Telnet et Secure Shell (SSH)
- Secure Sockets Layer (SSL)
- RADIUS
- SNMPv1 et SNMPv3

En outre, cette annexe décrit la manière d'utiliser l'Assistant de sécurité de la PDU en rack pour créer les composants requis pour la sécurité de haut niveau fournie par les protocoles SSL et SSH.

Fonctions de sécurité

Protection des mots de passe et des clés

Aucun mot de passe ni aucune clé n'est enregistré sur la PDU en rack en simple texte.

- Les mots de passe sont scindés à l'aide d'un algorithme de hachage dans un sens.
- Les clés, utilisées pour l'authentification et le cryptage, sont codées avant leur enregistrement sur la PDU en rack.

Présentation succincte des méthodes d’accès

Accès série à l'interface par lignes de commande.

Accès sécurisé	Description
Accès par le nom d'utilisateur et le mot de passe.	Toujours activé.

Accès à distance à l'interface par lignes de commande.

Accès sécurisé	Description
Méthodes disponibles : • Nom d'utilisateur et mot de passe • Port du serveur sélectionnable • Protocoles d'accès pouvant être activés ou désactivés • Secure Shell (SSH)	Pour une haute sécurité, utilisez SSH. • Avec le protocole Telnet, le nom d’utilisateur et le mot de passe sont transmis en simple texte. • L'activation du protocole SSH désactive Telnet et fournit un accès crypté à l'interface par lignes de commande pour offrir une protection supplémentaire contre les tentatives d'interception, de contrefaçon ou d'altération des données au cours de leur transmission.

SNMPv1 et SNMPv3.

Accès sécurisé	Description
Méthodes disponibles (SNMPv1) : • Nom de communauté • Nom d'hôte • Filtres NMS IP • Agents pouvant être activés ou désactivés. • Quatre communautés d'accès avec fonction de lecture/écriture/ désactivation	Pour les deux méthodes SNMPv1 et SNMPv3, le nom d'hôte limite l'accès au NMS (système de gestion réseau) uniquement à cet emplacement, et les filtres NMS IP permettent uniquement l'accès aux NMS spécifiés par l'un des formats d'adresse IP des exemples suivants : • 159.215.12.1: Accès au NMS uniquement à l'adresse IP 159.215.12.1. • 159.215.12.255: Accès à tous les NMS sur le segment 159.215.12. • 159.215.255.255: Accès à tous les NMS sur le segment 159.215. • 159.255.255.255: Accès à tous les NMS sur le segment 159. • 0.0.0.0 ou 255.255.255.255 : Tous les NMS. SNMPv3 comprend des fonctions de sécurité supplémentaires, notamment : • Clé d'authentification permettant de garantir que le NMS qui tente d'accéder à la PDU en rack est bien le NMS qu'il prétend être. • Cryptage des données au cours de la transmission, avec une clé de confidentialité requise pour le cryptage et le décryptage.
Méthodes disponibles (SNMPv3) : • Quatre profils utilisateur • Authentification par l'intermédiaire d'une clé d'authentification • Cryptage par l'intermédiaire d'une clé de confidentialité • Authentification SHA ou MD5 • Algorithme de cryptage AES ou DES • Filtres NMS IP	

Protocoles de transfert de fichiers.

Accès sécurisé	Description
Méthodes disponibles : • Nom d'utilisateur et mot de passe • Port du serveur sélectionnable • Serveur FTP et protocoles d'accès pouvant être activés ou désactivés • Secure CoPy (SCP)	Avec FTP, le nom d'utilisateur et le mot de passe sont transmis sous forme de simple texte, et les fichiers sont transférés sans cryptage. Utilisez SCP pour crypter le nom d'utilisateur, le mot de passe et les fichiers transférés, tels que les mises à jour de microprogramme, les fichiers de configuration, les fichiers journaux, les certificats Secure Sockets Layer (SSL) et les clés d'hôtes Secure Shell (SSH). Si vous utilisez SCP comme protocole de transfert de fichiers, activez SSH et désactivez FTP.

Serveur Web.

Accès sécurisé	Description
Méthodes disponibles : • Nom d'utilisateur et mot de passe • Port du serveur sélectionnable • Accès à l'interface Web pouvant être activés ou désactivés • Secure Sockets Layer (SSL)	En mode d'authentification HTTP simple, le nom d'utilisateur et le mot de passe sont transmis au moyen d'un code en 64 bits (sans cryptage). Le protocole SSL est disponible sur les navigateurs Internet compatibles avec la carte de gestion réseau ou un périphérique réseau ainsi que sur la plupart des serveurs Web. Le protocole Internet HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) permet de crypter et décrypter les demandes de pages au serveur Web et les pages que ce serveur renvoie à l'utilisateur.

RADIUS.

Accès sécurisé	Description
Méthodes disponibles : • Authentification centralisée des droits d'accès • Secret de serveur partagé entre le serveur RADIUS et la PDU en rack ou l'appareil	RADIUS (Remote Authentication Dial-In User Service) est un service d'authentification, d'autorisation et de comptabilisation utilisé pour gérer de manière centralisée l'accès à distance pour chaque PDU en rack (la PDU en rack prend en charge les fonctions d'authentification et d'autorisation).

Priorités d'accès

Les priorités d'accès suivantes s'appliquent, en ordre décroissant :

- Accès local à l'interface par lignes de commande depuis un ordinateur connecté directement en série à la PDU en rack.
- Accès Telnet ou Secure Shell (SSH) à l'interface par lignes de commande depuis un ordinateur distant.
- Accès Web.

Modification immédiate des noms d'utilisateurs et mots de passe par défaut

Après l'installation de la PDU en rack et sa configuration initiale, modifiez immédiatement les noms d'utilisateurs et les mots de passe par défaut en les remplaçant par des valeurs uniques afin d'établir une sécurité de base.

Affectations de ports

Si Telnet, le serveur FTP, SSH/SCP ou le serveur Web utilise un port non standard, un utilisateur doit spécifier le port dans la ligne de commande ou l'adresse Web utilisée pour accéder à la PDU en rack. Un numéro de port non standard offre un niveau de sécurité supplémentaire. Pour les protocoles, les ports sont initialement réglés sur les « ports bien connus » standard. Pour accroître la sécurité, redéfinissez les ports sur des numéros de port inutilisés compris entre 5001 et 32768 pour le serveur FTP et entre 5000 et 32768 pour les autres protocoles et serveurs (le serveur FTP utilise à la fois le port du numéro spécifié et celui du numéro immédiatement inférieur).

Noms d'utilisateur, mots de passe et noms de communauté avec SNMPv1

Tous les noms d'utilisateur, les mots de passe et les noms de communauté pour SNMPv1 sont transmis sur le réseau sous forme de simple texte. Un utilisateur capable de surveiller le trafic du réseau peut découvrir les noms d'utilisateur et les mots de passe requis pour se connecter aux comptes de l'interface par lignes de commande et de l'interface Web de la PDU en rack. Si votre réseau nécessite un niveau de sécurité plus élevé grâce aux options codées d'accès à l'interface par lignes de commande et à l'interface Web, désactivez l'accès à SNMPv1 ou réglez-le sur **Read** (Lecture) (l'accès **Read** permet de recevoir les informations d'état et d'utiliser les interruptions SNMPv1).

Pour désactiver l'accès SNMPv1, sous l'onglet **Administration**, sélectionnez **Network** (Réseau) dans la barre de menu supérieure et **access** sous l'en-tête **SNMPv1** du menu de navigation gauche. Décochez la case **Enable SNMPv1 access** (Activer l'accès SNMPv1) et cliquez sur **Apply**.

Pour régler l'accès SNMPv1 sur **Read** (Lecture), sous l'onglet **Administration**, sélectionnez **Network** (Réseau) dans la barre de menu supérieure et **access control** (contrôle d'accès) sous l'en-tête **SNMPv1** du menu de navigation gauche. Ensuite, pour chaque système de gestion réseau (NMS) configuré, cliquez sur les noms de communauté et réglez le type d'accès sur **Read**.

Authentification

Vous pouvez choisir pour la PDU en rack des fonctions de sécurité sans cryptage, qui permettent de contrôler l'accès par une authentification simple à l'aide de noms d'utilisateurs, de mots de passe et d'adresses IP. Ces fonctions de sécurité élémentaires sont suffisantes pour la plupart des environnements au sein desquels aucune donnée stratégique n'est transférée.

GET, SET et interruptions SNMP

Pour une meilleure authentification lorsque vous utilisez le protocole SNMP pour surveiller ou configurer la PDU en rack, choisissez SNMPv3. La clé d'authentification utilisée avec les profils utilisateurs SNMPv3 garantit que le système de gestion réseau (NMS) qui tente d'accéder à la PDU en rack est bien le NMS qu'il dit être, que le message n'a pas été modifié au cours de la transmission et n'a subi aucun retard, et qu'il n'a pas été copié puis renvoyé ultérieurement à une heure inappropriée. SNMPv3 est désactivé par défaut.

L'implémentation Dell du protocole SNMPv3 permet d'utiliser le protocole SHA-1 ou MD5 comme protocole d'authentification.

Interface Web et interface par lignes de commande

Pour s'assurer que les données et les communications entre la PDU en rack et les interfaces client (interface par lignes de commande et interface Web) ne puissent être interceptées, vous pouvez optimiser la sécurité en utilisant une ou plusieurs des méthodes de protection par cryptage suivantes :

- Pour l'interface Web, utilisez le protocole Secure Sockets Layer (SSL).
- Pour crypter les noms d'utilisateurs et les mots de passe d'accès à l'interface par lignes de commande, utilisez le protocole Secure SHell (SSH).
- Pour crypter les noms d'utilisateurs, les mots de passe et les données pour un transfert sécurisé des fichiers, utilisez le protocole Secure CoPy (SCP).

Pour plus d'informations sur les protocoles de sécurité codés, voir Cryptage.

Cryptage

GET, SET et interruptions SNMP

Pour une communication cryptée lorsque vous utilisez le protocole SNMP pour surveiller ou configurer la PDU en rack, choisissez SNMPv3. La clé de confidentialité utilisée avec les profils utilisateurs SNMPv3 garantit la confidentialité des données par cryptage (à l'aide de l'algorithme de cryptage AES ou DES) qu'un NMS envoie à la PDU en rack ou reçoit de cet appareil.

Protocoles Secure Shell (SSH) et Secure CoPy (SCP) pour l'interface par lignes de commande

Protocole Secure Shell. Le protocole SSH offre un mécanisme sécurisé d'accès à distance aux consoles d'ordinateur (*dites « shells »*). Le protocole authentifie le serveur (dans le cas présent la PDU en rack) et crypte toutes les transmissions entre le client SSH et le serveur.

- SSH est une alternative à sécurité élevée à Telnet. Le protocole Telnet n'utilise pas de cryptage.
- SSH empêche le nom d'utilisateur et le mot de passe, qui sont les informations d'authentification, d'être utilisés par quiconque intercepterait le trafic réseau.
- Pour authentifier le serveur SSH (la PDU en rack) auprès du client SSH, le protocole SSH utilise une clé d'hôte unique pour le serveur SSH. La clé d'hôte est une identification infalsifiable. Elle empêche un serveur non valide situé sur le réseau d'obtenir un nom d'utilisateur et un mot de passe en se présentant comme un serveur valide.

Pour des informations sur les applications de client SSH prises en charge, consultez Telnet et Secure Shell (SSH). Pour créer une clé d'hôte, consultez Création d'une clé d'hôte SSH.

- La PDU en rack prend en charge le protocole SSH version 2, qui fournit une protection contre les tentatives d'interception, de contrefaçon ou d'altération des données au cours de leur transmission.
- Lorsque vous activez le protocole SSH, Telnet est automatiquement désactivé.
- L'interface, les comptes utilisateur et les droits d'accès utilisateur sont les mêmes pour un accès à l'interface par lignes de commande par protocole SSH ou Telnet.

Secure CoPy. SCP est une application de transfert de fichiers sécurisée que vous pouvez utiliser à la place du protocole FTP. SCP utilise le protocole SSH comme protocole de transport sous-jacent pour le cryptage des noms d'utilisateurs, des mots de passe et des fichiers.

- Lorsque vous activez et configurez le protocole SSH, vous activez et configurez automatiquement le protocole SCP. Aucune configuration supplémentaire du protocole SCP n'est requise.
- Vous devez explicitement désactiver le protocole FTP. Celui-ci n'est pas désactivé lorsque vous activez le protocole SSH. Pour désactiver FTP, dans l'onglet **Administration**, sélectionnez **Network** (Réseau) dans la barre de menus supérieure, puis l'option **FTP Server** dans le menu de navigation gauche. Décochez la case **Enable** (Activer) et cliquez sur **Apply**.

Protocole Secure Sockets Layer (SSL) pour l'interface Web

Pour une communication Web sécurisée, activez le protocole Secure Sockets Layer (SSL) en sélectionnant HTTPS comme mode de protocole à utiliser pour accéder à l'interface Web de la PDU en rack. Le protocole HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) est un protocole Web qui crypte et décrypte les demandes de pages effectuées par l'utilisateur et les pages renvoyées à l'utilisateur par le serveur Web.

La PDU en rack prend en charge SSL version 3.0 et le protocole associé Transport Layer Security (TLS) version 1.0. La plupart des navigateurs permettent de sélectionner la version SSL à activer.

Lorsque le protocole SSL est activé, votre navigateur affiche une petite icône représentant un cadenas.

Le protocole SSL utilise un certificat numérique pour permettre au navigateur d'authentifier le serveur (dans le cas présent, la PDU en rack). Le navigateur vérifie les points suivants :

- Le format du certificat du serveur est correct.
- La date et l'heure d'expiration du serveur ne sont pas dépassées.
- Le nom DNS ou l'adresse IP spécifiés lorsqu'un utilisateur se connecte correspondent au nom commun mentionné dans le certificat du serveur.
- Le certificat du serveur est signé par une autorité de certification de confiance.

Les navigateurs des principaux concepteurs contiennent en magasin (cache) des certificats racine CA de l'autorité de certification commerciale afin de leur permettre de comparer la signature du certificat du serveur et celle d'un certificat racine CA.

Vous pouvez utiliser l'Assistant de sécurité de la PDU en rack pour créer une demande de signature par certificat auprès d'une autorité de certification extérieure ou, si vous ne souhaitez pas utiliser une autorité de certification existante, créer un certificat racine Dell et le télécharger dans le magasin de certificats (cache) du navigateur. Vous pouvez également utiliser l'assistant pour créer un certificat de serveur à télécharger sur la PDU en rack.

Consultez Création et installation de certificats numériques pour un récapitulatif des modes d'utilisation de ces certificats.
Pour créer des certificats et des demandes de certificats, voir Création d'un certificat racine et de certificats de serveur et Création d'un certificat de serveur et d'une demande de signature.

Le protocole SSL utilise aussi divers algorithmes et méthodes de cryptage pour authentifier le serveur, crypter les données ainsi que pour garantir leur intégrité, c'est-à-dire garantir qu'elles n'ont pas été interceptées et envoyées par un autre serveur.

Les pages Web que vous avez récemment consultées sont enregistrées dans la mémoire cache de votre navigateur Web. Cela permet de revenir sur ces pages ultérieurement sans nécessité d'entrer à nouveau votre nom d'utilisateur et votre mot de passe. Fermez toujours la session de votre navigateur lorsque vous laissez votre ordinateur sans surveillance.

Création et installation de certificats numériques

Objet

Pour les communications réseau qui nécessitent un niveau de sécurité plus élevé qu'un cryptage du mot de passe, l'interface Web de la PDU en rack prend en charge l'utilisation de certificats numériques avec le protocole Secure Sockets Layer (SSL). Les certificats numériques permettent au navigateur Web (client SSL) d'authentifier la PDU en rack (serveur).

Vous pouvez générer une clé à 1024 bits ou bien une clé à 2048-bits qui offre un cryptage complexe et un niveau de sécurité plus élevé.

Les sections qui suivent résument les trois méthodes de création, de mise en œuvre et d'utilisation des certificats numériques pour vous aider à déterminer laquelle est la plus appropriée à votre système.

- Méthode 1 : utilisez le certificat par défaut généré automatiquement par la PDU en rack.
- Méthode 2 : utilisez l'Assistant de sécurité de la PDU en rack pour créer un certificat CA et un certificat de serveur.
- Méthode 3 : utilisez l'Assistant de sécurité de la PDU en rack pour créer une demande de signature par certificat qui sera signée par le certificat racine d'une autorité de certification extérieure, et pour créer un certificat de serveur.

Vous pouvez aussi utiliser la méthode 3 si votre société ou votre agence utilise sa propre autorité de certification. Utilisez l'Assistant de sécurité de la PDU en rack de la même manière, mais avec votre propre autorité de certification à la place d'une autorité de certification commerciale.

Choix d'une méthode pour votre système

En utilisant le protocole Secure Sockets Layer (SSL), vous pouvez choisir l'une des méthodes suivantes pour utiliser des certificats numériques.

Méthode 1 : utilisez le certificat par défaut généré automatiquement par la PDU en rack. Lorsque vous activez le protocole SSL, vous devez redémarrer la PDU en rack. Pendant le redémarrage, s'il n'existe pas de certificat de serveur, la PDU en rack génère un certificat de serveur par défaut qui est signé automatiquement mais que vous ne pouvez pas configurer.

La méthode 1 présente les avantages et inconvénients suivants.

- **Avantages**
  - Avant leur transmission, le nom d'utilisateur, le mot de passe et l'ensemble des données en direction et en provenance de la PDU en rack sont cryptés.
  - Vous pouvez utiliser ce certificat de serveur par défaut pour fournir une sécurité à base de cryptage pendant que vous configurez l'une des deux autres options de certificats numériques, ou choisir de le conserver pour bénéficier du cryptage qu'offre le protocole SSL.
- **Inconvénients**
  - La PDU en rack prend jusqu'à une minute pour créer ce certificat ; pendant ce temps, l'interface Web est inaccessible (ce délai intervient lors de votre première connexion après l'activation du protocole SSL).
  - Dans cette méthode, il n'y a pas d'authentification fournie par un certificat CA (certificat signé par une autorité de certification) contrairement aux méthodes 2 et 3. Aucun certificat CA n'est enregistré en cache dans le navigateur. Par conséquent, lorsque vous vous connectez à la PDU en rack, le navigateur génère une alerte de sécurité indiquant qu'un certificat signé par une autorité de confiance n'est pas disponible, et demande si vous voulez continuer. Pour éviter ce message, vous devez installer le certificat de serveur par défaut dans le magasin

de certificats (cache) du navigateur pour chaque utilisateur qui doit accéder à la PDU en rack, et chaque utilisateur doit toujours utiliser le nom de domaine complet du serveur lorsqu'il se connecte à la PDU en rack.

– Le certificat de serveur par défaut utilise le numéro de série de la PDU en rack à la place d'un *nom commun* valide (nom DNS ou adresse IP de la PDU en rack). Par conséquent, bien que la PDU en rack puisse contrôler l'accès à son interface Web par nom d'utilisateur, mot de passe et type de compte (**Administrateur**, **Utilisateur de périphérique** ou **Utilisateur en lecture seule**), le navigateur ne peut pas identifier quelle PDU en rack envoie ou reçoit des données.
– Par défaut, la longueur de la *clé publique* (clé RSA) utilisée pour le cryptage lors de la mise en place d'une session SSL est de 2048 bits.

Méthode 2 : utilisez l'Assistant de sécurité de la PDU en rack pour créer un certificat CA et un certificat de serveur. Utilisez l'Assistant de sécurité de la PDU en rack pour créer deux certificats numériques :

- Un *certificat racine CA* (certificat racine créé par une autorité de certification) que la PDU en rack utilise pour signer tous les certificats de serveur et que vous installez ensuite dans le magasin (cache) de certificats du navigateur de chaque utilisateur qui doit accéder à la PDU en rack.
- Un *certificat de serveur* que vous téléchargez sur la PDU en rack. Lorsque l'Assistant de sécurité de la PDU en rack crée un certificat de serveur, il utilise le certificat racine CA pour signer le certificat de serveur.

Le navigateur Web authentifie la PDU en rack qui envoie ou demande des données :

- Pour identifier la PDU en rack, le navigateur utilise le *nom commun* (adresse IP ou nom DNS de la PDU en rack) spécifié dans le *nom unique* du certificat de serveur au moment où le certificat a été crée.
- Pour confirmer que le certificat de serveur est signé par une autorité « de confiance », le navigateur compare la signature du certificat de serveur avec celle du certificat racine enregistré dans son cache. Une date d'expiration confirme si le certificat de serveur est actuel.

La méthode 2 présente les avantages et inconvénients suivants.

- **Avantages**
  - Avant leur transmission, le nom d'utilisateur, le mot de passe et l'ensemble des données en direction et en provenance de la PDU en rack sont cryptés.
  - Vous pouvez choisir la longueur de *clé publique* (clé RSA) utilisée pour le cryptage lors de la mise en place d'une session SSL (utilisez 1024 bits, paramètre par défaut, ou 2048 bits pour un cryptage plus complexe et un niveau de sécurité élevé).
  - Le certificat de serveur que vous téléchargez sur la PDU en rack active le protocole SSL pour confirmer que les données transmises dans les deux sens concernent bien la bonne PDU en rack. Ceci ajoute un niveau de sécurité supplémentaire au cryptage du nom d'utilisateur, du mot de passe et des données transmises.
  - Le certificat racine que vous installez dans le navigateur lui permet d'authentifier le certificat de serveur de la PDU en rack afin d'offrir une protection supplémentaire contre les accès non autorisés.
- **Inconvénient**
  Comme les certificats n'ont pas la signature numérique d'une autorité de certification commerciale, vous devez charger manuellement un certificat racine dans le magasin de certificats (cache) du navigateur de chaque utilisateur (les concepteurs de navigateurs fournissent déjà des certificats racine pour les autorités de certification commerciales dans le magasin de certificats du navigateur, comme indiqué en méthode 3).

Méthode 3 : utilisez l'Assistant de sécurité de la PDU en rack pour créer une demande de signature par certificat qui sera signée par le certificat racine d'une autorité de certification extérieure, et pour créer un certificat de serveur.

Utilisez l'Assistant de sécurité de la PDU en rack pour créer une demande (fichier **.csr**) à envoyer à une autorité de certification. L'autorité de certification renvoie un certificat signé (fichier **.crt**) sur la base des informations communiquées dans votre demande. Vous utilisez alors l'Assistant de sécurité de la PDU en rack pour créer un certificat de serveur (fichier **.p15**) comprenant la signature du certificat racine renvoyé par l'autorité de certification. Téléchargez le certificat de serveur sur la PDU en rack.

Vous pouvez aussi utiliser la méthode 3 si votre société ou votre agence utilise sa propre autorité de certification. Utilisez l'Assistant de sécurité de la PDU en rack de la même manière, mais avec votre propre autorité de certification à la place d'une autorité de certification commerciale.

La méthode 3 présente les avantages et inconvénients suivants.

- **Avantages**
  - Avant leur transmission, le nom d'utilisateur, le mot de passe et l'ensemble des données en direction et en provenance de la PDU en rack sont cryptés.
  - Vous bénéficiez de l'authentification par une autorité de certification qui possède déjà un certificat racine signé dans le magasin de certificats du navigateur (les certificats des autorités de certification commerciales sont distribués comme partie intégrante du logiciel de navigation, et une autorité de certification de votre propre société ou agence a sans doute déjà chargé son certificat CA dans le magasin de certificats du navigateur de chaque utilisateur). Par conséquent vous n'avez pas à télécharger un certificat racine dans le navigateur de chaque utilisateur devant accéder à la PDU en rack.
  - Vous pouvez choisir la longueur de *clé publique* (clé RSA) utilisée pour la mise en place d'une session SSL (utilisez 1024 bits, paramètre par défaut, ou 2048 bits pour un cryptage plus complexe et un niveau de sécurité élevé).

  - Le certificat de serveur que vous téléchargez sur la PDU en rack active le protocole SSL pour confirmer que les données transmises dans les deux sens concernent bien la bonne PDU en rack. Ceci ajoute un niveau de sécurité supplémentaire au cryptage du nom d'utilisateur, du mot de passe et des données transmises.
  - Le navigateur vérifie que la signature numérique du certificat de serveur que vous avez téléchargé sur la PDU en rack correspond à celle du certificat racine CA déjà présent dans son magasin de certificats pour fournir une protection supplémentaire contre les accès non autorisés.
- **Inconvénients**
  - La mise en place nécessite l'étape supplémentaire qui consiste à demander un certificat racine signé à une autorité de certification.
  - Une autorité de certification extérieure peut facturer la fourniture de certificats signés.

Pare-feu

Bien que certaines méthodes d'authentification offrent un niveau de sécurité plus élevé que d'autres, il est presque impossible de bénéficier d'une protection complète contre les atteintes à la sécurité. L'utilisation de pare-feu correctement configurés s'avère un élément crucial d'un plan de sécurité complet.

Utilisation de l'Assistant de sécurité de la PDU en rack

L'Assistant de sécurité crée les composants nécessaires pour un haut niveau de sécurité de la PDU en rack lorsque vous utilisez le protocole SSL (Secure Sockets Layer) et les protocoles et routines de codage connexes.

Authentification par certificats et clés d'hôtes

L'*authentification* permet de vérifier l'identité d'un utilisateur ou d'un périphérique réseau (tel qu'une PDU en rack). Les mots de passe identifient généralement les utilisateurs d'ordinateurs. Toutefois, pour des transactions ou des communications qui nécessitent des méthodes de sécurité plus rigoureuses sur Internet, la PDU en rack prend en charge des méthodes d'authentification plus sécurisées.

- Le protocole Secure Sockets Layer (SSL), utilisé pour un accès sécurisé à Internet, utilise une authentification par certificats numériques. Un certificat *racine CA* est émis par une autorité de certification (CA) en tant que partie d'une infrastructure de clé publique et sa signature numérique doit correspondre à celle d'un certificat de serveur présent sur la PDU en rack.
- Secure Shell (SSH), utilisé pour accéder depuis un terminal distant à l'interface par lignes de commande de la PDU en rack, utilise une *clé d'hôte* publique comme méthode d'authentification.

Utilisation des certificats. La plupart des navigateurs Web, notamment ceux pris en charge par les PDU en rack, contiennent un jeu de certificats racine CA émanant de toutes les autorités de certification commerciales.

L'authentification du serveur (dans notre cas la PDU en rack) intervient chaque fois qu'une connexion est établie entre le navigateur et le serveur. Le navigateur vérifie que le certificat du serveur est bien signé par une autorité de certification qu'il connaît.

Pour qu'une authentification ait lieu :

- Chaque serveur (PDU en rack) dont le protocole SSL est activé doit détenir lui-même un certificat de serveur.
- Tout navigateur utilisé pour accéder à l'interface Web de la PDU en rack doit contenir le certificat racine CA dont l'autorité a signé le certificat de serveur.

Si l'authentification échoue, un message du navigateur vous demande si vous souhaitez continuer bien qu'il ne puisse pas authentifier le serveur.

Si votre réseau ne nécessite pas une authentification fournie par des certificats numériques, vous pouvez utiliser le certificat par défaut généré automatiquement par la PDU en rack. La signature numérique du certificat par défaut ne sera pas reconnue par les navigateurs, mais un certificat par défaut vous permet d'utiliser le protocole SSL pour le cryptage des noms d'utilisateurs, des mots de passe et des données transmises (si vous utilisez le certificat par défaut, le navigateur vous demande d'accepter l'accès non authentifié avant de vous connecter à l'interface Web de la PDU en rack).

Utilisation des clés d'hôtes du protocole SSH. Une *clé d'hôte* SSH authentifie l'identité du serveur (la PDU en rack) chaque fois qu'un client SSH contacte ce serveur. Chaque serveur dont le protocole SSH est activé doit détenir lui-même une clé d'hôte SSH.

Fichiers créés pour la sécurité des protocoles SSH et SSL

Utilisez l'Assistant de sécurité de la PDU en rack pour créer les composants ci-dessous d'un système de sécurité SSL et SSH :

- Le certificat de serveur de la PDU en rack, si vous souhaitez bénéficier de l'authentification qu'offre un certificat de ce type. Vous pouvez créer les types de certificats de serveur suivants :
  - Certificat de serveur signé par un certificat racine CA personnalisé, lui-même créé à l'aide de l'Assistant de sécurité de la PDU en rack. Utilisez cette méthode si votre société ou votre agence ne possède pas sa propre autorité de certification et si vous ne souhaitez pas utiliser une autorité de certification extérieure pour signer le certificat de serveur.

  - Certificat de serveur signé par une autorité de certification extérieure. Cette autorité de certification peut être une autorité gérée par votre propre société ou agence ou l'une des autorités de certification commerciales dont les certificats racine CA sont distribués en tant que partie intégrante d'un navigateur.
- Demande de signature de certificat contenant toutes les informations requises pour un certificat de serveur à l'exception de la signature numérique. Cette demande est nécessaire si vous utilisez une autorité de certification extérieure.
- Certificat racine CA.
- Clé d'hôte de protocole SSH que le programme de votre client SSH utilise pour authentifier la PDU en rack lorsque vous vous connectez à l'interface par lignes de commande.

Vous devez définir si les clés publiques pour les certificats SSL et les clés d'hôte pour le protocole SSH, créées à l'aide de l'Assistant de sécurité de la PDU en rack, sont des clés RSA de 1024 bits (paramètre par défaut), ou des clés RSA de 2048 bits qui offrent un cryptage plus complexe et un niveau de sécurité plus élevé.

Si vous ne créez pas et n'utilisez pas de certificats de serveur SSL ni de clés d'hôtes SSH avec l'Assistant de sécurité de la PDU en rack, la PDU en rack génère des clés RSA de 2048 bits.

Seuls les PDU en rack Dell peuvent utiliser des certificats de serveur, des clés d'hôtes et des certificats racine CA créés par l'Assistant de sécurité de la PDU en rack. Ces fichiers ne fonctionnent pas avec des produits tels que OpenSSL® et Microsoft® Internet Information Services (IIS).

Création d'un certificat racine et de certificats de serveur

Résumé

Utilisez cette procédure si votre société ou votre agence ne possède pas sa propre autorité de certification et si vous ne souhaitez pas utiliser une autorité de certification commerciale pour signer vos certificats de serveur.

Définissez la taille de la clé publique RSA qui fait partie du certificat généré par l'Assistant de sécurité de la PDU en rack. Vous pouvez générer une clé de 1024 bits ou bien une clé de 2048 bits qui offre un cryptage plus complexe et un niveau de sécurité plus élevé (si vous n'utilisez pas l'assistant, la PDU en rack génère par défaut une clé de 2048 bits).

- Créez un certificat racine AC pour signer tous les certificats de serveur qui seront utilisés avec la PDU en rack. Au cours de cette tâche, deux fichiers sont créés :
  - Le fichier avec l'extension **.p15** est un fichier crypté qui contient la clé privée et le certificat racine public de l'autorité de certification. Ce fichier signe les certificats de serveur.
  - Le fichier avec l'extension **.crt** contient uniquement le certificat racine public de l'autorité de certification. Chargez ce fichier dans les navigateurs qui seront utilisés pour accéder à la PDU en rack afin qu'ils puissent valider le certificat de serveur de cette PDU en rack.
- Créez un certificat de serveur, enregistré dans un fichier avec l'extension **.p15**. Au cours de cette tâche, une invite vous demande le certificat racine CA qui signe le certificat de serveur.
- Chargez le certificat de serveur sur la PDU en rack.
- Pour chaque PDU en rack qui nécessite un certificat de serveur, répétez les tâches de création et de chargement du certificat de serveur.

Procédure

Création d'un certificat racine CA.

1. Si l'Assistant de sécurité de la PDU en rack n'est pas encore installé sur votre ordinateur, procurez-vous le programme d'installation (**Rack PDU Security Wizard.exe**) et exécutez-le.
2. Dans le menu **Démarrer** de Windows, sélectionnez **Programmes**, puis **Rack PDU Security Wizard** (Assistant de sécurité de la PDU en rack).
3. Dans l'écran intitulé **Step 1** (Étape 1), sélectionnez **CA Root Certificate** (Certificat racine CA) comme type de fichier à créer, puis la longueur de la clé à générer (1024 bits, paramètre par défaut, ou 2048 bits pour un cryptage plus complexe et un niveau de sécurité plus élevé).
4. Enntrez un nom pour ce fichier qui contiendra le certificat racine public et la clé privée de l'autorité de certification. Le fichier doit avoir l'extension **.p15** et, par défaut, il sera créé dans le dossier d'installation **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. Dans l'écran intitulé **Step 2** (Étape 2), renseignez les informations pour configurer le certificat racine CA. Les champs **Country** (Pays) et **Common Name** (Nom commun) sont les seuls champs requis. Dans le champ **Common Name**, entrez un nom identifiant votre société ou agence. Utilisez uniquement des caractères alphanumériques, sans espaces.

Par défaut, un certificat racine CA est valide pendant 10 ans à partir de la date et de l'heure de sa création, mais vous pouvez modifier les champs **Validity Period Start** (Début de validité) et **Validity Period End** (Fin de validité).

6. L'écran suivant contient un récapitulatif du certificat. Défilez vers le bas pour consulter le numéro de série et les « empreintes digitales » uniques du certificat. Pour modifier les informations que vous avez fournies, cliquez sur **Back** (Retour). Corrigez les informations.

   Les informations sur l'objet du certificat et celles sur l'émetteur du certificat doivent être identiques.

7. Le dernier écran vérifie que le certificat a été créé et affiche les informations nécessaires pour les tâches suivantes :
   - L'emplacement et le nom du fichier **.p15** que vous utiliserez pour signer les certificats de serveur.
   - L'emplacement et le nom du fichier **.crt** , qui est le certificat racine CA à charger dans le navigateur de chaque utilisateur devant accéder à la PDU en rack.

Chargez le certificat racine AC dans votre navigateur. Chargez le fichier **.crt** dans le navigateur de chaque utilisateur devant accéder à la PDU en rack.

Consultez l'aide du navigateur pour des informations sur le chargement du fichier **.crt** dans son magasin de certificats (cache). Vous trouverez ci-dessous un récapitulatif de la procédure pour Microsoft Internet Explorer.

1. Sélectionnez **Outils**, puis **Options Internet** dans la barre de menu.
2. Dans la boîte de dialogue, sous l'onglet **Contenu**, cliquez sur **Certificats...** puis sur **Importer...**.
3. L'Assistant Importation de certificat vous guide pour le reste de la procédure. Le type de fichier à sélectionner est X.509, et le certificat racine public CA est le fichier **.crt** créé au cours de la procédure Création d'un certificat racine et de certificats de serveur.

Création d'un certificat utilisateur de serveur SSL.

1. Dans le menu **Démarrer** de Windows, sélectionnez **Programmes**, puis **Rack PDU Security Wizard** (Assistant de sécurité de la PDU en rack).
2. Dans l'écran intitulé **Step 1** (Étape 1), sélectionnez **SSL Server Certificate** (Certificat de serveur SSL) comme type de fichier, puis la longueur de la clé à générer (1024 bits, paramètre par défaut, ou 2048 bits pour un cryptage plus complexe et un niveau de sécurité plus élevé).
3. Enntrez un nom pour ce fichier qui contiendra le certificat de serveur et la clé privée. Le fichier doit avoir l'extension **.p15** et, par défaut, il sera créé dans le dossier **C:\Program Files\Dell\Rack PDU Security Wizard**.
4. Cliquez sur **Parcourir** et sélectionnez le certificat racine CA créé au cours de la procédure Création d'un certificat racine et de certificats de serveur. Le certificat racine CA est utilisé pour signer le certificat utilisateur de serveur en cours de création.
5. Dans l'écran intitulé **Step 2** (Étape 2), renseignez les informations pour configurer le certificat de serveur. Les champs **Country** (Pays) et **Common Name** (Nom commun) sont les seuls champs requis. Dans le champ **Common Name**, entrez l'adresse IP ou le nom DNS du serveur (la PDU en rack). Par défaut, un certificat de serveur est valide pendant 10 ans, mais vous pouvez modifier les champs **Validity Period Start** (Début de validité) et **Validity Period End** (Fin de validité).

   Les informations de configuration faisant partie de la signature, les informations de chaque certificat doivent être uniques. La configuration d'un certificat de serveur ne peut pas être la même que celle d'un certificat racine CA (la date d'expiration n'est pas considérée comme faisant partie de la configuration unique. Certaines autres configurations peuvent aussi différer).

6. L'écran suivant contient un récapitulatif du certificat. Défilez vers le bas pour consulter le numéro de série et les « empreintes digitales » uniques du certificat. Pour modifier les informations que vous avez fournies, cliquez sur **Back** (Retour). Corrigez les informations.

7. Le dernier écran vérifie que le certificat a été créé et vous demande de charger le certificat de serveur dans la PDU en rack. Il affiche l'emplacement et le nom du certificat de serveur qui porte l'extension **.p15** et contient la clé privée et le certificat racine public de la PDU en rack.

Chargez le certificat de serveur sur la PDU en rack.

1. Dans l'onglet **Administration**, sélectionnez **Network** (Réseau) dans la barre de menus supérieure, puis **ssl certificate** (certificat SSL) sous l'en-tête **Web** dans le menu de navigation de gauche.
2. Sélectionnez **Add or Replace Certificate File** (Ajouter ou remplacer le fichier du certificat), et recherchez le certificat de serveur, c'est-à-dire le fichier **.p15** que vous avez créé au cours de la procédure Création d'un certificat racine et de certificats de serveur (emplacement par défaut : **C:\Program Files\Dell\Rack PDU Security Wizard**).

Vous pouvez aussi utiliser les protocoles FTP ou Secure CoPy (SCP) pour transférer le certificat de serveur. Pour SCP, la commande pour transférer un certificat intitulé **cert.p15** à une PDU en rack dont l'adresse IP est 156.205.6.185 serait :

```
scp cert.p15 dell@156.205.6.185
```

Création d'un certificat de serveur et d'une demande de signature

Résumé

Utilisez cette procédure si votre société ou votre agence possède sa propre autorité de certification ou si vous prévoyez d'utiliser une autorité de certification commerciale pour signer vos certificats de serveur.

- Créez une demande de signature de certificat (CSR). La CSR contient toutes les informations nécessaires pour un certificat de serveur à l'exception de la signature numérique. Ce processus crée deux fichiers de sortie :
  - Le fichier avec l'extension **.p15** contient la clé privée de la PDU en rack.
  - Le fichier avec l'extension **.csr** contient la demande de signature du certificat, que vous envoyez à une autorité de certification extérieure.
- Lorsque vous recevez le certificat signé de l'autorité de certification, importez-le. L'importation du certificat combine le fichier **.p15** qui contient la clé privée et le fichier qui contient le certificat signé de l'autorité de certification extérieure. Le fichier de sortie est un nouveau fichier crypté de certificat de serveur avec l'extension **.p15**.
- Chargez le certificat de serveur sur la PDU en rack.
- Pour chaque PDU en rack qui nécessite un certificat de serveur, répétez les tâches de création et de chargement du certificat de serveur.

Procédure

Création d'une demande de signature de certificat (CSR).

1. Si l'Assistant de sécurité de la PDU en rack n'est pas encore installé sur votre ordinateur, procurez-vous le programme d'installation (**Rack PDU Security Wizard.exe**) et exécutez-le.
2. Dans le menu **Démarrer** de Windows, sélectionnez **Programmes**, puis **Rack PDU Security Wizard** (Assistant de sécurité de la PDU en rack).

3. Dans l'écran intitulé **Step 1** (Étape 1), sélectionnez **Certificate Request** (Demande de certificat) comme type de fichier à créer, puis la longueur de la clé à générer (1024 bits, paramètre par défaut, ou 2048 bits pour un cryptage plus complexe et un niveau de sécurité plus élevé).
4. Entrez un nom pour ce fichier qui contiendra la clé privée de la PDU en rack. Le fichier doit avoir l'extension **.p15** et, par défaut, il sera créé dans le dossier d'installation **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. Dans l'écran intitulé **Step 2** (Étape 2), renseignez les informations nécessaires pour configurer la demande de signature de certificat (CSR), c'est-à-dire les informations que le certificat de serveur signé devra contenir. Les champs **Country** (Pays) et **Common Name** (Nom commun) sont obligatoires. Les autres champs sont facultatifs. Dans le champ **Common Name**, entrez l'adresse IP ou le nom DNS de la PDU en rack.

   Par défaut, un certificat de serveur est valide pendant 10 ans à partir de la date et de l'heure actuelle, mais vous pouvez modifier les champs **Validity Period Start** (Début de validité) et **Validity Period End** (Fin de validité).

6. L'écran suivant contient un récapitulatif du certificat. Défilez vers le bas pour consulter le numéro de série et les empreintes digitales uniques du certificat. Pour modifier les informations que vous avez fournies, cliquez sur **Back** (Retour). Corrigez les informations.

   Les informations sur l'objet du certificat et celles sur l'émetteur du certificat doivent être identiques.

7. Le dernier écran vérifie que la demande de signature de certificat a été créée et affiche l'emplacement et le nom du fichier, dont l'extension est **.csr**.

8. Envoyez la demande de signature de certificat à une autorité de certification extérieure (autorité de certification commerciale ou, le cas échéant, autorité de certification gérée par votre propre société ou agence).

Consultez les instructions fournies par l'autorité de certification relatives à la signature et à l'émission de certificats de serveur.

Importation du certificat signé. Lorsque l'autorité de certification extérieure renvoie le certificat signé, importez-le. Cette procédure combine le certificat signé et la clé privée dans un certificat de serveur SSL que vous téléchargez ensuite sur la PDU en rack.

1. Dans le menu **Démarrer** de Windows, sélectionnez **Programmes**, puis **Rack PDU Security Wizard** (Assistant de sécurité de la PDU en rack).
2. Dans l'écran intitulé **Step 1** (Étape 1), sélectionnez **Import Signed Certificate** (Importer le certificat signé).
3. Recherchez le certificat de serveur signé que vous avez reçu de l'autorité de certification extérieure et sélectionnez-le. Ce fichier porte l'extension **.cer** ou **.crt**.
4. Recherchez et sélectionnez le fichier créé à l'Étape 4 de la tâche Création d'une demande de signature de certificat (CSR). Ce fichier avec l'extension **.p15** contient la clé privée de la PDU en rack et se trouve par défaut dans le dossier d'installation **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. Spécifiez un nom pour le fichier de sortie qui sera le certificat de serveur signé que vous allez charger sur la PDU en rack. Ce fichier doit avoir l'extension **.p15**.
6. Cliquez sur **Next** (Suivant) pour générer le certificat de serveur. Dans l'écran récapitulatif, **Issuer Information** (Informations sur l'émetteur) confirme que l'autorité de certification extérieure a signé le certificat.

7. Le dernier écran vérifie que le certificat a été créé et vous demande de charger le certificat de serveur dans la PDU en rack. Il affiche l'emplacement et le nom du certificat de serveur, qui a l'extension **.p15** et contient la clé privée de la PDU en rack et la clé publique obtenue à partir du fichier **.cer** ou **.crt**.

Chargez le certificat de serveur sur la PDU en rack.

1. Dans l'onglet **Administration**, sélectionnez **Network** (Réseau) dans la barre de menus supérieure, puis **ssl certificate** (certificat SSL) sous l'en-tête **Web** dans le menu de navigation de gauche.
2. Sélectionnez **Add or Replace Certificate File** (Ajouter ou remplacer le fichier du certificat), et recherchez le certificat de serveur, c'est-à-dire le fichier **.p15** que vous avez créé au cours de la procédure Création d'un certificat racine et de certificats de serveur (emplacement par défaut : **C:\Program Files\Dell\Rack PDU Security Wizard**).

Vous pouvez aussi utiliser les protocoles FTP ou Secure CoPy (SCP) pour transférer le certificat de serveur à la PDU en rack. Pour SCP, la commande pour transférer un certificat intitulé **cert.p15** à une PDU en rack dont l'adresse IP est 156.205.6.185 serait :

```
scp cert.p15 dell@156.205.6.185
```

Création d'une clé d'hôte SSH

Résumé

Cette procédure est optionnelle. Si vous sélectionnez le cryptage SSH, mais que vous ne créez pas de clé d'hôte, la PDU en rack génère une clé RSA de 2048 bits lorsqu'elle redémarre. Il vous appartient de décider si les clés d'hôtes pour le protocole SSH créées avec l'Assistant de sécurité de la PDU en rack sont des clés RSA de 1024 bits ou 2048 bits.

Vous pouvez générer une clé de 1024 bits ou bien une clé de 2048 bits qui offre un cryptage complexe et un niveau de sécurité plus élevé.

- Utilisez l'Assistant de sécurité de la PDU en rack pour créer une clé d'hôte cryptée et enregistrée dans un fichier avec l'extension **.p15**.
- Chargez la clé d'hôte sur la PDU en rack.

Procédure

Création de la clé d'hôte.

1. Si l'Assistant de sécurité de la PDU en rack n'est pas encore installé sur votre ordinateur, procurez-vous le programme d'installation (**Rack PDU Security Wizard.exe**) et exécutez-le.
2. Dans le menu **Démarrer** de Windows, sélectionnez **Programmes**, puis **Rack PDU Security Wizard** (Assistant de sécurité de la PDU en rack).
3. Dans l'écran intitulé **Step 1** (Étape 1), sélectionnez **SSH Server Host Key** (Clé d'hôte de serveur SSH) comme type de fichier à créer, puis la longueur de la clé à générer (1024 bits, paramètre par défaut, ou 2048 bits pour un cryptage plus complexe et un niveau de sécurité plus élevé).
4. Entrez un nom pour ce fichier qui contiendra la clé d'hôte. Ce fichier doit avoir l'extension **.p15**. Par défaut, le fichier sera créé dans le dossier d'installation **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. Cliquez sur **Next** (Suivant) pour générer la clé d'hôte.
6. L'écran récapitulatif affiche les empreintes digitales SSH version 2, qui sont uniques pour chaque clé d'hôte et permettent de l'identifier. Après avoir chargé la clé d'hôte sur la PDU en rack, vous pouvez vous assurer que la clé d'hôte correcte a été chargée en vérifiant que les empreintes digitales affichées ici correspondent aux empreintes SSH sur la PDU en rack, affichées par votre programme client SSH.
7. Le dernier écran confirme que la clé d'hôte a été créée, vous demande de la charger sur la PDU en rack et affiche l'emplacement et le nom de la clé d'hôte (fichier avec l'extension **.p15**).

Chargez la clé d'hôte sur la PDU en rack.

1. Dans l'onglet **Administration**, sélectionnez **Network** (Réseau) dans la barre de menus supérieure, puis **ssl host key** (clé d'hôte SSL) sous l'en-tête **Console** dans le menu de navigation de gauche.
2. Sélectionnez **Add or Replace Host Key** (Ajouter ou remplacer la clé d'hôte), et recherchez la clé d'hôte, c'est-à-dire le fichier **.p15** que vous avez créé au cours de la procédure Création de la clé d'hôte (emplacement par défaut : **C:\Program Files\Dell\Rack PDU Security Wizard**).
3. En bas de la page **User Host Key** (Clé d'hôte utilisateur), notez l'empreinte digitale SSH. Connectez-vous à la PDU en rack par l'intermédiaire de votre programme client SSH et assurez-vous que la clé d'hôte correcte a été chargée en vérifiant que ces empreintes correspondent à celles affichées par le programme client.

Vous pouvez aussi utiliser les protocoles FTP ou Secure CoPy (SCP) pour transférer la clé d'hôte sur la PDU en rack. Pour SCP, la commande suivante permettrait de transférer une clé d'hôte intitulée **hostkey.p15** à une PDU en rack dont l'adresse IP est 156.205.6.185 :

```
scp hostkey.p15 dell@156.205.6.185
```

Accès à l'interface par lignes de commande et sécurité

Les utilisateurs titulaires de comptes Administrateur ou Utilisateur de périphérique peuvent accéder à l'interface par lignes de commande par l'intermédiaire du protocole Telnet ou Secure Shell (SSH), selon lequel est activé (un administrateur peut activer ces méthodes d'accès en sélectionnant l'onglet **Administration**, puis **Network** (Réseau) dans la barre de menus supérieure et **access** sous l'en-tête **Console** du menu de navigation gauche). Par défaut, le protocole Telnet est activé. L'activation de SSH provoque la désactivation automatique de Telnet.

Telnet pour un accès de base. Telnet fournit une sécurité de base grâce à une authentification par nom d'utilisateur et mot de passe mais ne présente pas les avantages d'une haute sécurité par cryptage.

SSH pour un accès hautement sécurisé. Si vous utilisez le mode haute sécurité du protocole SSL pour l'interface Web, utilisez Secure Shell (SSH) pour accéder à l'interface par lignes de commande. SSH crypte les noms d'utilisateurs, les mots de passe et les données transmises.

Que vous utilisiez l'interface par lignes de commande via SSH ou Telnet, l'interface, les comptes et les droits d'accès utilisateurs restent les mêmes ; mais pour utiliser SSH, vous devez d'abord le configurer et installer une application client SSH sur votre ordinateur.

Telnet et Secure Shell (SSH)

Lorsque SSH est activé, vous ne pouvez pas utiliser Telnet pour accéder à l'interface par lignes de commande. Activer le protocole SSH active automatiquement le protocole SCP.

Lorsque SSH est activé et que son port est configuré, aucune configuration supplémentaire n'est requise pour utiliser Secure CoPy (SCP). SCP utilise la même configuration que le protocole SSH.

Pour utiliser le protocole SSH, un client SSH doit être installé. La plupart des plateformes Linux et UNIX® comprennent un client SSH, mais pas les systèmes d'exploitation Microsoft Windows. Les clients SSH sont disponibles auprès de plusieurs fournisseurs.

Pour configurer les options pour les protocoles Telnet et Secure Shell (SSH) :

1. Dans l'onglet **Administration** de l'interface Web, sélectionnez **Network** (Réseau) dans la barre de menus supérieure, puis l'option **access** (accès) sous l'en-tête **Console** du menu de navigation de gauche.
2. Configurez les paramètres de port pour Telnet et SSH.

   Pour des informations sur la sécurité supplémentaire qu'offre un port non standard, voir Affectations de ports.

3. Sous **Console** dans le menu de navigation gauche, sélectionnez **ssh host key** (clé d'hôte SSH), spécifiez une clé d'hôte précédemment créée à l'aide de l'Assistant de sécurité de la PDU en rack, et chargez-la dans la PDU en rack.

   Si vous ne spécifiez pas de fichier de clé d'hôte ici, si vous installez une clé non valide, ou si vous activez le protocole SSH sans qu'une clé d'hôte soit installée, la PDU en rack génère une clé d'hôte RSA de 2048 bits. Pour que la PDU en rack crée une clé d'hôte, elle doit redémarrer. **La PDU en rack peut prendre jusqu'à une minute pour créer cette clé d'hôte ; pendant ce temps, SSH est inaccessible.**

   Depuis une interface par lignes de commande telle que l'invite de commande des systèmes d'exploitation Windows, vous pouvez également utiliser FTP ou Secure CoPy (SCP) pour transférer le fichier de clé d'hôte.

4. Affichez l'*empreinte digitale* de la clé d'hôte SSH pour le protocole SSH version 2. La plupart des clients SSH affichent l'empreinte digitale au début d'une session. Comparez l'empreinte digitale affichée par le client à celle que vous avez enregistrée à partir de l'interface Web ou de l'interface par lignes de commande de la PDU en rack.

Accès à l'interface Web et sécurité : HTTP et HTTPS (avec SSL)

Le protocole Hypertext Transfer Protocol (HTTP) fournit l'accès par nom d'utilisateur et mot de passe, mais sans crypter les noms d'utilisateurs, les mots de passe ni les données pendant la transmission. Le protocole HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) crypte les noms d'utilisateurs, les mots de passe et les données pendant la transmission, et fournit une authentification de la PDU en rack par l'intermédiaire de certificats numériques.

Consultez Création et installation de certificats numériques pour choisir la méthode d'utilisation des certificats numériques.

Pour configurer HTTP et HTTPS :

1. Dans l'onglet **Administration**, sélectionnez **Network** (Réseau) dans la barre de menus supérieure, puis **access** (accès) sous **Web** dans le menu de navigation de gauche.
2. Activez HTTP ou HTTPS et configurez les ports que chacun des deux protocoles va utiliser. Les modifications prennent effet à la prochaine connexion. Lorsque le protocole SSL est activé, votre navigateur affiche une petite icône représentant un cadenas.

Pour des informations sur la sécurité supplémentaire qu'offre un port non standard, voir Affectations de ports.

3. Sélectionnez **ssl certificate** (certificat ssl) sous **Web** dans le menu de navigation gauche pour déterminer si un certificat de serveur est installé sur la PDU en rack. Si un certificat a été créé avec l'Assistant de sécurité de la PDU en rack mais qu'il n'est pas installé :
   - Dans l'interface Web, recherchez le fichier de certificat et téléchargez-le dans la PDU en rack.
   - Vous pouvez également utiliser le protocole Secure CoPy (SCP) ou FTP pour télécharger le fichier de certificat dans la PDU en rack.

Créer et télécharger un certificat de serveur à l'avance permet de réduire le temps nécessaire pour activer le protocole HTTPS. Si vous activez HTTPS sans qu'aucun certificat de serveur ne soit chargé, la PDU en rack en crée un lors de son redémarrage. **La PDU en rack peut prendre jusqu'à une minute pour créer le certificat ; pendant ce temps, le serveur SSH est inaccessible.**

Un certificat généré par la PDU en rack présente certaines limites. Voir Méthode 1 : utilisez le certificat par défaut généré automatiquement par la PDU en rack.

4. Si un certificat de serveur numérique valide est chargé, le champ **Status** (État) affiche le lien **Valid Certificate (Certificat valide)**. Cliquez sur ce lien pour afficher les paramètres du certificat.

Paramètre	Description
Issued To (Émis pour) :	**Common Name (CN) [Nom commun (CN)]** : adresse IP ou nom DNS de la PDU en rack. Ce champ contrôle la manière dont vous devez vous connecter à l'interface Web. • Si une adresse IP a été spécifiée pour ce champ lorsque le certificat a été créé, utilisez une adresse IP pour vous connecter. • Si un nom DNS a été spécifié pour ce champ lorsque le certificat a été créé, utilisez le nom DNS pour vous connecter. Si vous n'utilisez pas l'adresse IP ou le nom DNS spécifié pour le certificat, l'authentification échoue et vous recevez un message d'erreur vous demandant si vous voulez continuer. Pour un certificat de serveur généré par défaut par la PDU en rack, ce champ contient à la place le numéro de série de la PDU en rack. **Organization (O)**, **Organizational Unit (OU)** [Unité organisationnelle (OU)] et **Locality, Country (Ville, Pays) :** nom, unité organisationnelle et emplacement de l'organisation qui utilise le certificat de serveur. Pour un certificat de serveur généré par défaut par la PDU en rack, le champ **Organizational Unit (OU)** [Unité organisationnelle (OU)] affiche « Internally Generated Certificate » (Certificat généré en interne). **Serial Number (Numéro de série)** : numéro de série du certificat de serveur.
Issued By (Émis par) :	**Common Name (CN) [Nom commun (CN)]** : nom commun spécifié par le certificat racine AC. Pour un certificat de serveur généré par défaut par la PDU en rack, ce champ contient à la place le numéro de série de la PDU en rack. **Organization (O)** et **Organizational Unit (OU)** [Unité organisationnelle (OU)] : nom et unité organisationnelle de l'organisation ayant émis le certificat de serveur. Si le certificat de serveur a été généré par défaut par la PDU en rack ou par le périphérique, ce champ affiche « Internally Generated Certificate » (Certificat généré en interne).

Paramètre	Description
Validity (Validité) :	**Issued on (Émis le)** : date et heure auxquelles le certificat a été émis. **Expires on (Expire le)** : date et heure auxquelles le certificat expire.
Empreintes	Chacune des deux empreintes digitales est composée d'une longue chaîne de caractères alphanumériques, ponctuée par deux points (:). Une empreinte digitale est un identifiant unique permettant une authentification supplémentaire du serveur. Enregistrez les empreintes digitales afin de les comparer à celles que contient le certificat, affichées dans le navigateur. **SHA1 Fingerprint (Empreinte SHA1)** : empreinte digitale créée par un algorithme de hachage sécurisé (SHA-1). **MD5 Fingerprint (Empreinte MD5)** : empreinte digitale créée par un algorithme Message Digest 5 (MD5).

Fonctions et serveurs RADIUS pris en charge

Fonctions prises en charge

Fonctions d'authentification et d'autorisation prises en charge : Remote Authentication Dial-In User Service (RADIUS). Utilisez RADIUS pour gérer de manière centralisée l'accès à distance à chaque PDU en rack. Lorsqu'un utilisateur accède à la PDU en rack, une demande d'authentification est envoyée au serveur RADIUS afin de déterminer le niveau d'autorisation de l'utilisateur.

Pour plus d'informations sur les niveaux d'autorisation, consultez Types de comptes utilisateurs.

Serveurs RADIUS pris en charge

Serveurs RADIUS pris en charge : FreeRADIUS et Microsoft IAS 2003. D'autres applications RADIUS courantes peuvent également convenir mais n'ont pas fait l'objet de tests complets.

Configuration de la PDU en rack

Authentification

Les noms d'utilisateurs RADIUS utilisés avec la PDU en rack sont limités à 32 caractères.

Dans l'onglet **Administration**, sélectionnez **Security** (Sécurité) dans la barre de menu supérieure. Ensuite, sous **Remote Users** (Utilisateurs distants) du menu de navigation gauche, sélectionnez **authentication** (authentification) pour définir une méthode d'authentification :

- **Local Authentication Only** (Authentification locale uniquement) : RADIUS est désactivé. L'authentification locale est activée.
- **RADIUS, then Local Authentication (Authentification RADIUS, puis locale)** : les authentifications RADIUS et locale sont activées. L'authentification est demandée d'abord au serveur RADIUS ; l'authentification locale est utilisée uniquement si le serveur RADIUS ne répond pas.
- **RADIUS Only (RADIUS uniquement)** : RADIUS est activé. L'authentification locale est désactivée.

Si **RADIUS Only (RADIUS uniquement)** est sélectionné, et que le serveur RADIUS n'est pas disponible, est incorrectement identifié ou incorrectement configuré, l'accès à distance est impossible pour tous les utilisateurs. Vous devez vous connecter à l'interface par lignes de commande à l'aide d'une connexion série et modifier le paramètre d'accès RADIUS en lui donnant la valeur `local` ou `radiusLocal` pour rétablir l'accès. Par exemple, la commande pour modifier le paramètre d'accès sur `local` serait :

```
radius -a local
```

RADIUS

Pour configurer RADIUS, dans l'onglet **Administration**, sélectionnez **Security** (Sécurité) dans la barre de menu supérieure. Puis, sous **Remote Users** (Utilisateurs distants) du menu de navigation gauche, sélectionnez **RADIUS**.

Paramètre	Définition
RADIUS Server (Serveur RADIUS)	Nom ou adresse IP du serveur RADIUS. **REMARQUE :** les serveurs RADIUS utilisent le port 1812 par défaut pour authentifier les utilisateurs. Pour utiliser un port différent, ajoutez le signe deux points, suivi du nouveau numéro de port, à la suite du nom ou de l'adresse IP du serveur RADIUS.
Secret	Secret partagé entre le serveur RADIUS et la PDU en rack.
Reply Timeout (Délai de réponse)	Durée en secondes pendant laquelle la PDU en rack attend une réponse du serveur RADIUS.
Test Settings (Paramètres de test)	Entrez le nom d'utilisateur et le mot de passe Administrateur pour tester le chemin d'accès du serveur RADIUS que vous avez configuré.
Skip Test and Apply (Ignorer le test et appliquer)	Ne pas tester le chemin d'accès du serveur RADIUS.

Si deux serveurs configurés sont répertoriés et si la méthode d'authentification locale activée est **RADIUS, then Local Authentication (RADIUS, puis authentification locale)** ou **RADIUS Only (RADIUS uniquement)**, vous pouvez changer le serveur RADIUS qui authentifiera les utilisateurs en cliquant sur le bouton **Switch Server Priority** (Changer la priorité des serveurs).

Configuration du serveur RADIUS

Vous devez configurer votre serveur RADIUS afin qu'il fonctionne avec la PDU en rack. Les exemples de cette section peuvent différer quelque peu du contenu requis ou du format de votre serveur RADIUS spécifique. Dans ces exemples, toute référence à des prises s'applique uniquement aux PDU en rack qui prennent en charge les utilisateurs de prises.

1. Ajoutez l'adresse IP de la PDU en rack à la liste des clients du serveur RADIUS (fichier).
2. Les utilisateurs doivent disposer d'attributs Service-Type sauf si des VSA (Vendor Specific Attributes) sont définis à la place. Si aucun attribut Service-Type n'est configuré, l'utilisateur ne dispose que de l'accès en lecture seule (uniquement à l'interface Web). Les deux valeurs acceptables pour Service-Type sont Administrative-User (6), qui accorde à l'utilisateur des autorisations Administrateur, et Login-User (1), qui lui accorde des autorisations de type Périphérique.

Consultez la documentation de votre serveur RADIUS pour des informations sur le fichier d'utilisateurs RADIUS.

Exemple utilisant les attributs Service-Type

Dans l'exemple suivant d'un fichier d'utilisateurs RADIUS :

- **RPDUAdmin** correspond à **Service-Type: Administrative-User, (6)**
- **RPDUDevice** correspond à **Service-Type: Login-User, (1)**
- **RPDUReadOnly** correspond à **Service-Type: null**

```
RPDUAdmin       Auth-Type = Local, Password = "admin"
   Service-Type = Administrative-User

RPDUDevice      Auth-Type = Local, Password = "device"
   Service-Type = Login-User

RPDUReadOnly    Auth-Type = Local, Password = "readonly"
```

Exemples utilisant les attributs Vendor Specific

Les attributs Vendor Specific (VSA) peuvent être utilisés au lieu des attributs Service-Type fournis par votre serveur RADIUS. Cette méthode nécessite une entrée de dictionnaire et un fichier d'utilisateurs RADIUS. Dans le fichier de dictionnaire, vous pouvez définir les noms des mots-clés ATTRIBUTE et VALUE, mais pas les valeurs numériques. Si vous modifiez les valeurs numériques, l'authentification et l'autorisation RADIUS ne fonctionnent pas correctement. Les VSA ont priorité sur les attributs RADIUS standard.

Fichier de dictionnaire. Voici un exemple de fichier de dictionnaire RADIUS (dictionary.dell) :

```
#
# dictionary.dell
#
#
VENDOR   DELL 318
#
# Attributes
#
ATTRIBUTE DELL-Service-Type 1 integer DELL
ATTRIBUTE DELL-Outlets      2 string DELL

VALUE DELL-Service-Type Admin    1
VALUE DELL-Service-Type Device   2
VALUE DELL-Service-Type ReadOnly 3
#
# For devices with outlet users only
#
VALUE DELL-Service-Type Outlet   4
```

Utilisateurs RADIUS avec VSA. Voici un exemple de fichier d'utilisateurs RADIUS avec VSA :

```
VSAAdmin     Auth-Type = Local, Password = "admin"
             DELL-Service-Type = Admin

VSADevice    Auth-Type = Local, Password = "device"
             DELL-Service-Type = Device

VSAReadOnly Auth-Type = Local, Password = "readonly"
             DELL-Service-Type = ReadOnly

# Give user access to device outlets 1, 2 and 3.
VSAOutlet    Auth-Type = Local, Password = "outlet"
             DELL-Service-Type = Outlet,
             DELL-Outlets = "1,2,3"
```

Consultez les rubriques connexes suivantes :

- Types de comptes utilisateurs pour des informations sur les trois niveaux d'autorisation de base accordés à l'utilisateur (Administrateur, Utilisateur de périphérique, Utilisateur en lecture seule).
- Serveurs RADIUS pris en charge pour des informations sur les serveurs RADIUS testés et pris en charge.

Exemple avec mots de passe fantômes UNIX. Si vous utilisez des fichiers de mots de passe fantômes UNIX (**/etc/passwd**) avec les fichiers de dictionnaire RADIUS, vous pouvez utiliser les deux méthodes suivantes pour authentifier les utilisateurs :

- Si tous les utilisateurs UNIX disposent de privilèges administratifs, ajoutez les informations suivantes au fichier « user » RADIUS. Pour autoriser uniquement les comptes Utilisateur de périphérique, modifiez le paramètre Dell-Service-Type sur **Device**.

```
DEFAULT    Auth-Type = System
           DELL-Service-Type = Admin
```

- Ajoutez les noms d'utilisateurs et les attributs au fichier « user » RADIUS et confirmez le mot de passe par rapport à **/etc/passwd**. L'exemple suivant concerne les utilisateurs **bconners** et **thawk** :

```
bconners          Auth-Type = System
                  DELL-Service-Type = Admin
thawk             Auth-Type = System
                  DELL-Service-Type = Outlet
                  DELL-Outlets = "1,2,3"
```

Index

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

X

11/2010 Référence 990-3926-012