GUIDE D'UTILISATION

CG2400

ID de document : CG2400 révision 1.0

CG2400 - GUIDE D'UTILISATION

Avis de non-responsabilité

Kontron attire l'attention sur le fait que les informations contenues dans ce guide sont susceptibles d'être modifiées, notamment en raison de l'évolution constante des produits Kontron. Ce document n'implique aucune garantie de la part de Kontron en ce qui concerne les processus techniques décrits dans le guide ou les caractéristiques du produit présentées dans le guide. Kontron n'assume aucune responsabilité quant à l'utilisation du ou des produits décrits, n'accorde aucune licence ou titre en vertu d'un brevet, d'un droit d'auteur ou d'un droit de masquage pour ces produits et ne garantit pas que ces produits sont exempts de violation de brevet, de droit d'auteur ou de droit de masquage, sauf indication contraire. Les applications décrites dans ce guide le sont à titre d'illustration uniquement. Kontron ne garantit pas qu'une telle application sera adaptée à l'utilisation spécifiée sans tests ou modifications supplémentaires.

Kontron informe expressément l'utilisateur que ce guide ne contient qu'une description générale des processus et des instructions qui peuvent ne pas être applicables dans chaque cas individuel. En cas de doute, veuillez contacter Kontron.

Kontron Canada, Inc.

4555 Ambroise-Lafortune

Boisbriand, QC

Canada J7H 0A4

www.kontron.com

Description du produit

Le serveur 2U haute disponibilité CG2400 est la 8e génération de plateformes de Kontron conçues pour satisfaire à la certification NEBS-3/ETSI. Ce serveur à la fois robuste et sophistiqué a évolué afin de prendre en charge bien plus que les systèmes de télécommunications classiques utilisés par les fournisseurs de services de communication.

Applications principales

- La plupart des utilisations dans les stations de base de télécommunication fixe-sans fil ou des utilisations vitales associées à l'informatique en périphérie qui nécessitent une haute disponibilité
- Applications pour la sécurité, la technologie financière, la surveillance, les données d'apprentissage profond et l'analyse vidéo
- Applications permanentes dans des environnements difficiles : fabrication, industries, hydrocarbures, services publics et armée
- Accélération des calculs complexes de divers réseaux neuronaux pour les applications d'inférence par apprentissage profond (notamment la reconnaissance d'images, la détection d'objets et l'analyse de données) grâce aux processeurs Intel® Xeon® Scalable dotés de la fonction Intel® Deep Learning Boost
- Rationalisation du déploiement de l'inférence d'apprentissage profond des types de données int8 grâce à la Distribution Intel® du kit d'outils OpenVINOTM

Caractéristiques principales

- Résiste aux environnements difficiles : poussière, haute altitude, risques d'incendie, régions à haut risque sismique et températures ambiantes élevées
- Facteur de forme compact 2U, 20 pouces de profondeur
- Deux processeurs Intel® Xeon® Scalable de 2e génération (nom de code Cascade Lake)
- Options d'alimentation doublée redondante CA ou CC
- Modules d'alimentation et ventilateurs redondants et remplaçables à chaud
- Mémoire supérieure, E/S flexibles et options de stockage
- Jusqu'à six disques durs de 2,5 pouces remplaçables à chaud
- Jusqu'à deux modules de stockage NVMe ou SATA en M.2
- Jusqu'à sept emplacements d'extension PCIe pour intégrer la plupart des cartes PCIe d'accélération des E/S
- Alimentation auxiliaire pour une carte PCIe de plus de 75 W fournie directement par une carte de distribution électrique interne
- Architecture évolutive permettant la prise en charge d'une variété de systèmes d'exploitation

Historique des révisions

Révision	Brève description des modifications	Date d'émission
1.0	Traduction de la version anglaise de janvier 2023	Février 2025

Garantie limitée

Veuillez vous reporter aux termes et conditions complets de la garantie standard sur le site Web de Kontron à l'adresse suivante : https://www.kontron.com/support-and-services/rma/canada/standard_warranty_policy_canada.pdf.

Conditions générales d'utilisation

Kontron garantit ses produits conformément aux périodes de garantie régionales définies. Pour plus d'informations sur la conformité et le respect de la garantie, ainsi que sur la période de garantie dans votre région, visitez le https://www.kontron.com/terms-and-conditions.

Kontron vend des produits dans le monde entier et déclare des conditions générales de vente et des conditions de commande régionales. Visitez le https://www.kontron.com/terms-and-conditions.

Pour obtenir des informations de contact, reportez-vous aux coordonnées des bureaux de l'entreprise figurant à la dernière page de ce guide de l'utilisateur ou visitez notre site Web.

Service à la clientèle

En tant qu'innovateur technologique de confiance et fournisseur de solutions globales, Kontron étend ses forces sur le marché de l'embarqué à un portefeuille de services permettant aux entreprises de briser les barrières des cycles de vie traditionnels des produits.

Une expertise produit éprouvée associée à un soutien collaboratif et hautement expérimenté permet à Kontron d'offrir une tranquillité d'esprit exceptionnelle pour construire et maintenir des produits performants.

Pour plus de détails sur les offres de service de Kontron, y compris les services de réparation améliorés, la garantie étendue et l'académie de formation Kontron, visitez https://www.kontron.com/en/support-and-services.

L'équipe du soutien technique de Kontron peut être jointe par les moyens suivants :

- Par téléphone : 1-888-835-6676
- Par courriel : support-na@kontron.com
- Via le site Web : www.kontron.com

Commentaires des clients

Si vous avez des difficultés à utiliser ce guide d'utilisation, si vous découvrez une erreur ou si vous souhaitez simplement faire part de vos commentaires, contactez Kontron. Détaillez les erreurs que vous trouvez. Nous corrigerons les erreurs ou les problèmes dès que possible et nous afficheront le nouveau guide dans notre site Web.

Symboles

Les symboles suivants sont utilisés dans la documentation de Kontron.

⚠DANGER	DANGER indique une situation dangereuse qui, si elle n'est pas évitée, entraînera la mort ou des blessures graves.
⚠WARNING	WARNING (AVERTISSEMENT) indique une situation dangereuse qui, si elle n'est pas évitée, pourrait entraîner la mort ou des blessures.
NOTICE	NOTICE (AVIS) indique un message de dommages matériels.
⚠CAUTION	CAUTION (ATTENTION) indique une situation dangereuse qui, si elle n'est pas évitée, peut entraîner des blessures mineures ou modérées.
	**Choc électrique!** Ce symbole et ce titre mettent en garde contre les risques de chocs électriques (> 60 V) en cas de contact avec des produits ou des parties de produits. Le non-respect des précautions indiquées et/ou prescrites par la loi peut mettre en danger votre vie/santé et/ou entraîner des dommages matériels. Veuillez également vous reporter à la section Instructions de sécurité pour la haute tension ci-dessous.
	**Appareil sensible aux décharges électrostatiques!** Ce symbole et ce titre indiquent que les cartes électroniques et leurs composants sont sensibles à l'électricité statique. Des précautions doivent donc être prises lors de toutes les opérations de manipulation et d'inspection de ce produit afin d'en garantir l'intégrité à tout moment.
	**Surface chaude!** Ne pas toucher! Laisser refroidir avant de procéder à l'entretien.
	Ce symbole indique des informations générales sur le produit et la documentation. Ce symbole indique également des informations détaillées sur la configuration spécifique du produit.
	Ce symbole précède des conseils utiles et des astuces pour l'utilisation quotidienne.

Table of Contents

List of Tables

List of Figures

1/ Informations sur la sécurité et la réglementation

NOTICE

Avant de travailler avec ce produit ou d'exécuter les instructions décrites dans la section Guide de démarrage ou dans d'autres sections, lire la section Informations sur la sécurité et la réglementation propre au produit. Les instructions d'assemblage contenues dans cette documentation doivent être suivies pour garantir et maintenir la conformité avec les certifications et approbations existantes associées au produit. Utiliser uniquement les composants décrits et réglementés spécifiés dans cette documentation. L'utilisation d'autres produits/composants annulera la certification CSA et les autres approbations réglementaires du produit et entraînera très probablement une non-conformité avec les réglementations relatives au produit dans la ou les régions dans lesquelles le produit est vendu.

1.1. Avertissements et précautions de sécurité d'ordre général

⚠WARNING

Pour éviter tout risque d'incendie ou d'électrocution, ne pas exposer ce produit à la pluie ou à l'humidité. Le châssis ne doit pas être exposé à des gouttes ou à des éclaboussures de liquides et aucun objet rempli de liquide ne doit être placé sur le capot du châssis.

Appareil sensible aux ESD!

Cet équipement est sensible à l'électricité statique. Des précautions doivent donc être prises lors de toutes les opérations de manipulation et d'inspection de ce produit afin d'en garantir l'intégrité à tout moment.

⚠CAUTION

L'étagère dans laquelle l'équipement est installé doit permettre une circulation d'air suffisante vers l'avant du serveur pour assurer un refroidissement adéquat.

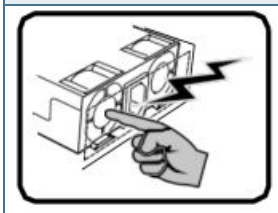
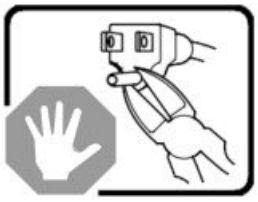
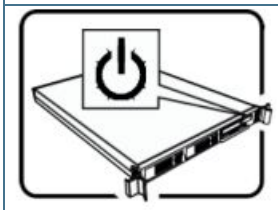
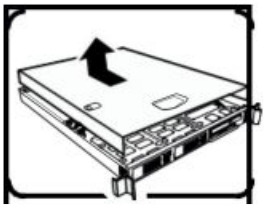
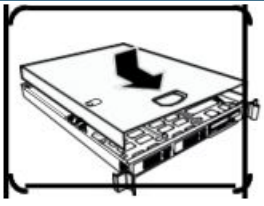
1.2. Température ambiante de fonctionnement élevée

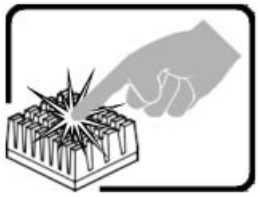
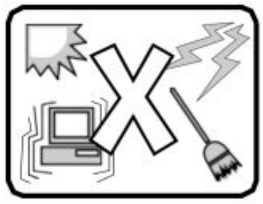
Si ce produit est installé dans une baie fermée ou à plusieurs unités, la température ambiante de fonctionnement dans l'environnement de la baie pourrait être supérieure à la température ambiante de la pièce. Par conséquent, veiller à installer le produit dans un environnement compatible avec la température maximale de fonctionnement indiquée par le fabricant dans les spécifications.

1.3. Charge mécanique

Ne pas charger l'équipement de manière inégale lors du montage de ce produit dans une étagère (rack), car cela pourrait créer des conditions dangereuses.

1.4. Précautions diverses

	Le bloc d'alimentation de ce produit ne contient aucune pièce pouvant être réparée par l'utilisateur. Ce produit peut contenir plus d'un bloc d'alimentation. Veuillez contacter un technicien qualifié en cas de problème.
	Ne pas tenter de modifier ou d'utiliser le cordon d'alimentation CA fourni s'il n'est pas du type exact requis. Le nombre de cordons d'alimentation CA fournis correspond au nombre de blocs d'alimentation du produit.
	Notez que le commutateur CC de mise sous tension/hors tension du panneau avant n'éteint pas l'alimentation CA du système. Pour mettre le système hors tension, vous devez débrancher chaque cordon d'alimentation de sa prise. Les cordons (ou le cordon) d'alimentation sont considérés comme le dispositif de déconnexion principal de l'alimentation CA. La prise de courant sur laquelle le système se branche doit être installée à proximité de l'équipement et être facilement accessible.
 	CONSIGNES DE SÉCURITÉ – Avant d'ouvrir le capot du châssis pour accéder à l'intérieur du système, suivez les consignes suivantes : 1. Mettez hors tension tous les périphériques connectés au système. 2. Éteignez le système en appuyant sur le bouton d'alimentation. 3. Débranchez tous les cordons d'alimentation CA du système ou des prises murales. 4. Identifiez et débranchez tous les câbles reliés aux connecteurs d'E/S ou aux ports derrière le système. 5. Pour prévenir les décharges électrostatiques lorsque vous touchez aux composants, portez un bracelet antistatique et reliez-le à la mise à la terre du châssis (toute surface métallique non peinte du châssis). Une fois les six CONSIGNES DE SÉCURITÉ respectées, vous pouvez retirer le capot : Procédez comme suit : 1. Si un cadenas a été installé sur à l'arrière du système, déverrouillez-le et retirez-le. 2. Retirez toutes les vis du capot et mettez-les dans un endroit sûr. 3. Retirez le capot. 4. N'utilisez pas le système lorsque la capot du châssis est retiré.
	Afin de permettre le refroidissement et l'aération du système, réinstallez toujours le capot du châssis avant de mettre le système sous tension. Faire fonctionner le système sans son capot installé risque d'endommager ses composants. Pour installer le capot : 1. Assurez-vous de ne pas avoir oublié d'outils ou de pièces démontées dans le système. 2. Assurez-vous que les câbles, les cartes d'expansion et les autres composants sont bien installés. 3. Revissez solidement le capot du châssis avec les vis retirées plus tôt. 4. Remettez le cadenas en place et verrouillez-le afin de prévenir tout accès non autorisé à l'intérieur du système. 5. Rebranchez tous les cordons d'alimentation CA et câbles externes au système.

	Le processeur et le dissipateur thermique peuvent être chauds si le système a été sous tension. Faites également attention aux broches aiguës des cartes et aux bords tranchants du capot. Nous vous recommandons l'usage de gants de protection.
	Danger d'explosion si la batterie n'est pas remontée correctement. Remplacer uniquement avec une batterie du même type ou d'un type équivalent recommandé par le fabricant. Disposez des piles usées selon les instructions du fabricant.
	Le système a été conçu pour fonctionner dans un environnement de bureau typique. L'emplacement choisi doit être : Propre et dépourvu de poussière en suspension (sauf la poussière normale). Bien ventilé et éloigné des sources de chaleur, y compris de la lumière directe du soleil. À l'abri des chocs et des sources de vibrations. Isolé de forts champs électromagnétiques générés par des appareils électriques. Dans les régions sujettes aux orages électriques, il est recommandé de brancher le système dans un limiteur de surtension, et de débrancher toutes les lignes de télécommunications de votre modem durant un orage. Muni d'une prise murale correctement mise à la terre. Suffisamment spacieux pour vous permettre d'accéder aux cordons d'alimentation (ceux-ci étant le seul moyen de mettre le système hors tension).

Ce produit est généralement équipé de plus d'un cordon d'alimentation. Débrancher tous les cordons d'alimentation avant toute intervention sur le produit afin d'éviter tout risque de choc électrique.

⚠WARNING

L'installation de ce produit doit être effectuée conformément aux codes de câblage nationaux et aux réglementations locales.

1.5. Surcharge de circuit

Ne pas surcharger les circuits lorsque ce produit est connecté au circuit d'alimentation, car cela peut nuire à la protection contre les surintensités et au câblage d'alimentation. Vérifier la plaque signalétique de l'équipement d'alimentation afin de connaître ses caractéristiques nominales pour une utilisation adéquate.

1.6. Sécurité – blocs d'alimentation CA

1.6.1. Dispositif principal de déconnexion de l'alimentation CA

Les cordons (ou le cordon) d'alimentation CA sont considérés comme le dispositif de déconnexion principal du serveur et doivent être facilement accessibles une fois installés. Si les cordons (ou le cordon) d'alimentation de chaque serveur ne sont pas accessibles facilement pour permettre leur débranchement, vous êtes responsable d'installer un dispositif de déconnexion de l'alimentation CA pour l'ensemble de l'étagère. Ce dispositif de déconnexion électrique doit être facilement accessible et doit être étiqueté de façon à ce qu'il soit clair qu'il contrôle l'alimentation de l'ensemble de l'étagère, et pas seulement celle du ou des serveurs.

1.6.2. Mise à la terre fiable

Pour éviter tout risque de choc électrique, il faut inclure un troisième conducteur de mise à la terre avec l'installation de l'étagère. Si le cordon d'alimentation du serveur est branché dans une prise CA qui fait partie de l'étagère, il faut prévoir une mise à la terre adéquate pour l'étagère elle-même. Si le cordon d'alimentation du serveur est branché dans une prise murale CA, le conducteur de mise à la terre du cordon d'alimentation assure une mise à la terre adéquate pour le serveur uniquement. Il est requis de prévoir une mise à la terre supplémentaire et appropriée pour l'étagère et les autres périphériques qui y sont installés.

1.6.3. Protection contre les surintensités

Le serveur est conçu pour une source de tension d'entrée CA avec une protection contre les surintensités allant jusqu'à 20 ampères par cordon d'alimentation. Si le système d'alimentation pour l'étagère destinée à l'équipement est installé sur un circuit de dérivation dont la protection est supérieure à 20 ampères, il est requis de fournir une protection supplémentaire pour le serveur. La consommation de courant nominale totale d'un serveur configuré est inférieure à 6 ampères.

⚠WARNING

Ne pas tenter de modifier ou d'utiliser un jeu de cordons d'alimentation CA qui n'est pas du type exact requis. Un jeu de cordons d'alimentation répondant aux critères suivants doit être utilisé :

Classification

États-Unis et Canada

Les cordons doivent être homologués UL (Underwriters' Laboratories, Inc.) ou certifiés CSA (Association canadienne de normalisation) – type SJT, calibre AWG no 18, 3 conducteurs.

Hors des États-Unis et du Canada

Les cordons doivent être de type souple harmonisé ou certifiés VDE (Verbena Deutscher Electrotechniker, Institut allemand des ingénieurs en électricité) avec 3 conducteurs de 0,75 mm classifiés 250 VCA.

Connecteur, côté prise murale

L'extrémité des cordons doit être une fiche mâle avec mise à la terre conçue pour être utilisée dans votre région. Le connecteur doit porter des marques d'homologation attestant d'une certification par un organisme reconnu dans votre région et, pour les États-Unis, il doit être homologué et classifié pour 125 % de la consommation de courant nominale totale du serveur. Connecteur, côté serveur

Les connecteurs qui se branchent sur la prise CA du serveur doivent être des connecteurs femelles homologués IEC (Commission électrotechnique internationale) 320, fiche C13.

Longueur et flexibilité du cordon

Les cordons doivent avoir une longueur inférieure à 4,5 mètres (14,8 pieds).

1.7. Sécurité – blocs d'alimentation CC

Les plateformes équipées de blocs d'alimentation CC doivent être installées dans une zone d'accès restreint conformément aux articles 110 - 26 et 110 - 27 du National Electric Code, ANSI/NFPA 70. Lorsqu'il est alimenté en courant continu, cet équipement doit être protégé par un dispositif de protection du circuit de dérivation homologué d'un calibre maximale de 25 A. La source de courant continu doit être isolée électriquement de toute source de courant alternatif dangereuse par une isolation double ou renforcée. La source de courant continu doit pouvoir fournir jusqu'à 1000 watts de puissance continue par paire de cordons.

Les blocs d'alimentation CC sont protégés contre l'inversion de polarité par des diodes internes et ne fonctionneront pas si le câblage est incorrect.

⚠CAUTION Cet appareil est conçu pour que le conducteur de mise à la terre (retour) du circuit d'alimentation en courant continu soit connecté au conducteur de mise à la terre de l'appareil (cosse de mise à la terre).

1.7.1. Dispositif principal de déconnexion de l'alimentation CC

Un dispositif de déconnexion de l'alimentation CC possédant la classification appropriée doit être installé pour le serveur. Ce dispositif de déconnexion électrique doit être facilement accessible et doit être étiqueté de façon à ce qu'il soit clair qu'il contrôle l'alimentation du serveur. Le disjoncteur homologué UL d'un système centralisé d'alimentation CC peut être utilisé comme dispositif de déconnexion électrique s'il est facilement accessible.

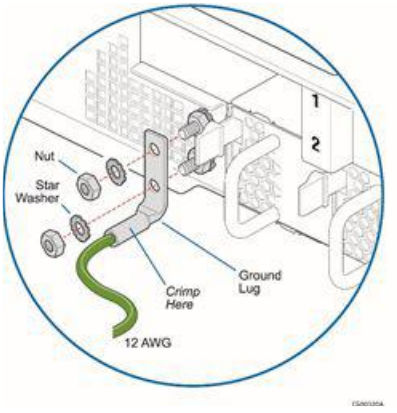
1.7.2. Protection contre les surintensités

Des disjoncteurs de protection contre les surintensités homologués UL doivent être fournis dans chaque étagère destinée à l'équipement et doivent être intégrés au câblage installé entre la source CC et le serveur. Le dispositif de protection du circuit de dérivation doit avoir une classification minimum de 75 VCC, et de maximum 25 A par paire de cordons.

1.7.3. Mise à la terre fiable

Ce serveur est conçu pour être installé avec un retour CC isolé (CC- I selon la norme NEBS GR-1089, édition 3). Pour éviter tout risque de choc électrique, il est requis de connecter de manière fiable un conducteur de mise à la terre au serveur. Le conducteur de mise à la terre doit avoir un calibre minimal AWG no 10 et être connecté aux goujons de mise à la terre situés à l'arrière du serveur. Le conducteur de mise à la terre de sécurité doit être connecté aux goujons du châssis à l'aide d'une cosse à sertir à deux trous, fermée et homologuée, avec un pas de 5/8 de pouce. Les écrous des goujons de mise à la terre du châssis doivent être installés avec un couple de 10 lb-po. Le conducteur de mise à la terre de sécurité assure une mise à la terre adéquate uniquement pour le serveur. Il est requis de prévoir une mise à la terre supplémentaire et appropriée pour l'étagère et les autres périphériques qui y sont installés.

Figure 1. Emplacement de la cosse de mise à la terre



1.8. Spécifications réglementaires

La plateforme répond aux exigences des tests et normes réglementaires suivants :

Tableau 1. Conformité en matière de sécurité

États-Unis/Canada	Ce produit porte la marque cCSAus. Ce produit est conforme aux normes UL 60950-1 2e édition et CSA C22.2 no 60950-1-07 2e édition.
Europe	Ce produit porte la marque CE et est conforme à la directive basse tension 2014/35/UE et à la norme EN 62368-1.
International	Ce produit détient un rapport CB et un certificat associé à la norme IEC 62368-1.

Tableau 2. Compatibilité électromagnétique

États-Unis/Canada	Ce produit est conforme à la norme FCC Title 47 Part 15/ICES-003 Class A.
Europe	Ce produit porte la marque CE et est conforme à la directive 2014/30/UE relative à la compatibilité électromagnétique sur la base des normes suivantes : EN55032, Limite de Classe A, Émissions rayonnées et conduites EN55035 Immunité EN61000 - 4 - 2 Immunité aux décharges électrostatiques EN61000 - 4 - 3 Immunité aux champs électromagnétiques rayonnés EN61000 - 4 - 4 Transitoires électriques rapides en salves EN61000 - 4 - 5 Ondes de choc EN61000 - 4 - 6 Immunité aux perturbations conduites, induites par les champs radioélectriques EN61000 - 4 - 11 Creux de tension, coupures brèves et variations de tension EN61000 - 3 - 2 Courants harmoniques EN61000 - 3 - 3 Fluctuations de tension et flicker.
Australie/Nouvelle-Zélande	Ce produit est conforme à la norme AS/NZS CISPR 32 Class A Limit. Ce produit est marqué RCM.
Japon	Ce produit est conforme à la norme VCCI Classe A pour les équipements de technologie de l'information (limite de Classe A de la norme CISPR 32).
Corée	Ce produit est marqué KCC.
International	Ce produit est conforme à la limite de Classe A de la norme CISPR 32 et à l'immunité selon la norme CISPR 35.

1.8.1. RoHS

Le marquage CE sur ce produit indique qu'il est conforme à la directive RoHS.

1.8.2. Directive sur les déchets d'équipements électrique et électronique

Ce produit contient des matériaux électriques ou électroniques. S'ils ne sont pas éliminés ou jetés correctement, ces matériaux pourraient avoir des effets néfastes sur l'environnement et la santé humaine. La présence de ce logo sur le produit signifie qu'il ne doit pas être jeté avec les déchets non triés et qu'il doit être récupéré séparément. Éliminer ce produit conformément aux règles, réglementations et lois locales en vigueur.

Figure 2. Logo de la directive DEEE

1.8.3. Filtre à air

Un filtre à air optionnel peut être installé derrière le panneau frontal du serveur CG2400.

Le filtre est fait de Quadrafoam UAF (25 pores par pouce), a une épaisseur de 6,35 mm, possède une cote d'inflammabilité UL94-HF1, et satisfait à la norme minimale d'arrêt de la poussière de 65 % (ASHRAE 52.1-1992) selon la documentation trouvée à http://www.uaf.com.

Le filtre à air peut être acheté directement auprès de Universal Air Filter (UAF) en appelant au 618 271-7300 ou en envoyant un courriel à uaf@uaf.com pour commander la pièce numéro K00737-001. Fournir le dessin ci-joint lorsqu'une commande est passée afin de confirmer la réception du filtre à air approprié.

Calendrier de remplacement du filtre à air recommandé : tous les 6 mois.

2/ Spécifications

2.1. Principales caractéristiques matérielles du CG2400

Tableau 3. Principales caractéristiques matérielles du CG2400

Caractéristique	Description
Système	• Conçu pour satisfaire aux normes NEBS GR-63 et GR-1089 • Conforme à la directive RoHS 6/6 • Cycle de vie prolongé (5-7 ans)
Châssis	• Renforcé, 2U x 508 mm (20 po) • Capot qui se bloque afin d'offrir une protection lors du remplacement à chaud des ventilateurs du système • Tôle externe plaquée après
Boutons du panneau avant	• Marche-arrêt • Réinitialisation du système • ID du châssis
DEL du panneau avant	• État de l'alimentation • Identification du châssis • État du système • État des ventilateurs • Activité/défaillance des disques durs • Activité des CIR • DEL d'alarme de télécom (critique, majeure, mineure, alimentation) **NOTE :** DEL installée, fonctionnalité disponible via une mise à jour du micrologiciel – à venir.
Stockage	• Jusqu'à six disques durs SAS ou disques SSD SATA de 2,5" remplaçables à chaud **NOTE :** La prise en charge des disques SAS nécessite un contrôleur RAID ou HBA PCIe supplémentaire. Voir Liste de compatibilité matérielle • Divers contrôleurs matériels SAS/RAID tiers pris en charge Voir Liste de compatibilité matérielle • Stockage flash interne pris en charge - SATA ou NVMe en M.2 (2280) Voir Liste de compatibilité matérielle • Contrôleur SATA 6 Gbps intégré avec RAID (logiciel) • Deux emplacements pour cartes SD accessibles par l'avant
Prise en charge du RAID hybride intégré	• Mise en œuvre via le jeu de puces C622 – sur la carte mère • SATA 6 ports avec prise en charge intégrée de RAID 0/1/10
Prise en charge de l'adaptateur matériel RAID	• Contrôleur RAID matériel SAS optionnel avec six ports internes et sauvegarde sans maintenance (SuperCap) (mémoire flash) o Utilisation d'un emplacement PCIe : l'emplacement 3 est celui à privilégier (support de montage inclus dans le châssis) o Le SuperCap (optionnel) a son propre support et un emplacement distinct dans le châssis
Refroidissement du système	• Six ventilateurs redondants de 80 mm remplaçables à chaud
Alimentation	• Deux blocs d'alimentation redondants de 850 W CA remplaçables à chaud, 80Plus® Platinum • Deux blocs d'alimentation redondants de 850 W CC remplaçables à chaud • Carte de distribution électrique (PDB) commune de 850 W • Prise en charge de la spécification PMBus 1.2 • Câble d'alimentation auxiliaire interne pour carte PCIe haute puissance

Caractéristique	Description
Puissance consommée	Voir section 8.2 Puissance consommée et budget énergétique
Carte	• Carte de serveur KMB-IXS100 de Kontron • Facteur de forme SSI EEB (12 po x 13 po)
Processeur	• Deux LGA3647 (socket carré) faits pour les processeurs Intel® Xeon® Scalable Voir Liste de compatibilité matérielle
Jeu de puces	• Jeu de puces Intel® C622 (PCH)
Mémoire	• 16 emplacements DIMM - 1 ou 2 emplacements DIMM par canal - 6 canaux de mémoire par processeur • Prise en charge de la mémoire DDR4 enregistrée (RDIMM) et de la mémoire DDR4 à charge réduite (LRDIMM) • Taux de transfert de données de la mémoire DDR4 allant jusqu'à 2933 MT/s* Voir Liste de compatibilité matérielle ** La vitesse maximale de la mémoire prise en charge dépend du processeur installé dans le système.*
E/S	• Prise en charge de deux cartes adaptatrices de connexion PCIe (4 cartes FL/FH) et de 3 adaptateurs LP pour un total de 7 cartes PCIe Gen 3 (6 avec E/S, 1 sans) Deux options de cartes adaptatrices de connexion pour chacun des deux emplacements PCIe o 2 emplacements pour une carte PCIe passive x8 FL/FH (côté droit* - Gen 3) o 2 emplacements pour une carte PCIe passive x8 FL/FH (côté gauche* - Gen 3) o 1 emplacement pour une carte PCIe passive x16 FL/FH (côté droit* - Gen 3) o 1 emplacement pour une carte PCIe passive x16 FL/FH (côté gauche* - Gen 3) • Panneau avant : un port série (connecteur RJ45), un port USB 2.0 • Panneau arrière : quatre ports USB 3.0, un port réseau 1000BASE-T, deux ports réseau 10GBASE-T, un port VGA, un connecteur de relais sec TAM ** Orientation à droite ou à gauche lorsqu'on regarde de l'avant du châssis.*
Gestion du serveur	• BMC intégré, voir les détails dans Principales caractéristiques logicielles du G2400 o IPMI 2.0 o Interface utilisateur Web avec KVM et redirection multimédia incluses dans le système de base **NOTE :** Aucun module supplémentaire n'est nécessaire (ex. AXXRMM4LITE dans la génération précédente de la plateforme CG).
Gestion des alarmes de télécom	• Connecteur de relais sur le panneau arrière qui prend en charge les systèmes d'alarme des stations de base **NOTE :** Disponible via une mise à jour du micrologiciel – à venir.
Vidéo	• Contrôleur graphique vidéo 2D intégré

NOTES :

1. L'utilisation de disques durs rotatifs SATA n'est pas recommandée dans ce système, car ils sont sensibles aux vibrations rotatives causées par les pales des ventilateurs du système et par d'autres disques durs.
2. Les disques peuvent consommer jusqu'à 12 W de puissance chacun. Les disques utilisés dans ce système doivent être spécifiés pour fonctionner à une température ambiante maximale de 40 ºC.

2.2. Principales caractéristiques logicielles du CG2400

Tableau 4. Principales caractéristiques logicielles du CG2400

Caractéristique	Description
Gestion de la plateforme	BMC intégré – ce sous-système comprend les bus de communication, les capteurs, le BIOS du système et le micrologiciel de gestion du serveur; il prend en charge les fonctionnalités IPMI standard ainsi que les fonctionnalités (supplémentaires) du constructeur OEM qui ne font pas partie d'IPMI • Prise en charge des fonctionnalités d'IPMI 2.0 • Mise à jour et maintenance des micrologiciels • Surveillance des ventilateurs • Prise en charge des ventilateurs remplaçables à chaud • Écran-clavier-souris (KVM) intégré Redirection KVM • Prise en charge et surveillance de la redondance des blocs d'alimentation • Prise en charge de la gestion des blocs d'alimentation compatibles avec le bus de gestion de l'alimentation (PMBus) 1.2 • Gestion du panneau avant comprenant une DEL d'état du système et une DEL pour l'identification du châssis (s'allume/s'éteint à l'aide d'un bouton sur le panneau avant ou d'une commande) Interface utilisateur du serveur Web intégrée • Améliorations apportées au serveur Web intégré : o SEL lisible en clair o Configurations supplémentaires offertes pour le système Capacités supplémentaires de surveillance du système Gestion acoustique • Prise en charge du gestionnaire de nœuds d'alimentation • Prise en charge de la gestion thermique • Surveillance de l'état du système de gestion du BMC • Alerte par courriel • Redirection multimédia à distance intégrée • Protocole allégé d'accès annuaire (LDAP) • Stockage et récupération de l'identificateur global unique (GUID) du système Fonctionnalités d'IPMI 2.0 • Horloge de surveillance IPMI (watchdog timer) • Prise en charge de la messagerie, y compris le pontage des commandes et la prise en charge des utilisateurs/sessions • Fonctionnalités reliées au châssis (chassis device), y compris la prise en charge du contrôle de l'alimentation et de la réinitialisation ainsi que des indicateurs d'amorçage du BIOS • Fonction SEL • Accès aux enregistrements de données des capteurs (SDR) du système • Gestion et interrogation des capteurs pour surveiller et signaler l'état du système • Série sur LAN (SOL) • Synchronisation de l'état ACPI selon les changements d'état fournis par le BIOS • Interfaces IPMI : o Interfaces hôtes comprenant le logiciel de gestion du système (SMS) avec prise en charge de la file d'attente des messages reçus, le mode de gestion du serveur (SMM) et l'interface du bus de gestion de la plateforme intelligente (IPMB) o Interface LAN prenant en charge le protocole IPMI sur LAN (RMCP, RMCP+)
Système d'exploitation	Voir Systèmes d'exploitation validés
Gestion thermique	• Interface de contrôle de l'environnement de la plateforme (PECI) pour la gestion thermique • Gestion thermique du CPU

2.3. Dimensions physiques du CG2400

Tableau 5. Dimensions physiques du CG2400

Châssis	Measures (mm [po])	Notes
Profondeur	508 [20] max.	Châssis
Largeur	435,3 [17,14] max.	Châssis
Hauteur	87,6 [3,45] max.	Châssis
Dégagement latéral	25 [1]	Entre les points de montage dans l'étagère
Dégagement avant	76 [2]	Recommandé
Dégagement arrière	92 [3,6]	Recommandé

2.4. Dimensions physiques de l'emballage du CG2400

Tableau 6. Dimensions physiques de l'emballage du CG2400

Profondeur (mm [po])	Largeur (mm [po])	Hauteur (mm [po])
675 [26,57]	550 [21,65]	210 [8,27]

2.5. Poids à l'expédition du CG2400

Tableau 7. Poids à l'expédition du CG2400

Composant	Poids (kg)	Poids (lb)
Poids du système – configuration complète (tous les adaptateurs PCIe, blocs d'alimentation CA ou CC)	20,0	44,0
Poids du système – configuration de base (tel qu'expédié de l'usine)	14,0	30,8
Emballage (boîte + mousse + sac)	2,8	6,2
Bloc d'alimentation (CA ou CC)	1,1	2,4

2.6. Spécifications environnementales du CG2400

Tableau 8. Spécifications environnementales du CG2400

Environnement	Spécifications
Température, en fonctionnement	-5 ºC à +55 ºC (+23 ºF à +131 ºF)
Température, hors fonctionnement	-40 ºC à +70 ºC (-40 ºF à +158 ºF)
Humidité, en fonctionnement	5 % à 85 %
Humidité, hors fonctionnement	95 %, sans condensation
Altitude, en fonctionnement	-60 m à 1 800 m (-197 pi à 5 906 pi) sans déclassement de la plage de températures 3 900 m (12 795 pi) 40 ºC
Vibrations, en fonctionnement	Ce produit est conforme aux exigences en matière de vibrations aléatoires en fonctionnement Profil d'essai basé sur GR-63, clause 5.4.2 Office vibration levels et ETSI EN 300 019-1-4

Environnement	Spécifications
Vibrations, hors fonctionnement	Ce produit est conforme aux exigences en matière de vibrations aléatoires lors du transport et du stockage Profil d'essai basé sur GR-63, clause 5.4.3 Transportation vibration - packaged equipment et ETSI EN 300 019-2-2 class 2.3
Choc, en fonctionnement	Ce produit est conforme aux normes en matière de chocs en fonctionnement Profil d'essai basé sur ETSI EN 300 019-2-3 class 3.2 (IEC 60068-2-27)
Acoustique	Ce produit satisfait ou dépasse les exigences de GR-63 et d'ETSI EN 300 753
Chute libre	Ce produit est conforme à la norme GR-63, clause 4.3.1
Décharge électrostatique	Ce produit est conforme à la méthode d'essai IEC 61000-4-2 pour une décharge au contact de 8 kV et une décharge dans l'air de 15 kV
DEEE	Ce produit est conforme à la directive européenne 2012/19/EU (DEEE)

3/ Composants de la plateforme

3.1. Panneau avant de la plateforme

Figure 3. Panneau avant de la plateforme

Tableau 9. Éléments du panneau avant

Élément	Description	Élément	Description
A	Boutons de contrôle, et DEL des états et des alarmes de télécom sur le panneau avant	C	Port USB 2.0
B	Port série RJ45	D	Vis captive du panneau frontal

Figure 4. Panneau avant de la plateforme populé

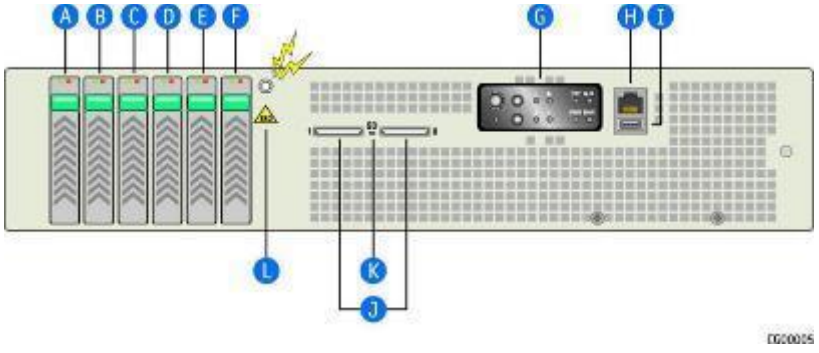


Tableau 10. Éléments du panneau avant populé

Élément	Description	Élément	Description
A	Emplacement de disque 5	G	Boutons de contrôle, et DEL des états et des alarmes de télécom sur le panneau avant
B	Emplacement de disque 4	H	Port série RJ45
C	Emplacement de disque 3	I	Port USB 2.0
D	Emplacement de disque 2	J	Emplacements pour cartes flash SD
E	Emplacement de disque 1	K	DEL du module flash SD
F	Emplacement de disque 0	L	Fixation pour le bracelet antistatique

Figure 5. Boutons et DEL de la plateforme

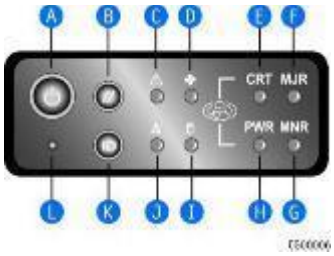


Tableau 11. Boutons et DEL de la plateforme

Élément	Description	Élément	Description
A	Bouton d'alimentation	G	Alarme mineure (ambre)
B	Bouton de réinitialisation du système	H	Alarme d'alimentation (ambre)
C	DEL d'état du système	I	DEL d'activité des disques
D	DEL d'état des ventilateurs	J	DEL d'activité des CIR
E	Alarme critique (ambre)	K	Bouton d'identification du châssis
F	Alarme majeure (ambre)	L	Bouton NMI

3.2. Panneau arrière de la plateforme

Figure 6. Panneau arrière de la plateforme

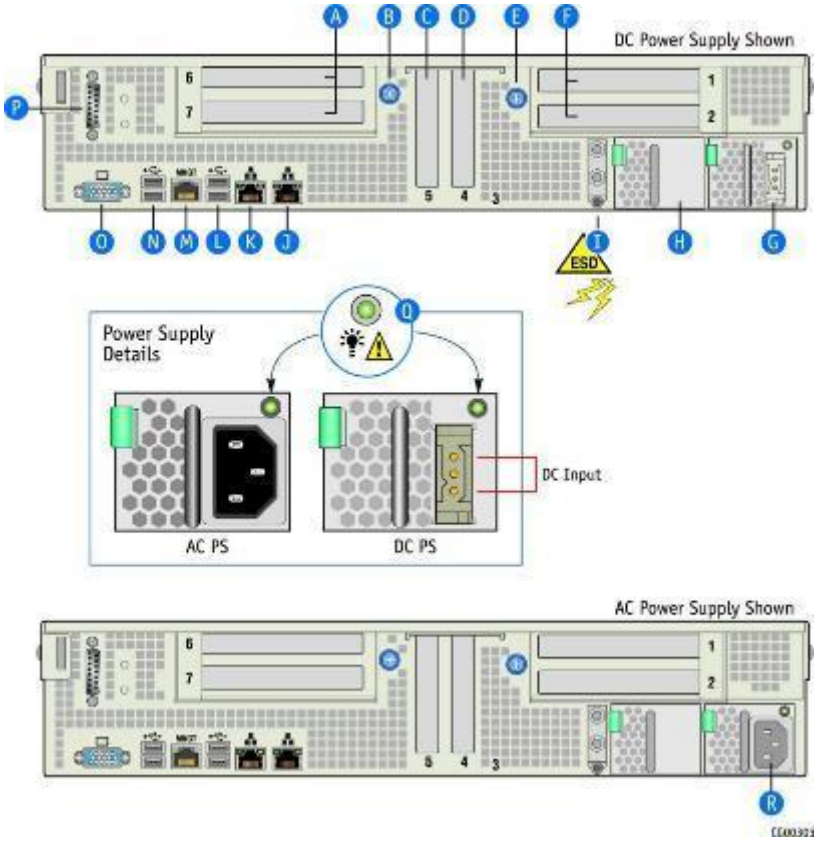


Tableau 12. Éléments du panneau arrière de la plateforme

Élément	Description	Élément	Description
A	Assemblage PCIe FL/FH à 2 emplacements de droite1 (emplacements 6 et 7)	J	CIR2 GbE
B	Vis à serrage à main pour fixer l'assemblage PCIe de droite (A)	K	CIR1 GbE
C	Adaptateur PCIe LP (emplacement 5)	L	USB 3 et USB 4 (tous deux des USB 3.0 et USB 3 est celui du dessus)
D	Adaptateur PCIe LP (emplacement 4)	M	CIR dédié de gestion du serveur
E	Vis à serrage à main pour fixer l'assemblage PCIe de gauche (F)	N	USB 1 et USB 2 (tous deux des USB 3.0 et USB 1 est celui du dessus)
F	Assemblage PCIe FL/FH à 2 emplacements de gauche (emplacements 1 et 2)	O	Connecteur vidéo
G	Bloc d'alimentation 1 (illustré avec le bloc d'alimentation CC installé)	P	Connecteur de relais sec TAM
H	Bloc d'alimentation 2 optionnel (illustré avec le panneau de remplissage)	Q	DEL des blocs d'alimentation
I	Cosse de mise à la terre du châssis	R	Bloc d'alimentation 1 (illustré avec l'alimentation CA installée)

NOTES :

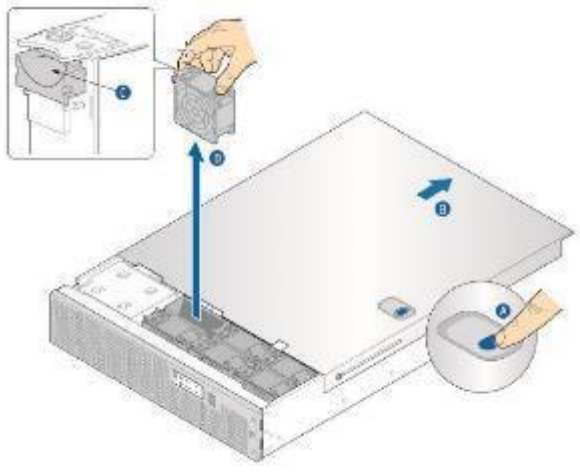
1. La notion de droite et de gauche pour les assemblages PCIe est établie en faisant face à l'avant du système.

2. Dans les configurations non redondantes, un panneau de remplissage doit être installé sur l'emplacement du bloc d'alimentation 2.

3.3. Module de ventilation de la plateforme

La plateforme CG2400 est équipée d'un module contenant 6 ventilateurs remplaçables à chaud. Aucune interruption de service n'est généralement nécessaire pour remplacer les ventilateurs. Suivre les instructions ci-dessous pour assurer l'entretien d'un ventilateur.

Figure 7. Module de ventilation de la plateforme



Étape_1	Appuyer sur le bouton de déverrouillage rapide (A) situé sur le capot supérieur.

Étape_2	Faire glisser le capot supérieur (B) vers l'arrière jusqu'à la traverse de support de manière à ce que les ventilateurs et les câbles du CPU situés derrière eux soient visibles.
Étape_3	Retirer le ventilateur (D) en saisissant les deux côtés de l'assemblage du ventilateur, en utilisant le protège-doigts en plastique (C) sur le côté gauche et en tirant le ventilateur hors du boîtier métallique qui abrite les ventilateurs et les câbles d'alimentation.

3.4. Blocs d'alimentation

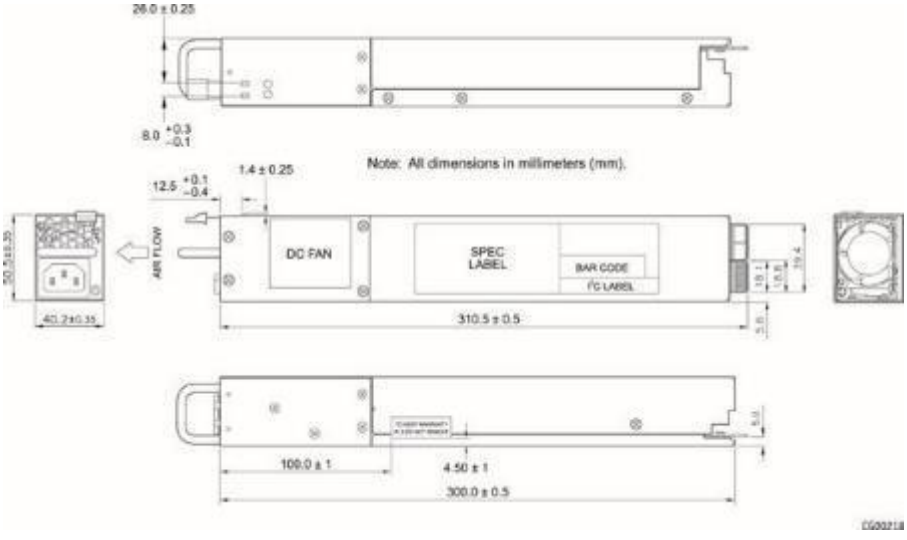
3.4.1. Sous-système d'alimentation CA

Le sous-système d'alimentation CA comporte jusqu'à deux blocs d'alimentation CA redondants et une carte de distribution électrique. Bien que cette sortie d'alimentation puisse fournir jusqu'à 850 W, la consommation électrique maximale estimée du système inscrite sur l'étiquette (située sur le capot supérieur) est calculée à partir d'une configuration maximale théorique. Une configuration maximale typique consommera beaucoup moins de puissance.

Le sous-système d'alimentation d'entrée CA présente les caractéristiques suivantes :

- Capacité de sortie du module d'alimentation de 850 W sur toute la plage de tension d'entrée CA
- DEL d'indication de bonne alimentation
- Avertissement prédictif de défaillance de ventilateur
- Ventilateurs de refroidissement internes à plusieurs vitesses
- Circuit CA_OK pour la protection contre les réductions de tension et le rétablissement
- Protection contre les réductions de tension et le rétablissement
- Capacité de répartition de la charge intégrée
- Capacité de protection contre les surcharges intégrée
- Informations sur les unités remplaçables par l'utilisateur (FRU) embarquées
- Interface PMBus 1.2 pour les fonctions de gestion du serveur
- Poignée intégrée pour insertion/extraction à chaud
- Le bloc d'alimentation contient un ventilateur de 40 mm

Figure 8. Sous-système d'alimentation CA



3.4.1.1. Exigences en matière de tension et de courant – CA

Le connecteur d'entrée d'alimentation CA est un connecteur d'entrée CA standard IEC320 C14.

Tableau 13. Caractéristiques CA

Tension d'entrée	
Nominal 110 VRMS (ligne basse)	
Minimum	90 VRMS
Plage standard	100-127 VRMS
Maximum	132 VRMS
Nominal 220 VRMS (ligne haute)	
Minimum	180 VRMS
Plage standard	200-240 VRMS
Maximum	264 VRMS
Tension de démarrage	85 VRMS ±5 VRMS
Tension d'arrêt	75 VRMS ±5 VRMS
Courant d'entrée	
Maximum	12 A à 100 VRMS / 6 A à 200 VRMS
Fréquence	
Minimum	47 Hz
Plage standard	50/60 Hz
Maximum	63 Hz

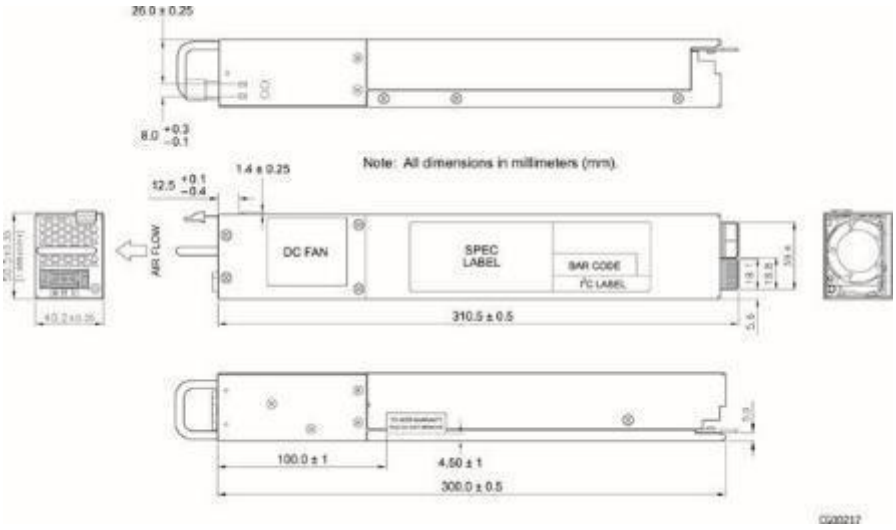
3.4.2. Sous-système d'alimentation CC

Le sous-système d'alimentation CC comprend jusqu'à deux modules d'alimentation CC capables de fonctionner en mode redondant, ainsi qu'une carte de distribution électrique. Bien que cette sortie d'alimentation puisse fournir jusqu'à 850 W, la consommation électrique maximale estimée du système inscrite sur l'étiquette (située sur le capot supérieur) est calculée à partir d'une configuration maximale théorique. Une configuration maximale typique consommera beaucoup moins de puissance.

Le sous-système d'alimentation d'entrée CC présente les caractéristiques suivantes :

- Capacité de sortie du module d'alimentation de 850 W sur toute la plage de tension d'entrée CC
- DEL d'indication de bonne alimentation
- Avertissement prédictif de défaillance de ventilateur
- Ventilateurs de refroidissement internes à plusieurs vitesses
- Circuit CC_OK pour la protection contre les réductions de tension et le rétablissement
- Capacité de répartition de la charge intégrée
- Capacité de protection contre les surcharges intégrée
- Informations sur les unités remplaçables par l'utilisateur (FRU) embarquées
- Interface PMBus 1.2 pour les fonctions de gestion du serveur
- Poignée intégrée pour insertion/extraction à chaud
- Le bloc d'alimentation contient un ventilateur de 40 mm

Figure 9. Sous-système d'alimentation CC



3.4.2.1. Exigences en matière de tension et de courant – CC

NOTE : Le courant maximal indiqué dans le tableau ci-dessous est le courant maximal que le système tirera du bloc d'alimentation à une tension d'entrée de -48 V.

Tableau 14. Caractéristiques CC

Tension d'entrée CC	
Nominal	-48 VCC
Minimum[1]	-40 VCC
Plage standard	-48 VCC à -72 VCC
Maximum	-75 VCC
Courant d'entrée CC	
Maximum	30 A à -40 VCC, 15 A à -72 VCC

[1] La tension d'entrée CC minimale en régime permanent à laquelle l'équipement reste pleinement opérationnel est de -40 VCC.

3.5. Comportement des boutons et des DEL de la plateforme

3.5.1. Panneau avant

Figure 10. Boutons et DEL de la plateforme - comportement

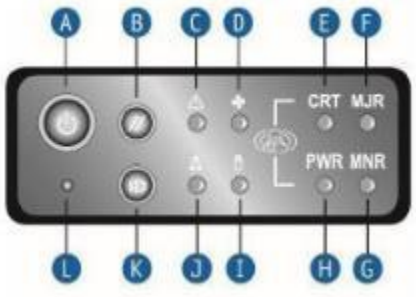


Tableau 15. Comportement des boutons et DEL de la plateforme

Élément	Description du bouton/de la DEL	Couleur	État	Description
A	Alimentation/veille (bouton de marche)	Vert	Allumée	Marche / état ACPI S0
		Vert	Clignotante	Veille / état ACPI S1
		-	Éteinte	Arrêt / état ACPI S4 ou S5
B	Bouton de réinitialisation du système			Bouton uniquement, pas de DEL
C	État du système	Vert	Allumée	Système prêt / fonctionnement normal
		Vert	Clignotante	Système prêt, mais dégradé
		Ambre	Allumée	État critique ou irrécupérable
		-	Éteinte	Système non prêt : POST / arrêt du système
D	État des ventilateurs	Ambre	Allumée	Défaillance de ventilateur
		-	Éteinte	Sous-système ventilateur OK - pas de défaillance
E	Alarme critique **NOTE :** Pris en charge à partir de la BMC 2.9.0955AB31	Ambre	Allumée	Condition de niveau critique activée
		-	Éteinte	Aucune condition de niveau critique ou condition désactivée
F	Alarme majeure **NOTE :** Pris en charge à partir de la BMC 2.9.0955AB31	Ambre	Allumée	Condition de niveau majeur activée
		-	Éteinte	Aucune condition de niveau majeur ou condition désactivée
G	Alarme mineure **NOTE :** Pris en charge à partir de la BMC 2.9.0955AB31	Ambre	Allumée	Condition de niveau mineur activée
		-	Éteinte	Aucune condition de niveau mineur ou condition désactivée
H	Alarme d'alimentation **NOTE :** Pris en charge à partir de la BMC 2.9.0955AB31	Ambre	Allumée	Condition du sous-système d'alimentation activée
		-	Éteinte	Aucune condition d'alimentation ou condition désactivée
I	Activité des disques	Vert	Clignotante	Activité des disques durs
		Ambre	Allumée	Défaillance des disques durs
		-	Éteinte	Pas d'accès et pas de défaillance des disques durs
J	Activité CIR1/CIR2	Vert	Allumée	Lien LAN pour CIR1 et CIR2
		Vert	Clignotante	Activité LAN pour CIR1 et CIR2
		-	Éteinte	Inactif / Aucun lien
K	ID du châssis (bouton de marche)	Blanc	Allumée	Identification du châssis active via commande ou bouton
		-	Éteinte	Identification du châssis inactive
L	Bouton NMI			Bouton uniquement, pas de DEL

Élément	Nom du signal	Description
A	Bouton d'alimentation	Permet d'activer ou de désactiver l'alimentation du système, et fonctionne également comme un bouton de mise en veille si la

		fonctionnalité est prise en charge par un système d'exploitation conforme à la norme ACPI. Une DEL d'état est intégrée à ce bouton.
B	Bouton de réinitialisation du système	Redémarre et initialise le système.
K	Bouton d'identification du châssis	Permet d'activer ou de désactiver la DEL ID du châssis du panneau avant et la DEL ID du châssis du panneau arrière. La DEL du panneau avant est intégrée dans le bouton.

Figure 11. Éléments du panneau avant de la plateforme - comportement

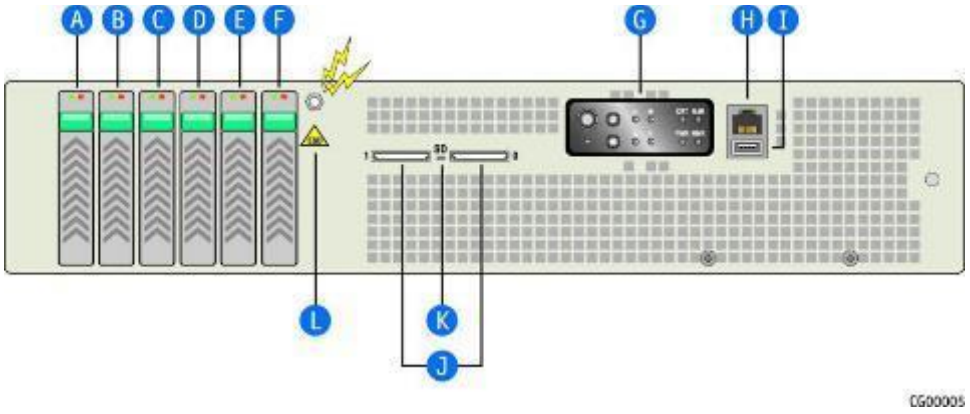


Tableau 16. Comportement des éléments du panneau avant de la plateforme

Élément	Description de la DEL	Couleur	État	Description
A, B, C, D, E, F	Disque dur de 2,5 pouces	Vert	Fixe	Disque dur présent
			Clignotante	Activité du disque dur
		Ambre	Fixe	Défaillance du disque dur
	Disque SSD de 2,5 pouces	Vert	Éteinte	Disque SSD présent
			Clignotante	Activité du disque SSD
		Ambre	Fixe	Défaillance du disque SSD
H	Port série RJ45			Aucune DEL Port série sur RJ45
K	Module flash SD	Vert	Éteinte	Aucune activité sur la carte SD
			Clignotante	Activité sur la carte SD

3.5.2. Panneau arrière

Figure 12. Connecteurs arrière de la plateforme - comportement

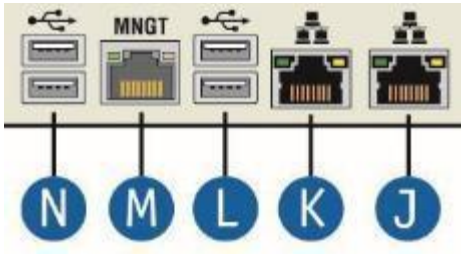


Tableau 17. Comportement des connecteurs arrière de la plateforme

Élément	Description de la DEL	Couleur	État	Description
J,K	Activité de liaison (gauche) CIR1 et CIR2	Vert	Éteinte	Aucune liaison établie
			Fixe	Liaison établie
			Clignotante	Activité de liaison
	Vitesse de liaison (droite) CIR1 et CIR2	Vert	Fixe	10 Gbps
		Jaune	Fixe	1 Gbps
M	Activité de liaison (gauche) CIR de gestion dédiée	Vert	Éteinte	Aucune liaison établie
			Fixe	Liaison établie
			Clignotante	Activité de liaison
	Vitesse de liaison (gauche) CIR de gestion dédiée	Vert	Fixe	1000 Mbps
		Jaune	Fixe	100 Mbps

Figure 13. DEL de l'alimentation CA et CC

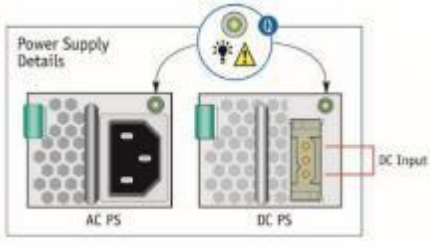


Tableau 18. Comportement des DEL de l'alimentation CA

État de l'alimentation CA	DEL bicolore
État de l'alimentation CA	DEL bicolore
Aucune alimentation CA vers tous les blocs d'alimentation	Éteinte
Aucune alimentation CA vers ce bloc d'alimentation uniquement (pour une configuration 1+1)	Rouge clignotante 0,5 Hz
CA présent / seule la tension de veille de 5 Vsb est fournie (bloc d'alimentation éteint)	Verte clignotante 1 Hz
Sortie du bloc d'alimentation active et OK	Vert
Défaillance du bloc d'alimentation	Rouge

État de l'alimentation CA	DEL bicolore
Avertissement associé au bloc d'alimentation	Rouge/verte clignotante 0,5 Hz*

* Fréquence de clignotement : 1 Hz (0,5 s rouge / 0,5 s vert)

Tableau 19. Comportement des DEL de l'alimentation CC

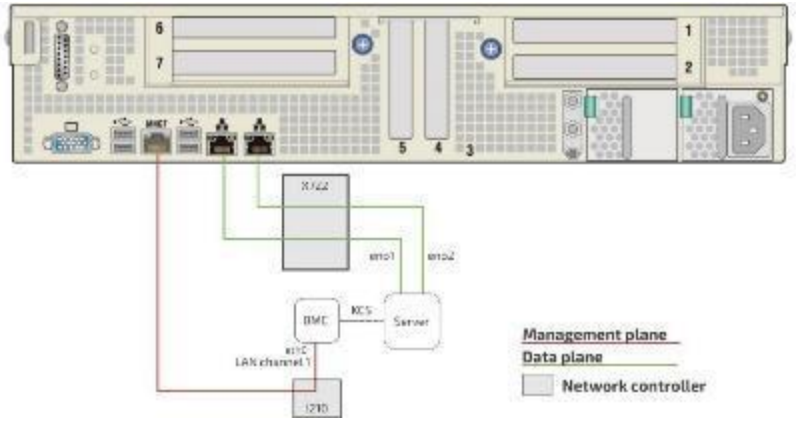
État de l'alimentation CC	DEL bicolore
Aucune alimentation CC vers tous les blocs d'alimentation	Éteinte
Aucune alimentation CC vers ce bloc d'alimentation uniquement (pour une configuration 1+1)	Rouge clignotante 0,5 Hz
CC présent / seule la tension de veille de 5 Vsb est fournie (bloc d'alimentation éteint)	Verte clignotante 1 Hz
Sortie du bloc d'alimentation active et OK	Vert
Défaillance du bloc d'alimentation	Rouge
Avertissement associé au bloc d'alimentation	Rouge/verte clignotante 0,5 Hz*

* Fréquence de clignotement : 1 Hz (0,5 s rouge / 0,5 s vert)

4/ Architecture du produit

4.1. Connexions internes

Figure 14. Connexions internes



4.2. Plans réseau

La plateforme CG2400 offre 2 plans réseau.

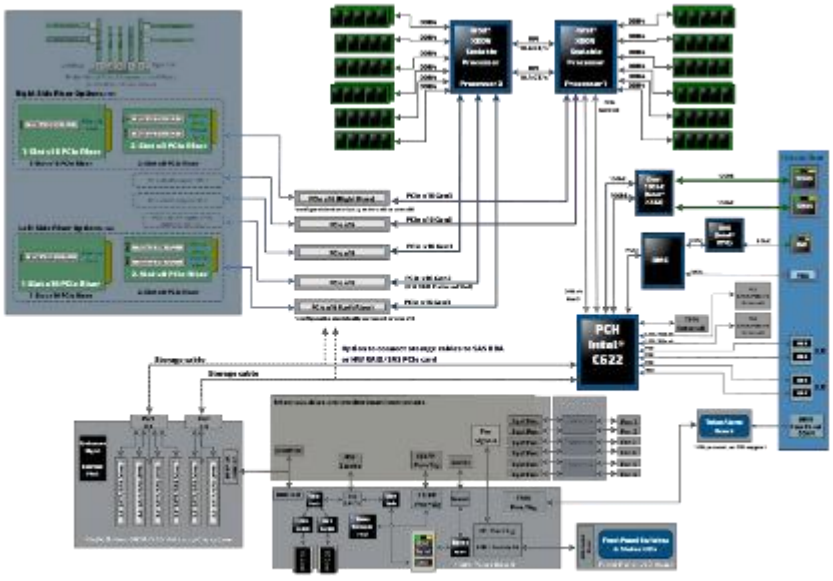
Tableau 20. Plans réseau

Plans réseau	Description	Vitesse (GbE)	Accès aux composants	Schéma d'adressage IP par défaut
Plan de gestion	Le plan de gestion achemine le trafic administratif de la plateforme. Ce plan est utilisé pour prendre en charge la gestion du matériel, la configuration et la surveillance de l'état, de la température et de l'alimentation.	1	BMC	DHCP
Plan des données	Le plan des données achemine le trafic des applications clients. Ce plan est utilisé pour fournir des services aux utilisateurs finaux.	10	Serveur, BMC	DHCP

4.3. Schéma fonctionnel

Ce schéma fonctionnel résume les connexions dans la plateforme.

Figure 15. Schéma fonctionnel



5/ Description des méthodes d'accès au système

Pour configurer, surveiller et dépanner la plateforme CG2400 et ses composants, plusieurs interfaces peuvent être utilisées :

- Système d'exploitation – via le plan de gestion, le plan des données, le port série ou le port VGA de la plateforme
- BIOS – via le plan de gestion, le port série ou le port VGA de la plateforme
- Interface de gestion (BMC) – via le plan de gestion de la plateforme

5.1. Méthodes d'accès au système d'exploitation

Pour toute connexion à un serveur, un système d'exploitation doit être installé. La redirection vers le port série est configurée dans le système d'exploitation. Si le système livré dispose d'un système d'exploitation installé par Kontron, la redirection de la console est activée par défaut.

Pour accéder au système d'exploitation par l'une des méthodes, voir Accéder au système d'exploitation d'un serveur.

Tableau 21. Méthodes d'accès au système d'exploitation

Méthodes d'accès au système d'exploitation	
Description de la méthode	Principales raisons de l'utiliser
KVM (écran-clavier-souris) *Méthode sans échec pour accéder au serveur si un composant (système d'exploitation, BIOS, etc.) est mal configuré. Accessible à partir du plan de gestion.*	• Installation initiale du système d'exploitation • Configuration de l'interface réseau du système d'exploitation • Accès à la vidéo du système d'exploitation • Accès à distance au système d'exploitation • Incapacité d'établir une session SSH sur le système d'exploitation
Écran/moniteur (carte VGA) *Il s'agit de la méthode recommandée pour la configuration initiale d'un système sorti de son emballage. En utilisant un clavier (USB), cette méthode permet d'établir un accès direct au système.*	• Accès local au système d'exploitation et au système • Installation initiale du système d'exploitation • Configuration de l'interface réseau du système d'exploitation • Accès à la vidéo du système d'exploitation • Incapacité d'établir une session SSH sur le système d'exploitation
Protocoles SSH, RDP et des applications clients *Méthode idéale après l'installation du système d'exploitation et la configuration de l'interface réseau du système d'exploitation. Accessible à partir du plan des données.*	• Faire fonctionner la plateforme dans des conditions normales • Accès à distance au système d'exploitation
Série sur LAN (SOL) *Accessible à partir du plan de gestion.*	• Configuration de l'interface réseau du système d'exploitation • Incapacité d'établir une session SSH sur le système d'exploitation • Accès à la console série du système d'exploitation
Console série (connexion physique) *Méthode sans échec pour accéder à tous les composants du serveur (système d'exploitation, BMC, BIOS) s'ils sont mal configurés.* *Accessible à partir du port physique.*	• Configuration initiale de l'interface réseau du système d'exploitation • Aucune configuration n'est effectuée sur les BMC • Dépannage

5.2. Méthode d'accès au BIOS

Pour accéder au BIOS par l'une des méthodes, voir Accéder au BIOS.

Tableau 22. Méthodes d'accès au BIOS

Méthodes d'accès au BIOS	
Description de la méthode	Principales raisons de l'utiliser
KVM (écran-clavier-souris) *Méthode sans échec pour accéder au serveur si un composant (système d'exploitation, BIOS, etc.) est mal configuré. Accessible à partir du plan de gestion.*	• Configuration initiale du BIOS • Accès à la vidéo du BIOS
Écran/moniteur (carte VGA) *Il s'agit de la méthode recommandée pour la configuration initiale d'un système sorti de son emballage. En utilisant un clavier (USB), cette méthode permet d'établir un accès direct au système.*	• Configuration initiale du BIOS • Aucune configuration n'est effectuée sur les BMC • Accès à la vidéo du BIOS • Dépannage
Série sur LAN (SOL) *Accessible à partir du plan de gestion.*	• Configuration initiale du BIOS • Accès à la console série du BIOS • Interfaces réseau du système d'exploitation non configurées, mais accès au réseau du BMC disponible
Console série (connexion physique) *Méthode sans échec pour accéder à tous les composants du serveur (système d'exploitation, BMC, BIOS) s'ils sont mal configurés.* *Accessible à partir du port physique.*	• Configuration initiale du BIOS • Aucune configuration n'est effectuée sur les BMC • Dépannage

5.3. Méthodes d'accès à l'interface de gestion (BMC)

Pour accéder à l'interface de gestion (BMC) par l'une des méthodes, voir Accéder au BMC.

Tableau 23. Méthodes d'accès au BMC

Méthodes d'accès à l'interface de gestion (BMC)	
Description de la méthode	Principales raisons de l'utiliser
Interface utilisateur Web du BMC *Il s'agit de la méthode recommandée pour la configuration initiale d'un système sorti de son emballage.* *Accessible à partir du plan de gestion.*	• Contrôle et surveillance à distance du serveur • Accès à la vidéo du système d'exploitation • Mises à niveau des micrologiciels
IPMI sur LAN (IOL) *Il s'agit d'une bonne méthode pour les scripts de surveillance/contrôle automatisés une fois la plateforme configurée pour la première fois.* *Accessible à partir du plan de gestion.*	• Contrôle et surveillance à distance du serveur • Mises à niveau des micrologiciels
IPMI/KCS *Accessible à partir du système d'exploitation local.*	• Accès local au BMC à partir du système d'exploitation pour la surveillance du serveur • Configuration initiale du BMC
Redfish *Il s'agit de la méthode idéale pour les scripts de surveillance/contrôle automatisés une fois la plateforme configurée pour la première fois.* *Accessible à partir du plan de gestion.*	• Surveillance à distance du serveur • Contrôle à distance du serveur

Méthodes d'accès à l'interface de gestion (BMC)	
Description de la méthode	Principales raisons de l'utiliser
SNMP *Il s'agit de la méthode idéale pour les scripts de surveillance/contrôle automatisés une fois la plateforme configurée pour la première fois.* *Accessible à partir du plan de gestion.*	• Surveillance à distance du serveur • Contrôle à distance du serveur

6/ Expertise technique recommandée

Les plateformes sont des périphériques réseau.

Il est recommandé d'identifier la topologie en amont appropriée avec l'aide du personnel informatique/réseau qui gère le matériel et la configuration du réseau en amont. Cela facilitera le processus par la suite.

Les adresses IP devront également être attribuées en fonction des adresses MAC connues, nécessitant donc une expertise informatique appropriée.

7/ Guide de démarrage – installation de l'application et évaluation des performances

NOTICE

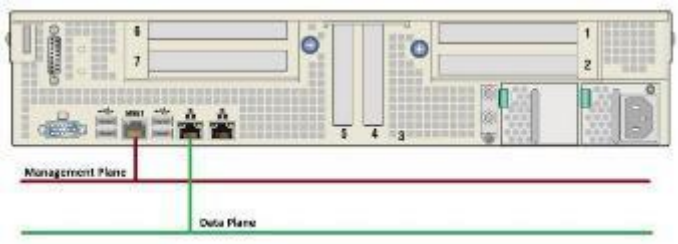
Avant de travailler avec ce produit ou d'exécuter les instructions décrites dans la section Guide de démarrage ou dans d'autres sections, lire la section Informations sur la sécurité et la réglementation propre au produit. Les instructions d'assemblage contenues dans cette documentation doivent être suivies pour garantir et maintenir la conformité avec les certifications et approbations existantes associées au produit. Utiliser uniquement les composants décrits et réglementés spécifiés dans cette documentation. L'utilisation d'autres produits/composants annulera la certification CSA et les autres approbations réglementaires du produit et entraînera très probablement une non-conformité avec les réglementations relatives au produit dans la ou les régions dans lesquelles le produit est vendu.

7.1. Introduction

La section Guide de démarrage décrit les étapes d'intégration réseau, d'accès à la plateforme et d'installation du système d'exploitation requises pour commencer à exploiter une plateforme CG2400 équipée de deux CPU, d'un ou deux blocs d'alimentation, de disques durs ou SSD et de cartes d'expansion PCIe fournies par le client, et utilisée pour exploiter deux liaisons réseau distinctes (un pour le plan de gestion et l'autre pour le plan des données).

L'image ci-dessous représente l'architecture simplifiée utilisée dans le Guide de démarrage qui inclut un plan de gestion et un plan des données.

Figure 16. Architecture simplifiée



Voir Architecture du produit pour les détails complets de l'architecture du réseau de la plateforme.

7.1.1. Hypothèses

Le scénario décrit dans ce Guide de démarrage est basé sur les hypothèses suivantes :

- Les connexions réseau du système sont les suivantes :
  - Un plan de gestion (ligne rouge) via le port de gestion RJ45
  - Un plan des données (ligne verte) via le port de données RJ45 de gauche
- Une connexion d'affichage via le port VGA est nécessaire pour obtenir l'adresse IP de gestion du BMC
- Le schéma d'adressage IP par défaut est DHCP
- La méthode d'installation préférée du système d'exploitation est via le KVM (écran-clavier-souris)
- La plateforme est équipée de deux CPU
- La plateforme est équipée d'au moins un bloc d'alimentation CC

7.2. Déballage de la plateforme

7.2.1. Contenu de la boîte

La boîte de la plateforme CG2400 comprend :

- Un serveur pour étagère 2U haute disponibilité CG2400 de 20 pouces de profondeur
- Deux boîtes de dissipateurs thermiques, l'une étiquetée « Avant » et l'autre « Arrière ».

7.2.2. Étapes de déballage

Étape_1	Ouvrir la boîte de la plateforme et retirer les petites boîtes de dissipateurs thermiques (il y en aura une ou deux selon la commande). Mettre les boîtes de côté jusqu'au moment d'installer les processeurs et les dissipateurs thermiques dans la plateforme. Voir Installation et assemblage des composants pour les instructions d'assemblage. **NOTE :** • Le processeur avec le dissipateur thermique « Avant » doit être installé sur le socket CPU1. • Le processeur avec le dissipateur thermique « Arrière » doit être installé sur le socket CPU2.
Étape_2	Retirer soigneusement la plateforme de la boîte et enlever les deux morceaux de mousse.
Étape_3	Retirer la plateforme du sac ESD.
Étape_4	Retirer la pellicule plastique installée sur la plateforme. Si la pellicule n'est pas retirée, l'efficacité de la circulation de l'air dans la plateforme risque d'être affectée, ce qui se traduirait par une mauvaise capacité de refroidissement
Étape_5	Remettre tous les éléments d'emballage dans la boîte (deux sachets déshydratants, un sac ESD, deux morceaux de mousse).

7.3. Planification

7.3.1. Matériel et informations requis

7.3.1.1. Installation et assemblage des composants

Élément_1	Tournevis Phillips no 1 (cruciforme) (ou tournevis à embouts interchangeables avec embouts Phillips nº 1 et no 2)
Élément_2	Tournevis Phillips no 2 (cruciforme) (ou tournevis à embouts interchangeables avec embouts Phillips nº 1 et nº 2)
Élément_3	Un tournevis Torx T30
Élément_4	Un tournevis à tête plate de 5 mm
Élément_5	Dispositif personnel de mise à la terre, tel qu'un bracelet antistatique et un tapis antistatique mis à la terre

Ce Guide montre l'installation de trois cartes d'expansion PCIe :

- Une carte RAID matériel SAS
- Une carte Ethernet à profil bas (demi-hauteur/demi-longueur)
- Une carte montée sur la carte adaptatrice de connexion PCIe de gauche (pleine hauteur)

Pour installer un module de sauvegarde à batterie SuperCap pour la carte RAID SAS, un support de montage est requis.

Élément_1	K00740-001	Support de montage pour le module de sauvegarde à batterie d'Intel

Pour installer une carte d'expansion PCIe pleine hauteur, une carte adaptatrice de connexion PCIe est requise.

Élément_1	CG2200-RISER2SX8L	Carte adaptatrice de connexion à emplacement double pour PCIe x8, Gen 3, pour l'emplacement 2 (côté gauche)

7.3.1.2. Cordons d'alimentation et outils

Élément_1	Fil noir toronné de calibre AWG no 12 pour fabriquer le cordon d'alimentation en fonction de la longueur requise
Élément_2	Fil rouge toronné de calibre AWG no 12 pour fabriquer le cordon d'alimentation en fonction de la longueur requise
Élément_3	Un connecteur homologue Positronic pour l'entrée du bloc d'alimentation CC (comprend un assemblage de décharge de traction)
Élément_4	Trois cosses à sertir de calibre 16 Positronic
Élément_5	Deux vis de décharge de traction
Élément_6	Une plaque de décharge de traction
Élément_7	Deux vis Phillips à tête plate
Élément_8	Une pince à sertir manuelle, DMC AF8
Élément_9	Un outil d'extraction manuelle
Élément_10	Un câble de mise à la terre de calibre AWG no 8 en fonction de la longueur requise
Élément_11	Une cosse de mise à la terre à angle droit, calibre AWG no 8 (numéro de pièce Kontron 1064-4226)
Élément_12	Clé de 10 mm ou outil équivalent
Élément_13	Une pince à sertir manuelle, Panduit CT-1700

7.3.1.3. Matériel d'installation dans l'étagère

Dans cette section, une étagère de 19 pouces à 4 montants de 20 à 24 pouces de profondeur est utilisée comme exemple. Pour une configuration différente, voir Installation dans une étagère.

Élément_1	TMLPMOUNT51

7.3.1.4. Câbles et modules réseau

Élément_1	Un câble Ethernet RJ45 pour le plan de gestion
Élément_2	Deux câbles Ethernet RJ45 pour le plan des données
Élément_3	Un câble de connexion série RJ45

7.3.1.5. Infrastructure réseau

Adresses IP :

- Une adresse IP pour le plan de gestion
- Jusqu'à 2 adresses IP pour le plan des données

7.3.2. Logiciels requis

Section pertinente :

Installation des logiciels courants

Élément_1	Une version de la communauté d'ipmitool est installée sur un ordinateur distant pour permettre la surveillance à distance – il est recommandé d'utiliser la version 1.8.18 d'ipmitool.

Élément_2	Un émulateur de terminal tel que puTTY est installé sur un ordinateur distant.
Élément_3	Un outil de détection des périphériques tel que pciutils est installé sur le serveur local pour visualiser des informations sur les périphériques connectés aux bus PCI du serveur.

> Vous disposez maintenant du matériel et des logiciels nécessaires. Procédez à l'installation des cartes d'expansion PCIe.

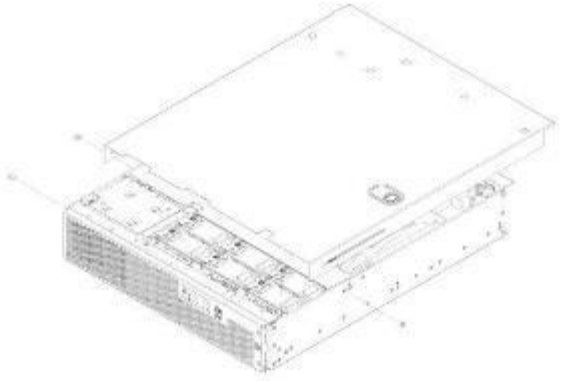
7.4. Installation des composants

Appareil sensible aux ESD!

Cet équipement est sensible à l'électricité statique. Des précautions doivent donc être prises lors de toutes les opérations de manipulation et d'inspection de ce produit afin d'en garantir l'intégrité à tout moment.

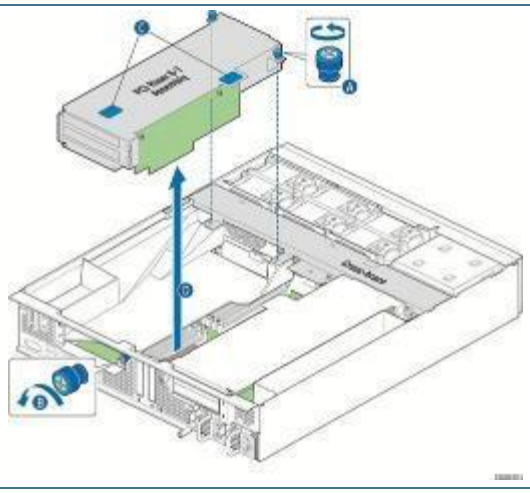
Débrancher le ou les cordons d'alimentation avant toute intervention sur le produit afin d'éviter tout risque de choc électrique. Si le produit est équipé de plusieurs cordons d'alimentation, débrancher tous les cordons.

7.4.1. Ouvrir le châssis

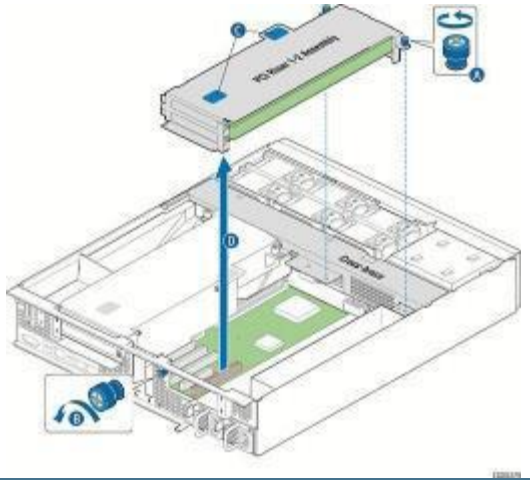
Étape_1	Retirer la vis d'expédition Phillips à tête hexagonale 6-32 située à l'avant gauche du capot, si elle est encore fixée, et la garder pour une utilisation ultérieure.	
Étape_2	Retirer les deux vis à épaulement (une de chaque côté) du capot.	
Étape_3	Tout en maintenant le bouton bleu de déverrouillage au milieu du capot supérieur, faire glisser le capot vers l'arrière jusqu'à ce qu'il s'arrête et que le bord dégage le support de verrouillage sur le panneau arrière du châssis.	
Étape_4	Soulever le capot vers le haut pour le retirer du châssis.	

7.4.2. Enlever la cage d’extension PCIe de droite

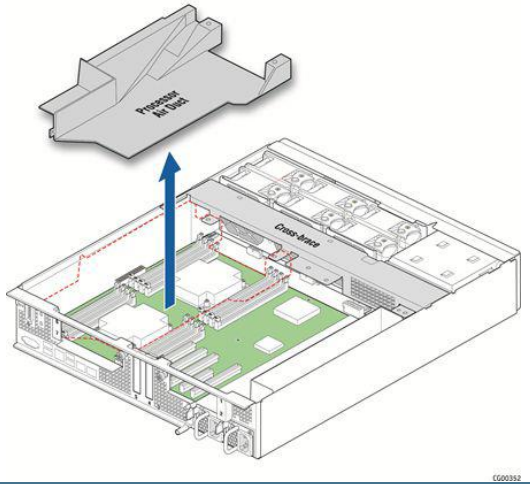
Étape_1	Desserrer les deux vis de retenue imperdables bleues (A) à l'avant de la cage d’extension PCIe et la vis imperdable bleue à l'arrière du châssis (B).	

Étape_2	En utilisant les deux points de contact bleus (C), soulever la cage d'extension hors du châssis (D).	

7.4.3. Enlever la cage d'extension PCIe de gauche

Étape_1	Desserrer les deux vis de retenue imperdables bleues (A) à l'avant de la cage d'extension PCIe et la vis imperdable bleue à l'arrière du châssis (B).	
Étape_2	En utilisant les deux points de contact bleus (C), soulever la cage d'extension hors du châssis (D).	

7.4.4. Retirer le conduit d'air des processeurs

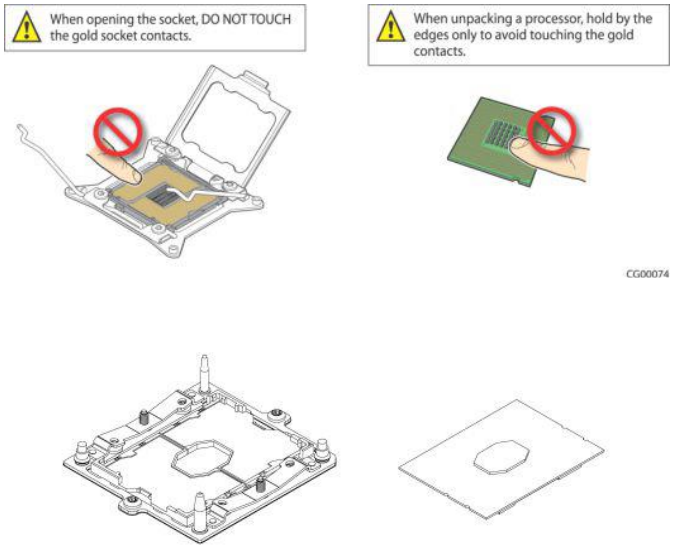
Étape_1	Pour retirer le conduit d'air des processeurs, il suffit de le soulever vers le haut hors du châssis.	

7.4.5. Installer les processeurs et les dissipateurs thermiques

7.4.5.1. Manipulation des sockets et processeurs et précautions contre les décharges électrostatiques

7.4.5.1.1. Précautions pour la manipulation

NOTICE

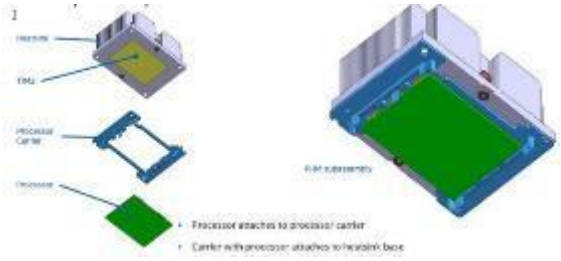


NOTICE

Les contacts des sockets sont fragiles et peuvent être facilement endommagés s'ils sont touchés. Intel a mis au point un sous-ensemble empilé pour assurer des mouvements uniformes et contrôlés lors de l'insertion et du retrait des processeurs des sockets. Kontron attend des utilisateurs et des intégrateurs de systèmes qu'ils utilisent la méthodologie conçue par Intel à tous les points des procédures de cette section où un processeur est retiré ou inséré dans un socket.

Le module dissipateur thermique et processeur (PHM) désigne le sous-ensemble où le dissipateur thermique et le processeur sont clipsés ensemble avant l'installation. Cela permet une installation plus robuste en offrant de meilleures caractéristiques d'alignement et en gardant les doigts à l'écart du champ de contact du socket.

Le sous-ensemble empilé se compose de trois parties.



Source de l'image : Intel Corporation

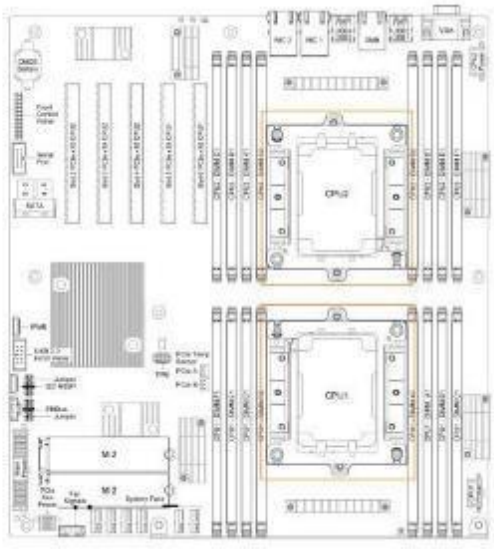
7.4.5.1.2. Précautions contre les décharges électrostatiques

Porter une attention particulière aux points suivants lors de la manipulation des processeurs et des sockets afin de réduire le risque de dommages dus aux décharges électrostatiques (ESD) sur les processeurs :

- **Toucher au châssis métallique avant de toucher le processeur ou la carte de serveur.**
- **Maintenir une partie de votre corps (ex. une main) en contact avec le châssis métallique pour dissiper la charge statique lors de la manipulation du processeur.**
- **Éviter de vous déplacer inutilement.**
- **Utiliser un bracelet antistatique attaché au panneau avant (avec le panneau frontal retiré).**

7.4.5.2. Emplacement des processeurs

Figure 17. Emplacement des processeurs



Effectuer les tâches suivantes pour chaque processeur.

7.4.5.3. Ajouter un processeur dans un PHM

NOTICE

Le processeur doit être approprié.

L'installation d'un processeur inapproprié pourrait gravement endommager la carte de la plateforme. Voir Liste de compatibilité matérielle pour une liste des composants.

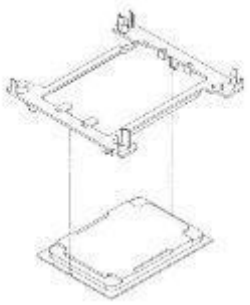
NOTICE

Kontron recommande d'inspecter le socket du CPU avant d'ajouter ou de remplacer un processeur pour s'assurer qu'il n'y a pas de problème avec les broches fragiles du socket.

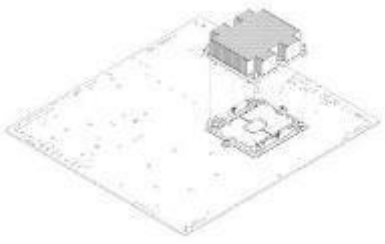
7.4.5.3.1. Préparer le processeur pour l'assemblage dans le PHM

Étape_1	Retirer le couvercle du plateau d'emballage du processeur. Dans cette position, le processeur est prêt à être clipsé au reste des composants du PHM. **ATTENTION :** Ne pas toucher le processeur.

7.4.5.3.2. Installer le processeur

<table>
<tr><td>Étape_1</td><td colspan="2">Retirer le dissipateur thermique de son emballage.
NOTE :
• Le processeur avec le dissipateur thermique « Avant » doit être installé sur le socket CPU1 (voir Emplacement des processeurs)
• Le processeur avec le dissipateur thermique « Arrière » doit être installé sur le socket CPU2 (voir Emplacement des processeurs)</td></tr>
<tr><td>Étape_2</td><td>Prendre le nouveau PHM (module dissipateur thermique et processeur) et le placer au-dessus du processeur, qui est dans son plateau d'emballage ouvert. Les triangles d'assemblage (indicateur de la broche 1) doivent être dans les positions appropriées avant d’abaisser le PHM.
NOTE : Sur cette image, le dissipateur thermique a été retiré pour plus de clarté. Seuls le support de processeur et le processeur sont représentés.</td><td rowspan="2">  </td></tr>
<tr><td>Étape_3</td><td>Clipser délicatement le processeur sur le PHM. Soulever l'ensemble. Le processeur doit être clipsé en place.</td></tr>
</table>

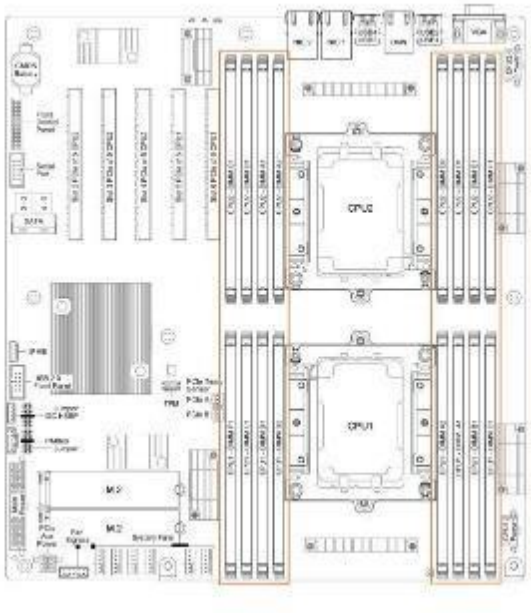
7.4.5.4. Installer un PHM dans la plateforme

<table>
<tr><td>Étape_1</td><td>Aligner le triangle de la plaque de renfort avec celui du processeur. Poser le PHM sur la plaque de renfort.</td><td rowspan="2">  </td></tr>
<tr><td>Étape_2</td><td>Serrer progressivement (en suivant un motif en étoile) et uniformément chacune des quatre vis selon un schéma diagonal jusqu'à ce que chacune soit fermement serrée (couple de 12,0 lb-po).</td></tr>
</table>

7.4.6. Installer des modules DIMM

7.4.6.1. Emplacement des modules DIMM

Figure 18. Emplacement des modules DIMM



7.4.6.2. Directives d'installation des modules DIMM pour une performance optimale

Il y a 8 emplacements DIMM par CPU, mais seulement 6 canaux par CPU – A1 et A2 sont sur le même canal et D1 et D2 sont sur le même canal. Par conséquent, ne pas remplir les emplacements A2 et D2 à moins d'avoir rempli tous les autres emplacements DIMM.

Pour une performance optimale, les deux CPU devraient avoir la même configuration DIMM, en configuration CPU simple ou double.

Pour chaque CPU, installer les modules DIMM conformément aux directives suivantes pour une performance optimale.

- Pour les configurations avec 1 à 3 modules DIMM – remplir les emplacements A1, B1 et C1, en commençant par A1.
- Pour les configurations avec 4 modules DIMM – remplir les emplacements A1, B1, D1 et E1.
- Les configurations avec 5 modules DIMM ne sont pas recommandées, car elles sont déséquilibrées et produiront une performance moins optimale.
- Pour les configurations avec 6 modules DIMM – remplir les emplacements A1, B1, C1, D1, E1 et F1.
- Les configurations avec 7 modules DIMM ne sont pas recommandées, car elles sont déséquilibrées et produiront une performance moins optimale.
- Pour les configurations avec 8 modules DIMM – remplir tous les emplacements DIMM.

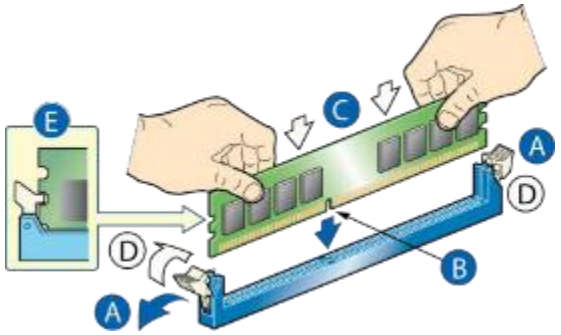
NOTICE

La configuration avec 8 modules DIMM par CPU réduira la vitesse des DIMM à 2933 MHz d'un cran par rapport à la valeur nominale, c'est-à-dire à 2666 MHz.

Si des mémoires à 2666 ou 2400 MHz (8 DIMM par CPU) sont utilisées, la vitesse négociée reste la vitesse nominale des modules DIMM, sauf si la vitesse maximale de la mémoire du CPU est inférieure à la vitesse nominale des modules DIMM.

- Exemple 1. Le processeur Xeon Silver 4114T à 2400 MHz négocie des modules DIMM à 2666 MHz à 2400 MHz
- Exemple 2. Le processeur Xeon Gold 5218T à 2666 MHz négocie des modules DIMM à 2666 MHz à 2666 MHz

7.4.6.3. Installer des modules DIMM

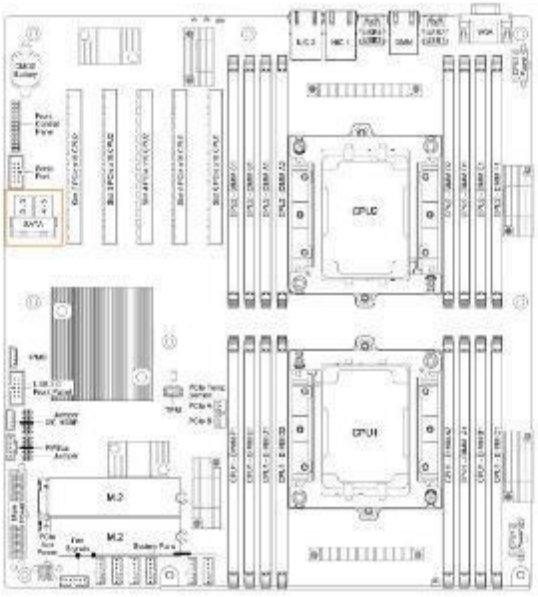
Étape_1	Ouvrir les onglets de l'emplacement DIMM. (A)	
Étape_2	Noter l'emplacement de l'encoche d'orientation sur le bord du module DIMM. (B)	
Étape_3	Insérer le module DIMM, en veillant à ce que le bord connecteur du module DIMM s'aligne correctement dans l'emplacement. (E)	
Étape_4	Avec les deux mains, appuyer fermement et uniformément sur les deux côtés du module DIMM jusqu'à ce qu'il s'enclenche et que les onglets se ferment. (C et D)	
Étape_5	Inspecter visuellement chaque onglet pour s'assurer qu'ils sont complètement fermés et correctement enclenchés dans les encoches du bord du module DIMM. (E)	

7.4.7. Installer un contrôleur RAID matériel

NOTE : On suppose que la plateforme est équipée de deux CPU pour permettre l'utilisation de l'emplacement 2 (cage d'extension PCIe de gauche) et de l'emplacement 4, comme indiqué ci-dessous dans le présent Guide de démarrage.

7.4.7.1. Emplacement des câbles SAS

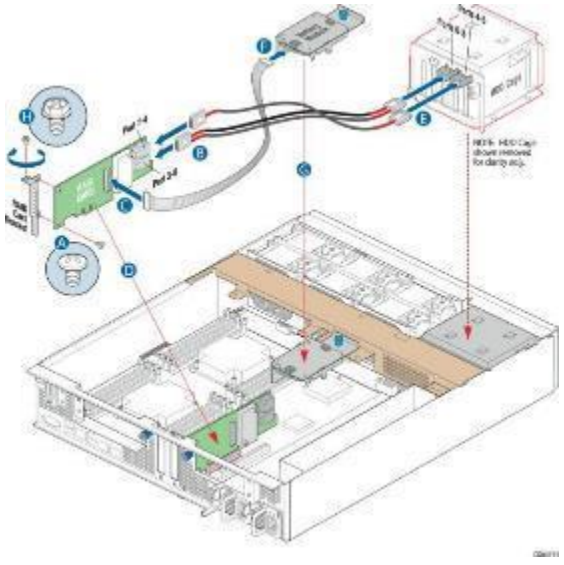
Figure 19. Emplacement des câbles SAS



7.4.7.2. Déconnecter les câbles SAS

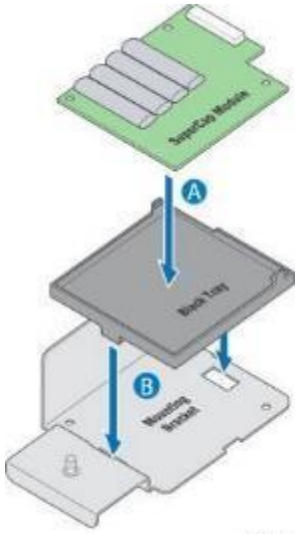
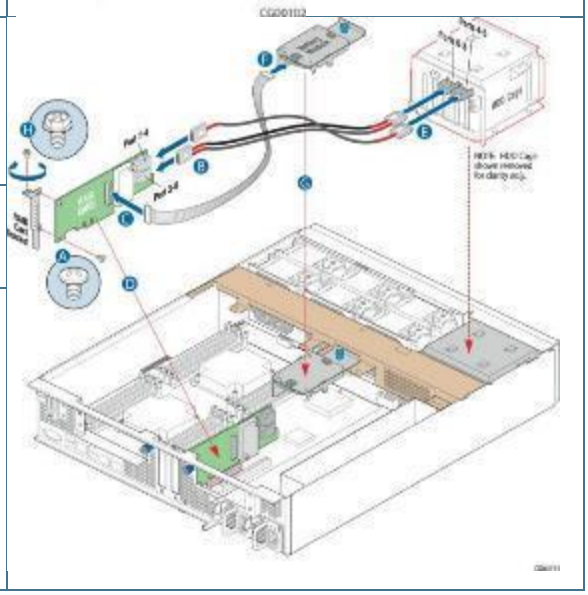
Étape_1	Déconnecter les deux câbles SAS (extrémités SFF-8643) de la carte mère.

7.4.7.3. Installer le contrôleur

Étape_1	Dévisser la vis qui maintient le support de la carte RAID de l'emplacement 3. Retirer le support du panneau arrière du châssis et le panneau de remplissage de l'emplacement PCIe 4.	
Étape_2	Fixer le support retiré du châssis à la carte contrôleur RAID à l'aide des deux vis du support (A).	
Étape_3	Faire correspondre le câble connecté aux ports 0-3 de la cage du disque dur au port 3-0 de la carte RAID/SAS, en connectant l'extrémité libre à la carte RAID (B). Faire correspondre le câble connecté aux ports 4-5 de la cage du disque dur au port 7-4 de la carte RAID/SAS, en connectant l'extrémité libre à la carte RAID (B). (Optionnel) Si un module de sauvegarde à batterie des configurations RAID SuperCap est utilisé : • Fixer le support du module de sauvegarde à batterie SuperCap sur la traverse du châssis (G). • Connecter le module de sauvegarde à batterie SuperCap à la carte RAID (C et F).	
Étape_4	Réinstaller le panneau de remplissage de l'emplacement PCIe 4 (retiré à l'étape 1), puis insérer la carte contrôleur RAID dans l'emplacement PCIe 3 de la carte mère et appuyer pour l'unir avec le connecteur (D). Le support de l'emplacement 3 est placé directement au-dessus du panneau de remplissage de l'emplacement 4.	
Étape_5	Fixer le panneau de remplissage de l'emplacement 3 avec la vis retirée précédemment (étape 1).	

7.4.7.4. Installer le module de sauvegarde à batterie SuperCap

Étape_1	Insérer l'unité dans le plateau en plastique noir (A).	
Étape_2	Fixer l'unité et le plateau au support en tôle en insérant les languettes dans les découpes du support (B).	

Étape_3	Faire glisser l'ensemble unité/plateau vers l'arrière (côté avec le connecteur) du support jusqu'à ce qu'il s'enclenche.	
Étape_4	Connecter le câble de signal/alimentation au connecteur approprié sur la carte contrôleur RAID matériel (C) et à l'arrière de l'assemblage du module de sauvegarde à batterie (F).	
Étape_5	Placer le support du module de sauvegarde à batterie sur la traverse, en l'alignant sur le trou central de la plaque d'appui centrale (G).	
Étape_6	Utiliser la vis de retenue bleue pour fixer l'assemblage du module de sauvegarde à batterie à la traverse. **NOTE :** Une fois la plateforme alimentée et fonctionnelle, procéder aux configurations logicielles requises.	

7.4.8. Installer une carte PCIe à profil bas dans l'emplacement 4 ou 5

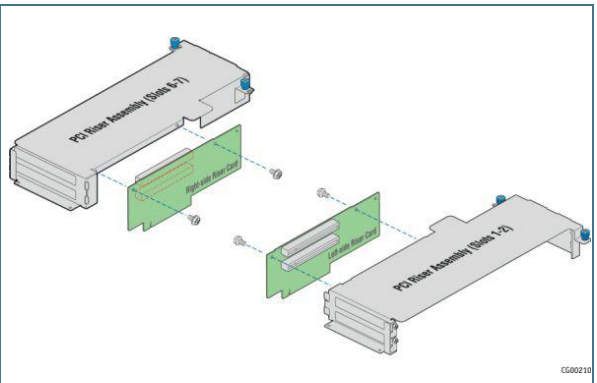
Les emplacements PCIe disponibles sur la carte mère dépendent du nombre de CPU. Pour plus de détails, voir Mappage PCI.

NOTE : Pour l'exemple du Guide de démarrage, on suppose que la plateforme est équipée de deux CPU afin de pouvoir utiliser l'emplacement 4.

Étape_1	Dévisser la vis qui maintient le panneau de remplissage de l'emplacement PCIe. Retirer le panneau de remplissage vierge et le garder pour une utilisation ultérieure.
Étape_2	Insérer la carte d'expansion PCIe dans l'emplacement PCIe de la carte mère et appuyer pour l'unir au connecteur.
Étape_3	Fixer la carte d'expansion PCIe au châssis avec la vis retirée à l'étape 1.

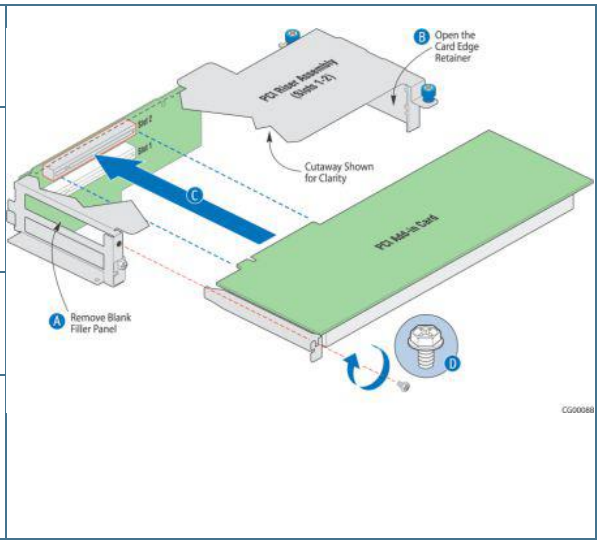
7.4.9. Installer une carte pleine hauteur montée dans la cage d'extension PCIe de gauche

7.4.9.1. Assembler la carte adaptatrice de connexion PCIe

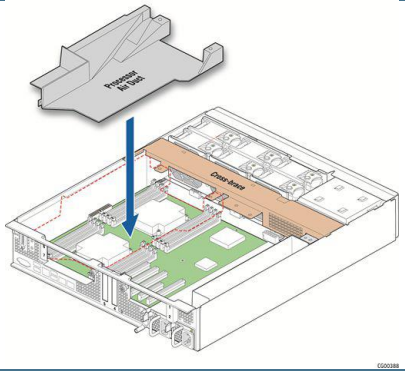
Étape_1	Fixer la carte adaptatrice de connexion gauche à son support avec les deux vis 6-32 (couple de 8 lb-po).	

La carte adaptatrice de connexion est maintenant prête à recevoir des cartes d'expansion.

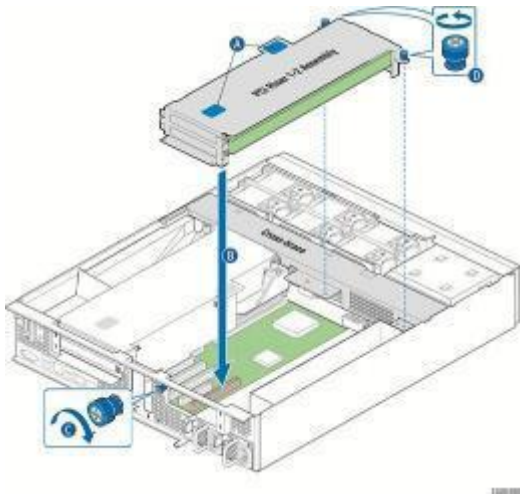
7.4.9.2. Installer une carte d'expansion PCIe dans la cage d'extension

Étape_1	Retirer le panneau de remplissage vierge de la cage d'extension (A) en dévissant la vis de l'emplacement sélectionné (D).	
Étape_2	Pour une carte d'expansion pleine longueur, ouvrir le support d'extrémité de carte en desserrant la vis imperdable bleue (B). **NOTE :** Cette étape s'applique uniquement aux cartes pleine longueur (pas aux cartes demi-longueur).	
Étape_3	Joindre la carte d'expansion au connecteur approprié de la carte adaptatrice de connexion (C), en veillant à ce qu'elle soit correctement unie avec le connecteur.	
Étape_4	Fixer la carte d'expansion au support de la cage d'extension avec la vis de retenue arrière (D). Pour les cartes pleine longueur, fixer également la carte dans les rainures du support d'extrémité de carte (B).	

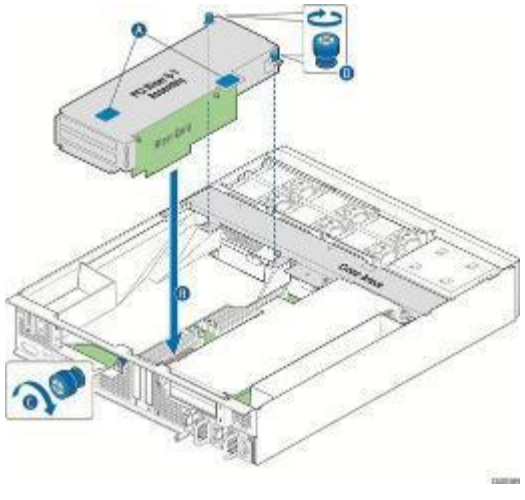
7.4.10. Remettre le conduit d'air des processeurs

Étape_1	Placer le conduit d'air des processeurs au-dessus des sockets des processeurs et des modules DIMM. Aligner les languettes avant avec les vis imperdables de la traverse. S'assurer que la goupille située à l'arrière du châssis est insérée dans la rainure moulée à l'arrière du conduit d'air des processeurs. Le conduit d'air est fixé lorsque la cage d'extension PCIe de droite est montée sur la traverse située au-dessus.	

7.4.11. Réinstaller la cage d'extension PCIe de gauche

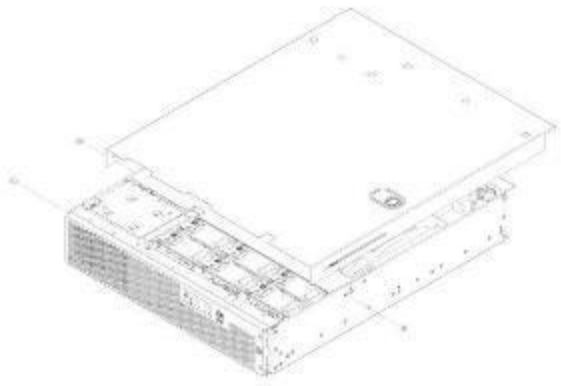
Étape_1	Positionner les languettes avant de la cage d'extension au-dessus des trous de la traverse.	
Étape_2	En utilisant les points de contact bleus sur le dessus de la cage (A), appuyer pour unir la carte adaptatrice de connexion au connecteur sur la carte de serveur (B, emplacement 2 pour la cage d'extension de gauche). **NOTES :** • Pour éviter d'endommager le bord de la carte, il faut s'assurer que la carte soit alignée directement avec le connecteur, et non de biais. • Si une carte contrôleur RAID matériel est installée dans l'emplacement PCIe 3, s'assurer de ne pas endommager les broches de diagnostic à l'arrière de la carte, près du panneau arrière du châssis, lors de la réinstallation de la cage d'extension PCIe de gauche.	
Étape_3	Aligner et serrer les vis de retenue imperdable bleues à l'avant de la cage avec les trous sur la traverse (D) et à l'arrière du châssis (C).	

7.4.12. Réinstaller la cage d'extension PCIe de droite

Étape_1	Positionner les languettes avant de la cage d'extension au-dessus des trous de la traverse (par-dessus le conduit d'air des processeurs).	
Étape_2	En utilisant les points de contact bleus sur le dessus de la cage (A), appuyer pour unir la carte adaptatrice de connexion au connecteur sur la carte de serveur (B, emplacement 6 pour la cage d'extension de droite). **NOTE :** Pour éviter d'endommager le bord de la carte, il faut s'assurer que la carte soit alignée directement avec le connecteur, et non de biais.	
Étape_3	Aligner et serrer les vis de retenue imperdable bleues à l'avant de la cage avec les trous sur la traverse (D) et à l'arrière du châssis (C).	

7.4.13. Fermer le châssis

Étape_1	En commençant par l'arrière du châssis, aligner la languette sur le bord arrière droit du couvercle avec le support de verrouillage sur l'extérieur du panneau arrière et déposer le capot sur le châssis avec les bords latéraux à l'extérieur des parois du châssis.	
Étape_2	Faire glisser le capot vers l'avant jusqu'à ce qu'il s'enclenche.	

Étape_3	Installer la vis d'expédition si l'entrée outillée est nécessaire ou si la plateforme doit être expédiée.	
Étape_4	Remettre les deux vis à épaulement en place (une de chaque côté) pour fixer le capot au cadre du châssis. Serrer les vis (couple de 8 lb-po).	
Étape_5	Rebrancher tous les périphériques et le(s) cordon(s) d'alimentation. **ATTENTION :** Le capot doit être installé lorsque la plateforme est en marche afin d'assurer un refroidissement adéquat.	

7.5. Installation de la plateforme dans une étagère

⚠CAUTION

Ancrer l'étagère destinée à l'équipement – L'étagère (rack) destinée à l'équipement doit être ancrée à un support impossible à déplacer pour l'empêcher de tomber lorsqu'un ou plusieurs rails coulissants équipés de serveurs sont sortis à l'avant. L'étagère destinée à l'équipement doit être installée conformément aux instructions du fabricant. Il est également requis de tenir compte du poids de tout autre appareil installé dans l'étagère.

Lorsqu'une étagère est utilisée, attendre que le serveur soit correctement monté dans l'étagère avant de brancher le ou les cordons d'alimentation

Dispositif de déconnexion principal **– Les cordons (ou le cordon) d'alimentation sont considérés comme le dispositif de déconnexion principal du serveur et doivent être facilement accessibles une fois installés. Si les cordons (ou le cordon) d'alimentation de chaque serveur ne sont pas accessibles facilement pour permettre leur débranchement, vous êtes responsable d'installer un dispositif de déconnexion électrique pour l'ensemble de l'étagère. Ce dispositif de déconnexion électrique doit être facilement accessible et doit être étiqueté de façon à ce qu'il soit clair qu'il contrôle l'alimentation de l'ensemble de l'étagère, et pas seulement celle du ou des serveurs. Pour couper entièrement l'alimentation, deux cordons d'alimentation doivent être débranchés.**

Mettre à la terre l'étagère destinée à l'équipement – Pour éviter tout risque de choc électrique, si l'alimentation est de type CA, il faut inclure un troisième conducteur de mise à la terre avec l'installation de l'étagère. Pour l'alimentation CC, les deux goujons de mise à la terre du boîtier du châssis doivent être utilisés pour une mise à la terre de sécurité adéquate. Pour une alimentation CA, si le cordon d'alimentation du serveur est branché dans une prise qui fait partie de l'étagère, il faut prévoir une mise à la terre adéquate pour l'étagère elle-même. Si le cordon d'alimentation du serveur est branché dans une prise murale, le conducteur de mise à la terre du cordon d'alimentation assure une mise à la terre adéquate pour le serveur uniquement. Il est requis de prévoir une mise à la terre supplémentaire et appropriée pour l'étagère et les autres périphériques qui y sont installés.

Protection contre les surintensités CA – Lorsqu'une alimentation CA est utilisée, le serveur est conçu pour une source de tension d'entrée avec une protection contre les surintensités allant jusqu'à 20 ampères par cordon d'alimentation. Si le système d'alimentation pour l'étagère destinée à l'équipement est installé sur un circuit de dérivation dont la protection est supérieure à 20 ampères, il est requis de fournir une protection supplémentaire pour le serveur. La consommation de courant nominale totale d'un serveur configuré avec deux blocs d'alimentation est inférieure à 6 ampères.

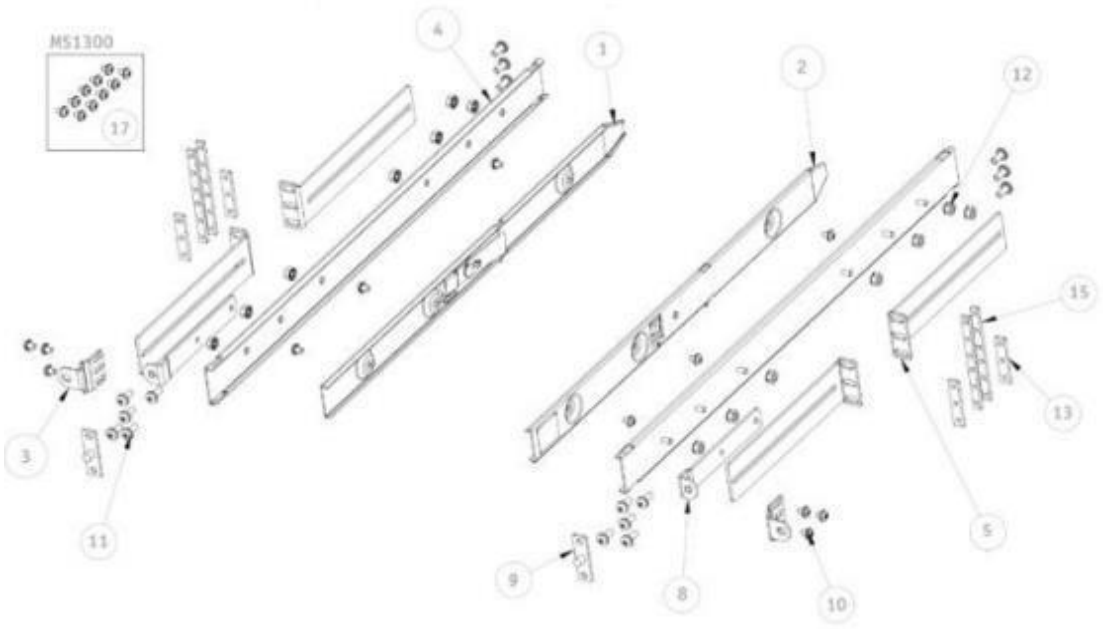
Voir la section Informations sur la sécurité et la réglementation **pour plus d'informations sur le dispositif de déconnexion principal, la mise à la terre et la protection contre les surintensités CA.**

NOTICE

Température – La température de fonctionnement du serveur, lorsqu'il est installé dans une étagère, ne doit pas être inférieure à 5 °C (41 °F) ni supérieure à 40 °C (104 °F). Les fluctuations extrêmes de température peuvent provoquer divers problèmes dans le serveur.

NOTE : La plateforme illustrée dans les instructions d'installation ci-dessous est différente du serveur CG2400 et n'est utilisée qu'à des fins de démonstration.

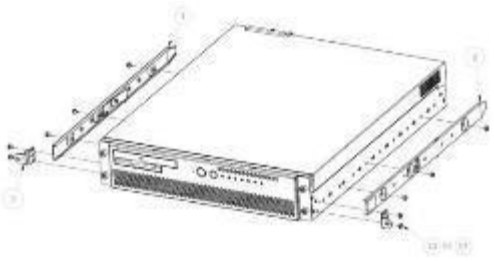
7.5.1. Ensemble pour montage en étagère TMLPMOUNT51



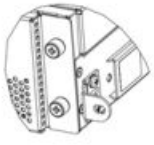
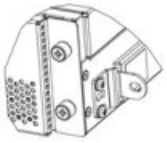
Élément	Qté	Description
1	1	RAIL INTÉRIEUR GAUCHE
2	1	RAIL INTÉRIEUR DROIT
3	2	OREILLE DE MONTAGE
4	2	RAIL EXTÉRIEUR
5	4	SUPPORT EN L 19 PO EIA
8	2	SUPPORT DE MONTAGE À 2 MONTANTS
9	2	ADAPTATEUR LARGE EIA
10	12	VIS « SEM » 8-32 X 1/4
11	16	VIS « SEM » 10-32 X 1/2
12	14	ÉCROU KEPS 8-32
13	4	BARRE AVEC TROUS FILETÉS 1U EIA
15	4	BARRE AVEC TROUS FILETÉS 2U EIA
17	12	VIS M4 X 0,7 pour MS1300

NOTE : Les barres avec trous filetés 2U permettent l'installation d'un ensemble de rails dans un emplacement d'étagère 1U lorsque de l'équipement est déjà installé au-dessus et au-dessous de cet emplacement ouvert.

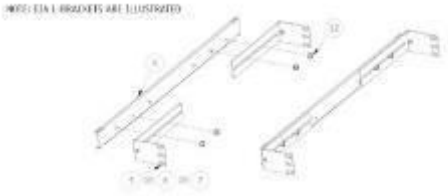
7.5.2. Installer les rails intérieurs et les oreilles de montage

Étape_1	Fixer le rail intérieur gauche (élément 1) et le rail intérieur droit (élément 2) au châssis avec 3 vis (élément 10) par rail intérieur.	
Étape_2	Fixer les 2 oreilles de montage (élément 3) au châssis à l'aide de 2 vis (élément 10) par oreille de montage.	

Les oreilles de montage (élément 3) peuvent être retournées pour positionner l'équipement plus en avant dans l'étagère.

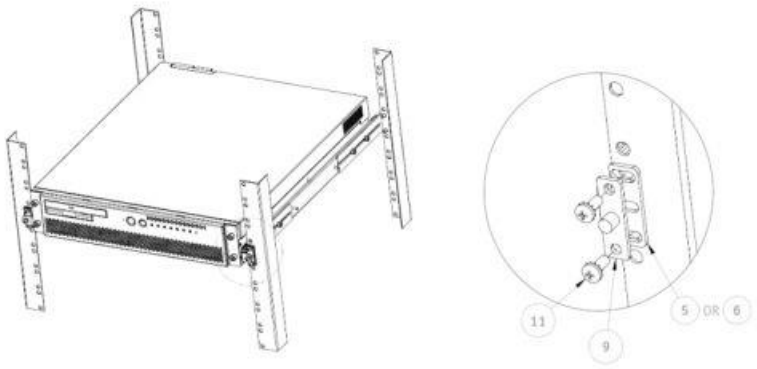



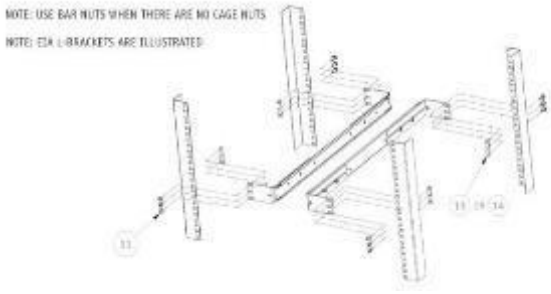
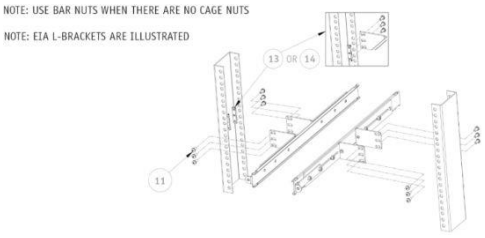
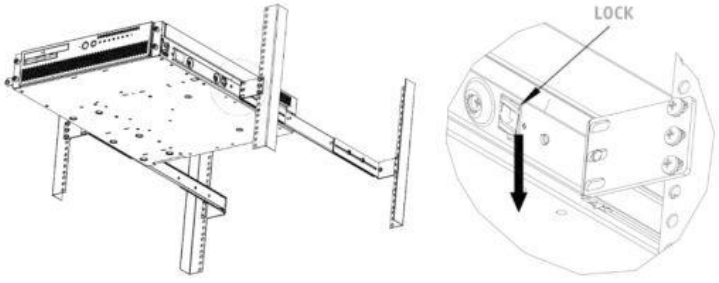
7.5.3. Bâtir l'assemblage des rails extérieurs

Étape_1	Insérer 2 supports en L (élément 5 pour 19 po EIA, élément 6 pour 23 po EIA ou élément 7 pour 23 po ETSI) sur les tiges filetées d'un rail extérieur (élément 4) comme montré sur la figure.	Assemblage des supports en L (4 montants de moins de 24 po de profondeur) 
Étape_2	Visser sans serrer 2 écrous (élément 12) par support en L.	
Étape_3	Ajuster les supports en L à la longueur requise et serrer les écrous.	
Étape_4	Répéter les étapes 1 à 3 pour bâtir un total de 2 assemblages de rails extérieurs.	

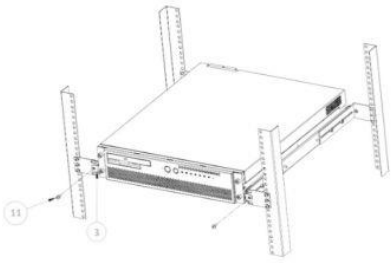
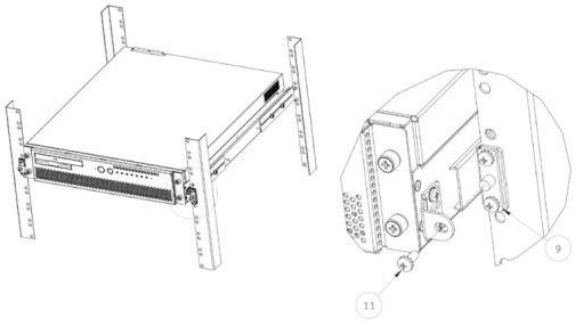
7.5.4. Fixer les assemblages de rails extérieurs aux montants de l'étagère

Lors d'une installation dans une étagère à 4 montants avec un espacement de trous EIA large, l'adaptateur large EIA (élément 9) doit être installé sur le dessus des supports en L avant avec 2 vis (élément 11) par support en L comme montré sur la figure.

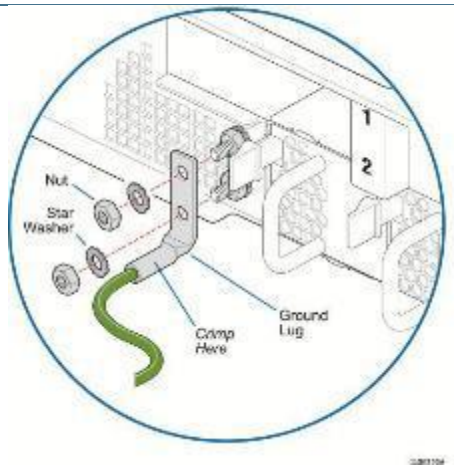


Étape_1	Fixer les assemblages de rails extérieurs (tels qu'ils ont été bâtis au cours de la phase Bâtir l'assemblage des rails extérieurs) à l'étagère avec 8 ou 12 vis (élément 11). Si l'étagère est conçue pour utiliser des écrous à cage, aucune barre avec trous filetés ne sera requise. Si l'étagère a des trous ronds, des barres avec trous filetés (élément 13 pour EIA et élément 14 pour ETSI) doivent être utilisées. S'assurer que le schéma des trous de la barre avec trous filetés correspond au schéma des trous du support en L. NOTE : Si l'étagère n'est pas conçue pour des écrous à cage et que plusieurs systèmes 1U doivent être installés immédiatement l'un au-dessus de l'autre, des barres avec trous filetés 2U (élément 15 pour EIA et élément 16 pour ETSI) doivent être utilisées pour des raisons de commodité.	Assemblage des rails extérieurs dans une étagère à 4 montants  Assemblage des rails extérieurs dans une étagère à 2 montants 
Étape_2	Faire glisser l'équipement dans l'étagère, en s'assurant que les rails intérieurs s'emboîtent dans les rails extérieurs. Soutenir le poids du système jusqu'à ce que le mécanisme de verrouillage s'enclenche dans les rails extérieurs. NOTE : Pour retirer l'équipement, le faire glisser vers l'avant jusqu'à ce que vous puissiez accéder aux mécanismes de verrouillage. Appuyer sur les mécanismes de verrouillage des deux côtés et continuer à sortir l'équipement, tout en supportant entièrement le poids du système.	Libération du mécanisme de verrouillage 

7.5.5. Fixer l'équipement

Étape_1	Fixer chaque oreille de montage (élément 3) à un support en L avant avec un total de 2 vis (élément 11) comme montré sur les figures.	Fixer l'équipement dans une étagère à 4 montants (EIA standard)  Fixer l'équipement dans une étagère à 4 montants (norme EIA large) 

7.5.6. Mise à la terre CC

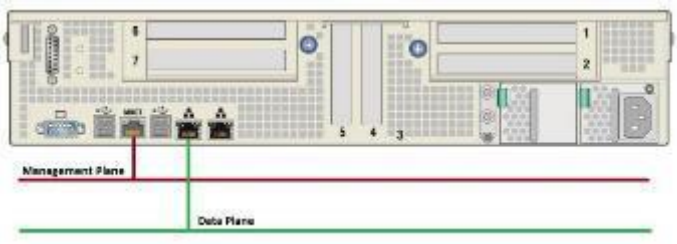
Étape_1	Si une cosse de mise à la terre est installée, retirer les 2 écrous et rondelles des goujons de la cosse de mise à la terre. Retirer la cosse de mise à la terre.	
Étape_2	Dénuder 19 mm (0,75 po) du câble de mise à la terre de calibre AWG no 8.	
Étape_3	Insérer le câble de mise à la terre de calibre AWG no 8 dans la cosse de mise à la terre. Sertir la cosse sur le câble à l'aide d'une pince à sertir manuelle appropriée (ex. l'outil de sertissage Panduit CT-1700 ajusté comme suit : code de couleur = rouge; numéro de matrice = P21).	
Étape_4	Installer la cosse de mise à la terre sur les goujons, en la fixant à l'aide des 2 écrous et rondelles.	

7.6. Raccordement des câbles réseau

Connecter les câbles réseau conformément à l'image ci-dessous :

1. Connecter un câble RJ45 au port MNGT pour le plan de gestion.
2. Connecter un câble RJ45 au port de données de gauche (CIR1) pour le plan des données.

Figure 20. Raccordement réseau



> Vous êtes maintenant prêt à fabriquer et à connecter les cordons d'alimentation.

7.7. Fabrication et connexion d'un cordon d'alimentation CC

NOTE : Pour un bloc d'alimentation CA ou pour plus d'informations, voir la section Câblage.

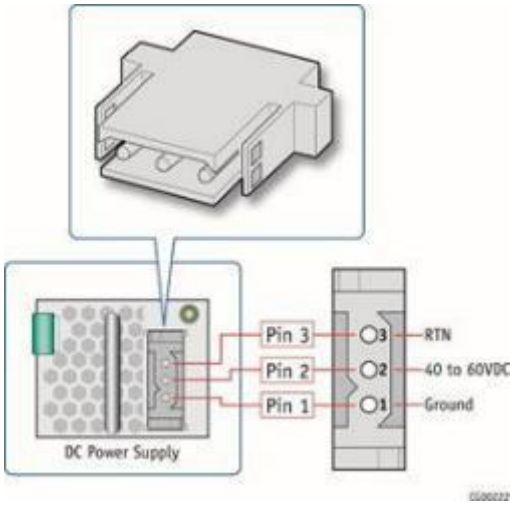
NOTICE

Avant de travailler avec ce produit ou d'exécuter les instructions décrites dans la section Guide de démarrage ou dans d'autres sections, lire la section Informations sur la sécurité et la réglementation propre au produit. Les instructions d'assemblage contenues dans cette documentation doivent être suivies pour garantir et maintenir la conformité avec les certifications et approbations existantes associées au produit. Utiliser uniquement les composants décrits et réglementés spécifiés dans cette documentation. L'utilisation d'autres produits/composants annulera la certification CSA et les autres approbations réglementaires du produit et entraînera très probablement une non-conformité avec les réglementations relatives au produit dans la ou les régions dans lesquelles le produit est vendu.

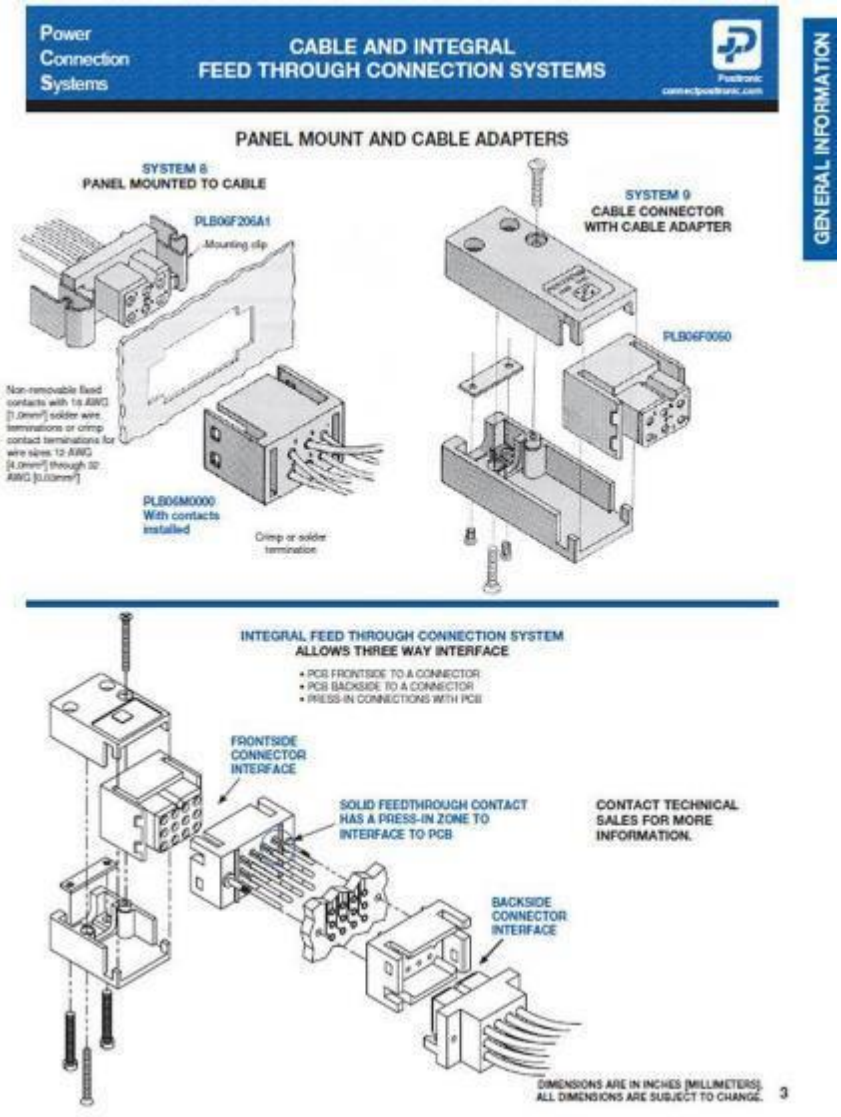
7.7.1. Connecteur d'entrée du bloc d'alimentation CC

Description du connecteur

Le connecteur d'entrée du bloc d'alimentation CC est un Positronic à 3 broches. Ce connecteur est conçu pour supporter 20 A par broche. Une broche de mise à la terre n'est pas nécessaire, car la plateforme est équipée de deux goujons de mise à la terre sur son panneau arrière.



Processus d'assemblage du connecteur



7.7.2. Fabrication des cordons d'alimentation

⚠WARNING **L'installation de ce produit doit être effectuée conformément aux codes de câblage nationaux et aux réglementations locales.**

Pour fabriquer les cordons d'alimentation (extrémités qui seront branchées dans le CG2400), le matériel, les outils et les fils spécifiés ci-dessous sont nécessaires.

NOTE : Les autres extrémités des cordons devront être fabriquées conformément aux codes de câblage nationaux et aux réglementations locales, en plus de tenir compte des exigences de l'installation d'alimentation électrique de votre centre de données.

Description	Quantité	Numéro de pièce du fabricant	Lien
Fil noir toronné de calibre AWG no 12 pour fabriquer le cordon	Longueur requise		

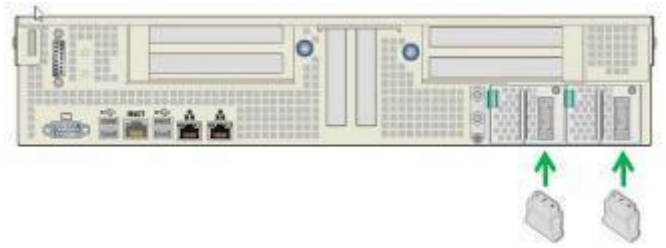
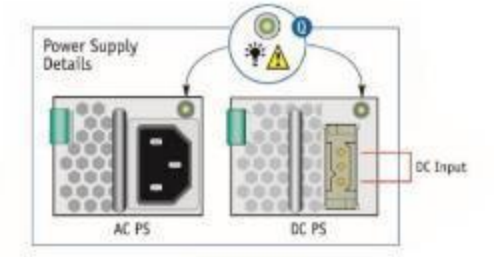
Description	Quantité	Numéro de pièce du fabricant	Lien
d'alimentation en fonction de la longueur requise			
Fil rouge toronné de calibre AWG no 12 pour fabriquer le cordon d'alimentation en fonction de la longueur requise	Longueur requise		
Connecteur homologue Positronic pour l'entrée du bloc d'alimentation CC (comprend un assemblage de décharge de traction)	1 (fourni avec le module d'alimentation CC)	PLA03F7050/AA	Catalogue Positronic
Cosse à sertir de calibre 16 Positronic	3 (fourni avec le module d'alimentation CC)	FC112N2/AA-14	Catalogue Positronic
Vis de décharge de traction	2 (fourni avec le module d'alimentation CC)	Fait partie de l'ensemble 1059-8642 Voir Plateforme, modules et accessoires	
Plaque de décharge de traction	1 (fourni avec le module d'alimentation CC)	Fait partie de l'ensemble 1059-8642 Voir Plateforme, modules et accessoires	
Vis Phillips à tête plate	2 (fourni avec le module d'alimentation CC)	Fait partie de l'ensemble 1059-8642 Voir Plateforme, modules et accessoires	
Pince à sertir manuelle DMC AF8	1	AF8	• Catalogue des pinces à sertir manuelle DMC • Fiche technique – DMC AF8
Outil d'extraction manuelle	1	9081-0-0-0	• Catalogue des outils d'extraction Molex • Spécifications

Voir la section Câblage pour un lien vers une vidéo montrant comment sertir les broches et les assembler dans le connecteur.

Étape_1	Dénuder l'extrémité d'un fil noir toronné de calibre AWG no 12 sur une longueur de 6,6 mm (0,26 po).
Étape_2	Dénuder l'extrémité d'un fil rouge toronné de calibre AWG no 12 sur une longueur de 6,6 mm (0,26 po).
Étape_3	Insérer chaque fil dans une cosse à sertir. Suivre la procédure du fabricant de la cosse à sertir, en utilisant la pince à sertir manuelle appropriée, comme spécifié dans la fiche technique du AF8 de DMC.
Étape_4	Insérer le fil rouge serti et le fil noir serti dans les douilles appropriées du boîtier de la prise.
Étape_5	Insérer la plaque de décharge de traction dans la partie appropriée de l'assemblage de décharge de traction.
Étape_6	Insérer le connecteur avec les fils dans le sous-ensemble de l'assemblage de décharge de traction.
Étape_7	Placer le couvercle pour compléter l'assemblage de décharge de traction.

Étape_8	Insérer et serrer les 2 vis Phillips à tête plate (une de chaque côté) pour bien fermer l'assemblage.
Étape_9	Insérer et serrer les 2 vis de décharge de traction pour fixer la plaque de décharge de traction.

7.7.3. Branchement de l'alimentation CC

Étape_1	Brancher un cordon avec une classification appropriée d'une source d'alimentation externe dans chaque bloc d'alimentation situé à l'arrière de la plateforme.	
Étape_2	Vérifier que la DEL de chaque bloc d'alimentation est verte clignotante (charge utile désactivée) ou verte fixe (charge utile activée). Si ce n'est pas le cas, voir Composants de la plateforme pour une description du comportement des DEL.	

7.8. Confirmation de l'établissement des liaisons réseau

Lorsque la DEL du bouton d'alimentation est **verte allumée** (clignotement normal ou allumée), confirmer la connexion LAN avec le plan de gestion et le plan des données :

- La DEL de droite du CIR de gestion du serveur (MNGT) doit être **verte allumée**.
- La DEL de droite du CIR1 de la charge utile doit être **verte allumée** si elle est connectée à un équipement/port 10GbE, et **jaune allumée** si elle est connectée à un équipement/port 1GbE.

Voir Composants de la plateforme pour plus d'informations sur le comportement des DEL.

Si le comportement des DEL n'est pas conforme aux attentes, demander au personnel des TI de vérifier l'état du réseau en amont (le port du commutateur de l'étagère pourrait être désactivé).

7.9. Découvrir l'adresse IP de gestion de la plateforme

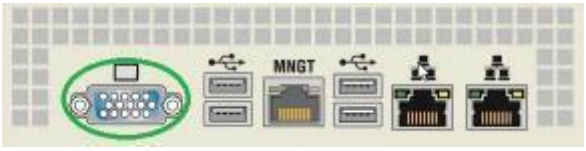
L'adresse IP de gestion de la plateforme peut être trouvée dans le BIOS à l'aide d'un port d'affichage VGA (connexion physique).

7.9.1. Découvrir l'adresse IP de gestion dans le BIOS via le port d'affichage VGA

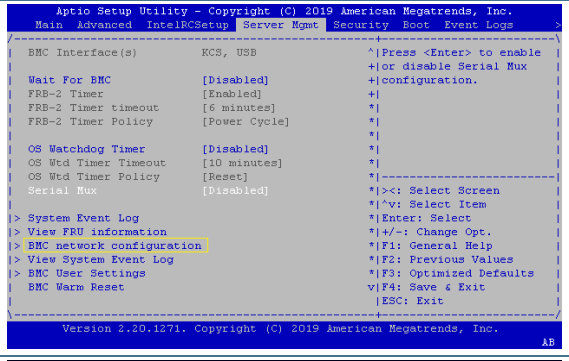
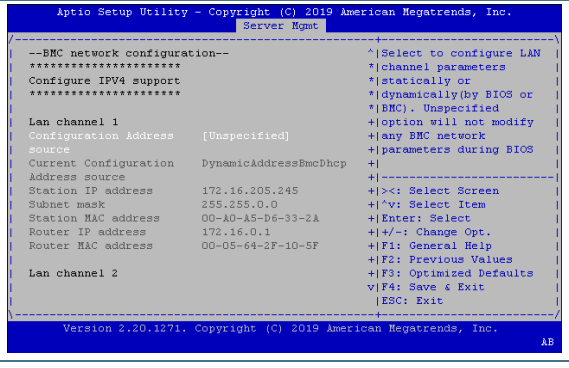
7.9.1.1. Préalables

1	Une connexion physique au port d'affichage VGA de l'appareil est requise.
2	Une souris et/ou un clavier sont connectés.

7.9.1.2. Emplacement du port



7.9.1.3. Accéder au menu BMC network configuration

Étape_1	À partir du menu UEFI/BIOS, naviguer jusqu'à l'onglet **Server Mgmt**.	
Étape_2	Sélectionner **BMC network configuration**.	
Étape_3	Le menu **BMC network configuration** s'affiche. **NOTE :** Lorsque la plateforme est démarrée après avoir été éteinte, l'UEFI/BIOS peut se charger avant que le BMC n'ait reçu son adresse IP. Dans ce cas, les informations du menu UEFI/BIOS devront être actualisées en redémarrant le serveur et en entrant à nouveau dans le menu UEFI/BIOS.	

> Avec l'IP de gestion, vous pouvez maintenant accéder à l'interface Web de gestion.

7.10. Préparation de l'installation du système d'exploitation

Étape_1	Choisir le système d'exploitation nécessaire en fonction des exigences de votre application (CentOS 7.6 ou la version la plus récente est recommandé).

Étape_2	Confirmer que la version du système d'exploitation à installer inclut ou est compatible avec le pilote d'interface réseau suivant : **i40e**.
Étape_3	Si requis, télécharger le fichier ISO du système d'exploitation à installer.

Pour une liste des systèmes d'exploitation compatibles connus, voir Systèmes d'exploitation validés.

Pour de l'information sur les composants, voir Mappage PCI.

7.11. Installation d'un système d'exploitation

7.11.1. Préalables

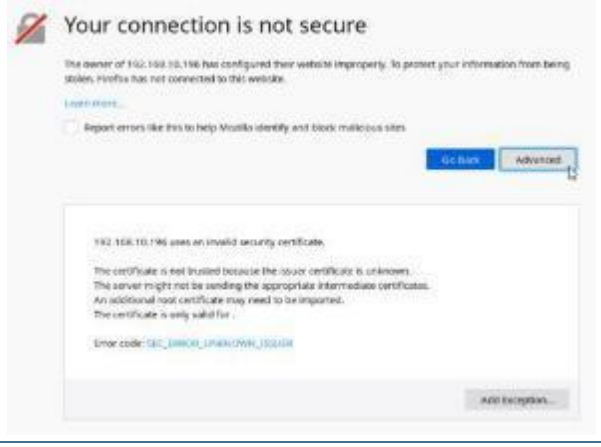
1	L'adresse IP du BMC est connue (voir la section Configuration > Contrôleur de gestion de carte mère – BMC pour obtenir le paramètre IP_GESTION_BMC).
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.

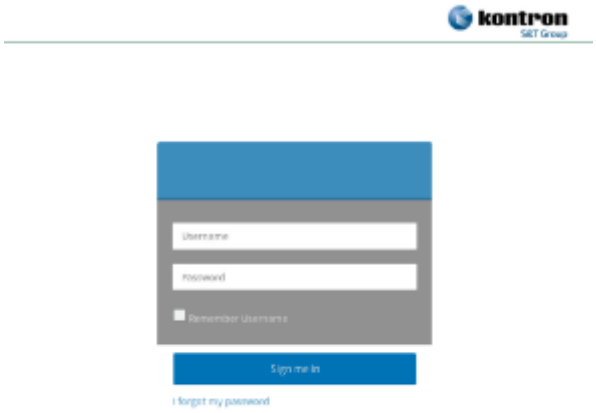
7.11.2. Considérations relatives au navigateur

HTML5	Pour établir une communication avec l'interface utilisateur Web, un navigateur Web prenant en charge HTML5 est nécessaire.
Certificat auto-signé HTTPS	Lors de l'établissement d'une connexion à l'interface Web, il est obligatoire d'accepter le certificat auto-signé HTTPS. Pour plus d'information sur l'acceptation des certificats auto-signés HTTPS, se reporter à la documentation du navigateur Web.
Autorisation de téléchargement de fichiers	Le téléchargement de fichiers à partir du site doit être autorisé. Pour plus d'information sur les autorisations de téléchargement de fichiers, se reporter à la documentation du navigateur Web.
Témoins	Les témoins doivent être activés pour pouvoir accéder au site Web. Pour plus d'information sur l'activation des témoins, se reporter à la documentation du navigateur Web.

NOTE : La procédure peut varier selon le navigateur utilisé. Les exemples fournis utilisent Firefox.

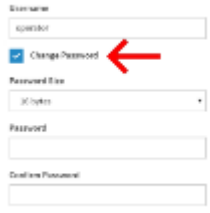
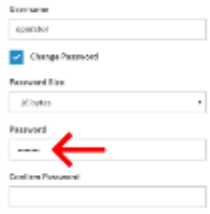
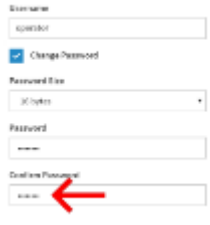
7.11.3. Établir la communication avec l'interface utilisateur Web du BMC

Étape_1	À partir d'un ordinateur distant ayant accès au réseau de gestion, ouvrir une fenêtre de navigateur et entrer l'adresse IP découverte pour le BMC. NOTE : Le préfixe HTTPS est obligatoire. *https://[IP_GESTION_BMC]*	
Étape_2	Cliquer sur **Advanced** pour lancer le processus d'acceptation du certificat auto-signé HTTPS. De l'information sur le message d'erreur s'affichera.	

Étape_3	Cliquer sur **Add Exception...** La fenêtre contextuelle Add Security Exception s'affichera. Cliquer sur **Confirm Security Exception** pour autoriser le navigateur à accéder à l'interface utilisateur Web de gestion de cette interface.	
Étape_4	Ouvrir une session dans l'interface utilisateur Web du BMC à l'aide des données d'accès appropriées. **NOTE :** Le nom d'utilisateur et le mot de passe par défaut de l'interface utilisateur Web sont admin/admin.	
Étape_5	Vous avez maintenant accès à l'interface utilisateur Web de gestion du BMC. Vous pouvez utiliser l'interface.	

7.11.4. Changer le nom d'utilisateur et le mot de passe

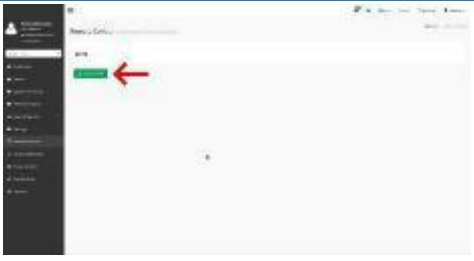
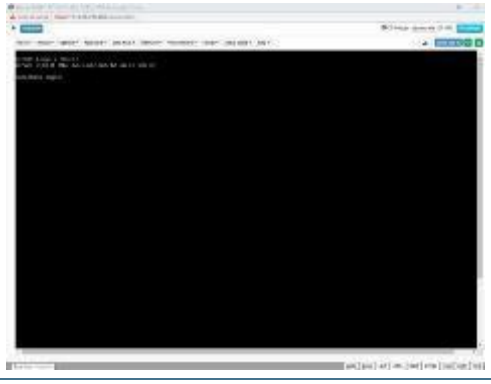
Noter que le champ du mot de passe est obligatoire, **qu'il doit comporter un minimum de 8 caractères et qu'il ne doit pas contenir de mots du dictionnaire.** Il est recommandé, mais pas obligatoire, de saisir un mot de passe fort composé d'au moins une lettre majuscule, d'un caractère alphanumérique et d'un caractère spécial. **Ne pas utiliser les symboles du code ASCII étendu, car ils ne sont pas gérés par l'outil IPMI.**

Étape_1	Cliquer sur **Settings** dans le menu de gauche puis cliquer sur **User Management**.	
Étape_2	Sélectionner l'utilisateur à gérer. **NOTE :** Le premier et le deuxième utilisateur sont des champs réservés, leurs noms d'utilisateur ne peuvent donc pas être modifiés.	
Étape_3	Modifier le champ **Username** si nécessaire.	
Étape_4	Cocher la case **Change Password**.	
Étape_5	Créer un nouveau mot de passe. **NOTE :** Il est recommandé, mais pas obligatoire, de saisir un mot de passe fort composé d'au moins une lettre majuscule, d'un caractère alphanumérique et d'un caractère spécial**. Ne pas utiliser les symboles du code ASCII étendu, car ils ne sont pas gérés par l'outil IPMI.** Noter que le champ du mot de passe est obligatoire et qu'il doit comporter un minimum de 8 caractères lorsque le service SNMP est activé.	
Étape_6	Confirmer le mot de passe.	

Étape_7	Cliquer sur **Save**.	

7.11.5. Lancer le KVM

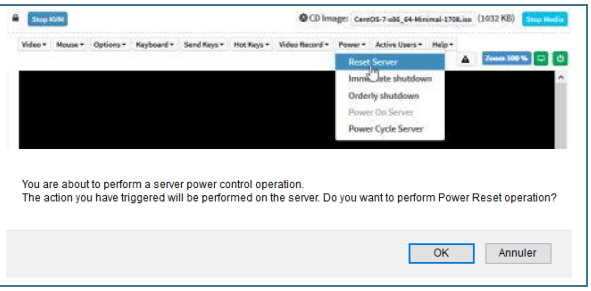
L'interface utilisateur Web permet de contrôler le serveur à distance via une interface KVM (écran-clavier-souris).

Étape_1	Dans le menu de gauche, cliquer sur **Remote Control**.	
Étape_2	Dans le menu **Remote Control**, cliquer sur le bouton **Launch KVM**.	
Étape_3	Une nouvelle fenêtre de navigateur s'ouvre et affiche l'écran du serveur. **NOTE :** Si un système d'exploitation est installé, l'image affichée pourrait être celle du système d'exploitation.	

7.11.6. Monter l'image du système d'exploitation via un support virtuel

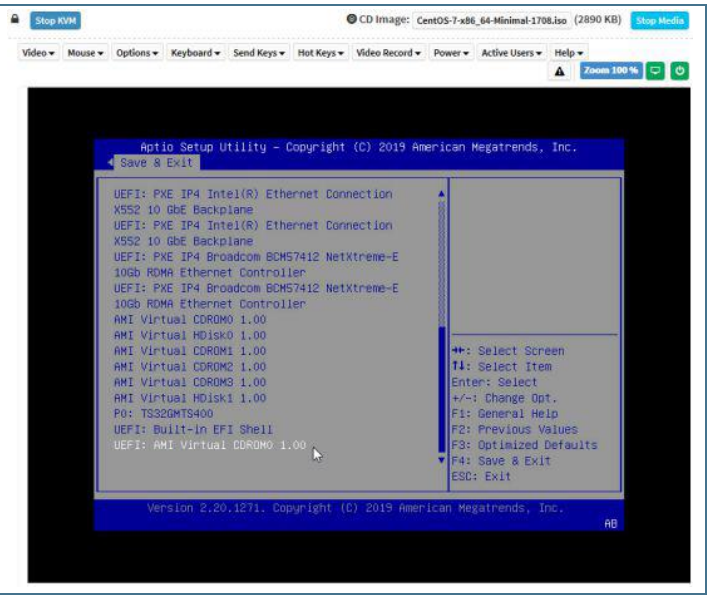
Étape_1	Dans la vue du KVM de l'écran du serveur, cliquer sur **Browse File** en haut à droite de l'écran. Sélectionner le fichier ISO à monter et cliquer sur **Open**.	
Étape_2	Une fois le fichier ISO chargé, cliquer sur **Start Media** en haut à droite de l'écran. **NOTE :** Une fois cliqué, le bouton Start Media devient le bouton **Stop Media**.	

7.11.7. Accéder au menu de configuration du BIOS

Étape_1	Dans le menu déroulant **Power**, sélectionner **Reset Server** pour accéder au menu BIOS. Cliquer sur **OK** pour confirmer l'opération. **NOTE :** Lorsqu'une commande de réinitialisation du serveur est lancée, quelques secondes peuvent s'écouler avant que l'écran d'accueil du BIOS ne s'affiche.	

Étape_2	Lorsque l'écran d'accueil du BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration du BIOS. **NOTE :** Il peut s'écouler quelques secondes avant que l'écran d'accueil du BIOS n'affiche le message de confirmation "Entering Setup…". **Conseil :** Certains utilisateurs appuient plusieurs fois et très rapidement sur Échap/F2 (DEL/F2) pour s'assurer que le serveur attrape la touche et entre dans le menu de configuration du BIOS. Cela peut entraîner l'affichage du message suivant sur l'écran du KVM : **HID Queue is about to get full. Kindly hold on a second(s)...** Kontron suggère de modifier le paramètre **Setup Prompt Timeout** pour donner aux utilisateurs plus de temps pour réagir. Maintenir l'attention (monotâche) sur la fenêtre KVM est également une bonne pratique pour entrer dans le menu de configuration du BIOS chaque fois que c'est nécessaire. Le paramètre **Setup Prompt Timeout** se trouve dans l'onglet **Boot** du menu de configuration du BIOS. La valeur par défaut est de 1 seconde. La changer pour une valeur comprise entre 3 et 10 secondes constitue une bonne cible.	
Étape_3	L'écran d'accueil du BIOS affiche **"Entering Setup..."**. NOTE : L'affichage et l'entrée dans le menu de configuration du BIOS prendront quelques secondes.	
Étape_4	Le menu de configuration du BIOS s'affiche.	

7.11.8. Sélectionner l'ordre de démarrage dans le menu Boot Override

Étape_1	Dans le menu de configuration du BIOS et à l'aide des flèches du clavier, sélectionner le menu **Save & Exit**. Dans la section **Boot Override**, sélectionner **UEFI: AMI Virtual CDROM0 1.00** et appuyer sur **Entrée**. Le serveur redémarrera et la procédure d'installation des supports démarrera.	

> Vous avez maintenant tout ce qu'il faut pour terminer l'installation du système d'exploitation en fonction des exigences de votre application.

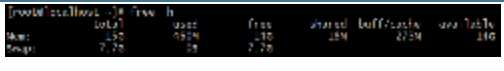
7.11.9. Compléter l'installation du système d'exploitation

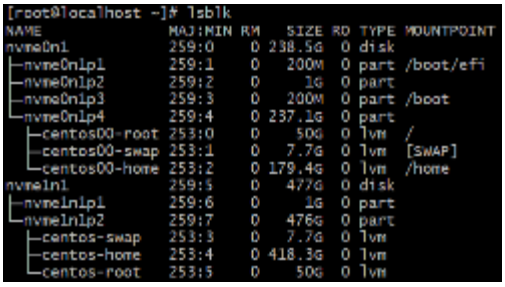
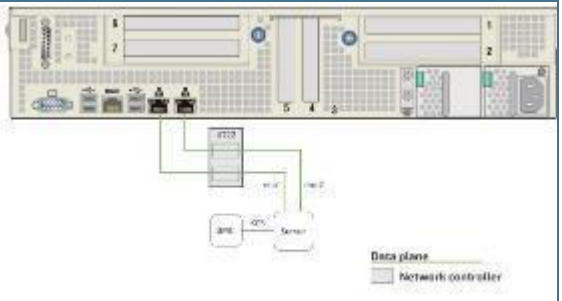
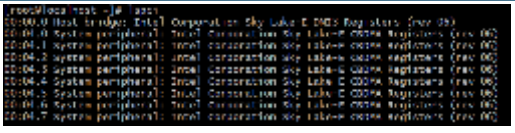
Étape_1	Terminer l'installation en suivant les invites à l'écran du système d'exploitation installé.

> (Optionnel) Après l'installation, si un démarrage à partir du réseau (PXE) se produit et n'est pas souhaité, il se peut que le programme d'installation de votre système d'exploitation n'ait pas modifié l'ordre du démarrage dans le BIOS. Pour remédier à la situation, entrer à nouveau dans le menu de configuration du BIOS et suivre les étapes ci-dessous.

7.11.10. Vérifier l'installation du système d'exploitation

Tous les résultats et toutes les commandes peuvent varier en fonction du système d'exploitation et des périphériques ajoutés.

Étape_1	Redémarrer le système d'exploitation comme recommandé, puis accéder à l'invite de commande du système d'exploitation.	
Étape_2	Vérifier qu'aucun message d'erreur ou d'avertissement n'est affiché dans dmesg à l'aide des commandes suivantes. InviteSE_ServeurLocal:~# **dmesg | grep -i fail** InviteSE_ServeurLocal:~# **dmesg | grep -i Error** InviteSE_ServeurLocal:~# **dmesg | grep -i Warning** InviteSE_ServeurLocal:~# **dmesg | grep -i "Call trace"** **NOTE :** Si des messages ou des avertissements s'affichent, consulter la documentation du système d'exploitation pour y remédier.	
Étape_3	Vérifier que les modules DIMM sont détectés. InviteSE_ServeurLocal:~# **free -h**	

Étape_4	Vérifier que toutes les unités de stockage sont détectées. InviteSE_ServeurLocal:~# **lsblk**	
Étape_5	Confirmer que les contrôleurs d'interfaces réseau du plan des données sont chargés par le pilote **i40e**. InviteSE_ServeurLocal:~# **dmesg | grep i40e** **NOTE :** Deux CIR 10GbE devraient être découverts.	
Étape_6	Confirmer que toutes les interfaces réseau sont détectées. InviteSE_ServeurLocal:~# **ip address** **NOTE :** Deux interfaces réseau devraient être détectées.	
Étape_7	Configurer les contrôleurs d'interfaces réseau en fonction de vos exigences. **NOTE :** Les noms des interfaces pourraient différer selon le système d'exploitation installé. Cependant, les paramètres « Bus:Device.Function » restent les mêmes pour l'interface, quel que soit le système d'exploitation.	
Étape_8	Installer ipmitool et pciutils à l'aide du gestionnaire de paquets et mettre à jour les paquets du système d'exploitation. La version recommandée d'ipmitool est la 1.8.18. Exemple : InviteSE_ServeurLocal:~# **yum update** InviteSE_ServeurLocal:~# **yum install ipmitool** InviteSE_ServeurLocal:~# **yum install pciutils** **NOTE :** La mise à jour des paquets peut prendre quelques minutes.	
Étape_9	(Optionnel) Si des cartes d'expansion PCIe ou d'autres composants matériels sont installés, vérifier qu'ils sont détectés. InviteSE_ServeurLocal:~# **lspci | grep [MOT-CLÉ]** **NOTE :** Le mot-clé est un mot unique qui permet d'identifier le composant matériel. Le Mappage PCI du produit pourrait aider avec cette validation.	

Étape_10	Vérifier la communication entre le système d'exploitation et le BMC. InviteSE_ServeurLocal:~# **ipmitool mc info**	LocalServer_OSPrompt:~# ipmitool mc info Device ID : 32 Device Revision : 1 Firmware Revision : 0.01 IPMI Version : 2.0 Manufacturer ID : 15000 Manufacturer Name : Kontron Product ID : 1100 (0x044c) Product Name : Unknown (0x44C) Device Available : yes Provides Device SDRs : no Additional Device Support : Sensor Device SDR Repository Device SEL Device FRU Inventory Device IPMB Event Receiver IPMB Event Generator Chassis Device Aux Firmware Rev Info 0x09 0x33 0x9b 0xf8

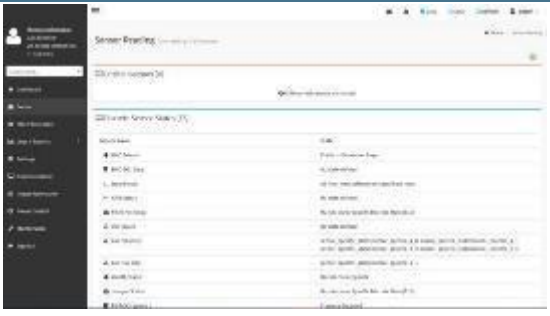
7.12. Conduite de tests de performance sur une application

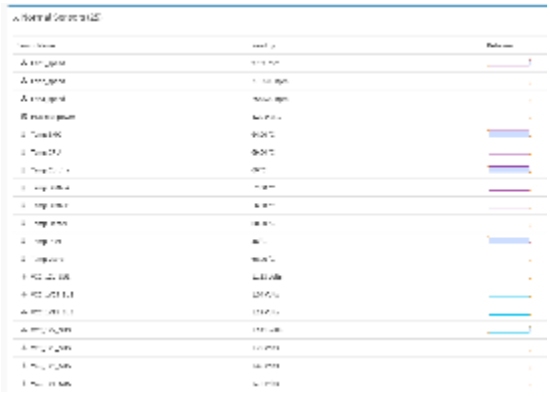
Installer l'application et procéder aux tests de performance.

7.13. Surveillance des capteurs de la plateforme

NOTE : Voir Accéder au BMC pour accéder à l'interface utilisateur Web du BMC. Les principaux capteurs à considérer sont les suivants :

- Capteurs de température
- Capteurs d'alimentation

Étape_1	Accéder à l'interface utilisateur Web du BMC.	
Étape_2	Dans le menu de gauche, cliquer sur **Sensor**.	
Étape_3	La liste des capteurs s'affiche.	

Étape_4	Faire défiler vers le bas pour voir la liste des capteurs.	
Étape_5	Cliquer sur un capteur pour afficher plus de détails.	

Pour une liste de tous les capteurs, voir Liste des capteurs.

Pour d'autres méthodes de surveillance, voir Surveillance des capteurs.

8/ Planification

8.1. Considérations environnementales

La plateforme CG2400 est destinée à être déployée dans les centres de données, mais elle a été conçue pour fonctionner dans une plage de température étendue de -5 °C à +55 °C (23 °F à +131 °F) et pour résister à des taux d'humidité sans condensation allant jusqu'à 95 %.

Si la plateforme est installée dans un environnement chaud, c.-à-d. où il fait entre 30 °C et 55 °C, il est recommandé de prendre des mesures supplémentaires pour optimiser le refroidissement et la circulation de l'air, car une exposition constante à des températures élevées réduit la durée de vie des équipements électroniques.

Des précautions particulières doivent être prises si la plateforme est exposée à un choc thermique, par exemple si elle est sortie d'un camion de service laissé à l'extérieur pendant la nuit à des températures inférieures à zéro puis entrée à l'intérieure en vue d'une installation dans un endroit chauffé. Dans de tels cas, il est recommandé de laisser la plateforme s'acclimater à la nouvelle température ambiante pendant au moins 4 heures avant de la mettre sous tension, afin d'éviter la condensation.

La plateforme CG2400 satisfait aux normes relatives aux vibrations aléatoires en fonctionnement, aux chocs en fonctionnement, et aux vibrations aléatoires lors du transport et du stockage. Les tests sont basés sur ETSI EN 300 019-2-3 class 3.2, ETSI EN 300 019-2-2 class 2.3 et GR-63 clause 5.4.3 et section 5.3.

Cet équipement ne doit pas être exposé directement aux éléments (soleil, pluie, vent, poussière).

8.2. Puissance consommée et budget énergétique

8.2.1. Renseignements généraux sur l'alimentation

- La puissance de sortie nominale du CG2400 est de 850 W. Cela signifie que le système doit consommer moins de 850 W à tout moment pendant le fonctionnement.
- Dans une configuration à deux blocs d'alimentation (redondants), le courant sera automatiquement partagé entre les deux blocs d'alimentation. Si une source d'alimentation ou un bloc d'alimentation connaît une défaillance, la totalité de la charge sera supportée par le bloc d'alimentation opérationnel.

8.2.2. Budget énergétique

Le budget énergétique global peut être déterminé avec l'outil Kontron Power Budget Tool disponible sur le site WEB de Kontron, ou en évaluant la puissance consommée à l'aide des chiffres ci-dessous fournis aux fins d'estimation.

8.2.2.1. Déterminer le budget énergétique

La puissance consommée est déterminée en additionnant la consommation de tous les composants de la configuration matérielle finale.

Noter que la puissance consommée par le système dépend de la configuration matérielle et des applications en cours d'exécution, qui nécessiteront rarement que tous les composants consomment simultanément leur puissance maximale. Par conséquent, les estimations réalisées avec les chiffres ci-dessous constituent les scénarios de la pire éventualité à température ambiante.

Type de composant	Composant	Watts par composant	Quantité	Sous-total (watts)
Ventilateur	Ventilateur du système	25	6	150

Type de composant	Composant	Watts par composant	Quantité	Sous-total (watts)
CPU	Processeur Xeon® Scalable	En fonction du modèle	1 ou 2	75 à 300
DIMM		En fonction du modèle Règle générale : DIMM 8 Go : 5 W DIMM 16 Go : 6 W DIMM 32 Go : 7 W DIMM 64 Go : 8 W	1 à 16	5 à 128
Carte mère	Jeu de puces, LAN, autres	30	1	30
Stockage	Disque dur de 2,5 po (SAS)	8	0 à 6	0 à 48
	Disque SSD de 2,5 po (SATA)	4	0 à 6	0 à 24
	M.2 (SATA ou NVMe)	2	0 à 2	0 à 4
PCIe	RAID / HBA	15	0 ou 1	0 ou 15
	Carte PCIe typique à faible consommation (ex. adaptateur Ethernet)	10	0 à 7	0 à 70
	Carte à haute puissance (ex. processeur graphique)	75 à 250 en fonction du modèle	1	75 à 250
			Total	**335 à 1019**

8.2.2.2. Exemple de la puissance consommée pour une configuration de taille moyenne

Dans cet exemple, la consommation maximale est de 487 W, ce qui laisse une marge de 363 W par rapport à la limite du système établie à 850 W.

Type de composant	Composant	Watts par composant	Quantité	Sous-total (watts)
Ventilateur	Ventilateur du système	25	6	150
CPU	Xeon® Scalable Gold 5218T	105	2	210
DIMM	DIMM 16 Go	6	8	48
Carte mère	Jeu de puces, LAN, autres	30	1	30
Stockage	Disque dur de 2,5 po (SAS)	8	4	32
	M.2 (SATA ou NVMe)	2	1	2
PCIe	RAID	15	1	15
			Total	**487**

8.2.3. Puissance de sortie de l'alimentation selon le déclassement thermique

Le déclassement thermique ne s'applique que lorsque le CG2400 est alimenté par un seul bloc d'alimentation.

Dans les configurations à un seul bloc d'alimentation, la puissance de sortie nominale est affectée par la température d'entrée au niveau du bloc d'alimentation (50 °C et plus). En d'autres termes, la limite de 850 W peut être abaissée selon la température d'entrée.

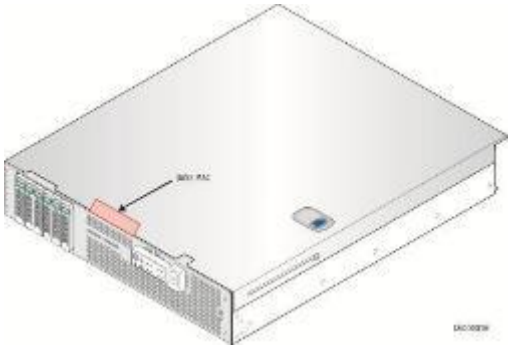
Pour cette raison, il est recommandé de planifier le budget énergétique en tenant compte de la température d'entrée. Les chiffres ci-dessous peuvent aider à la planification.

Modèle	50 ºC	55 ºC	60 ºC	65 ºC
Puissance de sortie nominale du bloc d'alimentation CA (entrée = 90 VCA)	850 W	705 W	650 W	600 W
Puissance de sortie nominale du bloc d'alimentation CC (entrée = -40 VCC)	850 W	850 W	790 W	725 W

8.3. Adresses MAC

8.3.1. Adresses MAC du CG2400

Description de l'interface	Adresse MAC	Notes
Port MNGT du BMC	MAC_BASE	Port de gestion dédié (équivalent RMM4/RMM4Lite)
CPU X722 port 1	MAC_BASE + 3	Plan des données du serveur (charge utile 10 Gbps/1 Gbps)
CPU X722 port 2	MAC_BASE + 4	Plan des données du serveur (charge utile 10 Gbps/1 Gbps)



8.3.2. Découvrir les adresses MAC de la plateforme

Les adresses MAC de la plateforme peuvent être découvertes :

- En utilisant IPMI
- En utilisant le BIOS

8.3.2.1. Découvrir une adresse MAC en utilisant IPMI

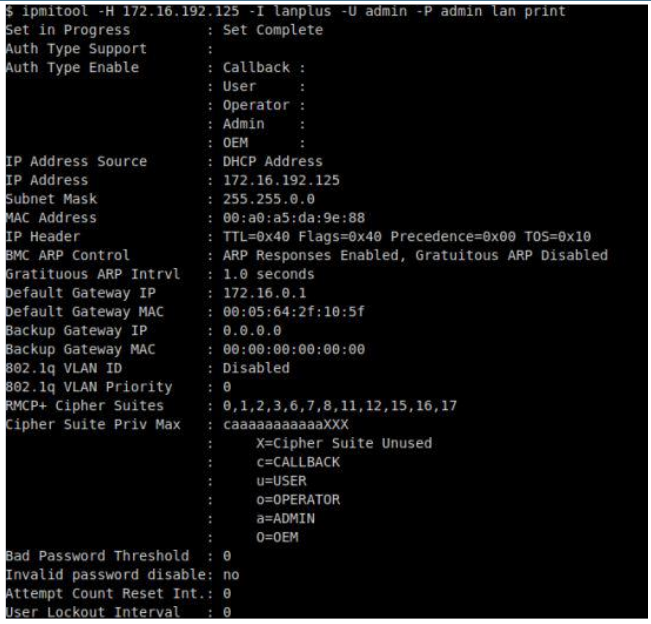
8.3.2.1.1. Préalable

1	Une version de la communauté d'ipmitool est installée sur un ordinateur distant pour permettre la surveillance à distance – il est recommandé d'utiliser la version 1.8.18 d'ipmitool.

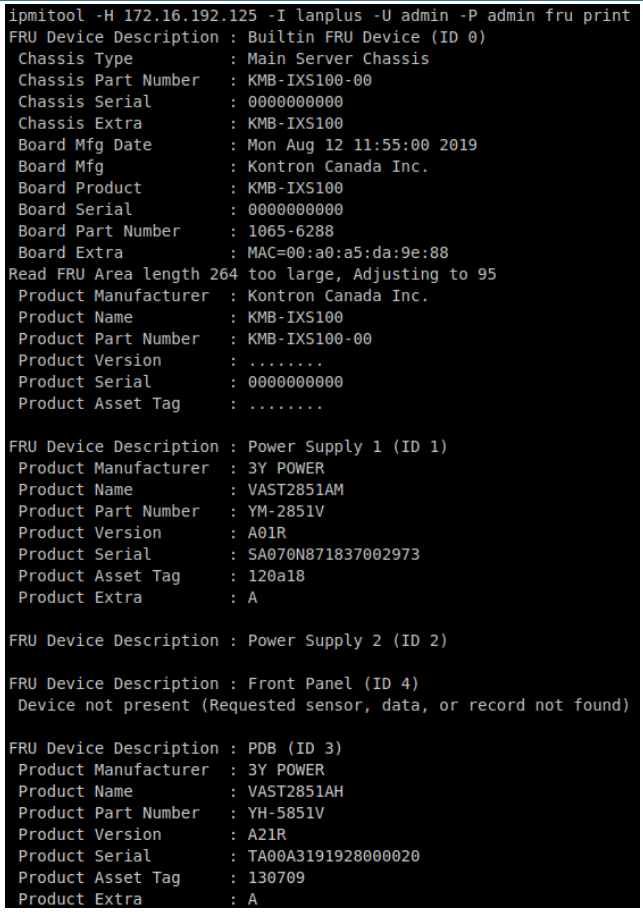
Une adresse MAC peut être découverte en utilisant IPMI avec les commandes suivantes :

- lan print
- fru print

8.3.2.1.2. Procédure avec la commande lan print d'ipmitool

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, saisir la commande souhaitée. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] lan print**	

8.3.2.1.3. Procédure avec la commande fru print d'ipmitool

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, saisir la commande souhaitée. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] fru print** L'adresse MAC est affichée dans le champ **Board Extra**.	

8.3.2.2. Découvrir une adresse MAC en utilisant le BIOS

Il y a deux méthodes pour découvrir une adresse MAC à partir du BIOS :

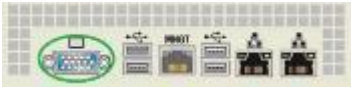
- En utilisant le port d'affichage VGA (connexion physique)
- En utilisant une console série (connexion physique)

8.3.2.2.1. Accéder au BIOS en utilisant le port d'affichage VGA (connexion physique)

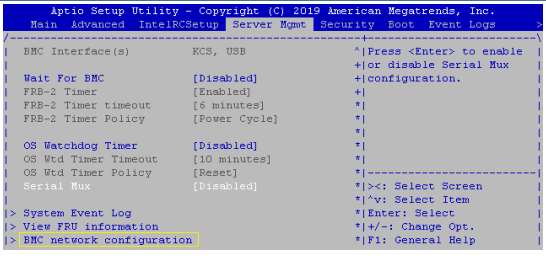
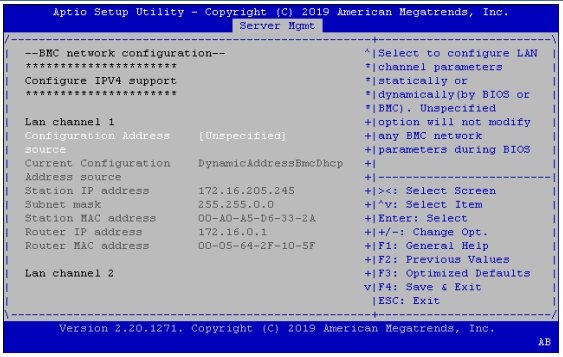
8.3.2.2.1.1. Préalables

1	Une connexion physique au port d'affichage VGA de l'appareil est requise.
2	Une souris et/ou un clavier sont connectés.

8.3.2.2.1.2. Emplacement du port



8.3.2.2.1.3. Accéder au menu BMC network configuration

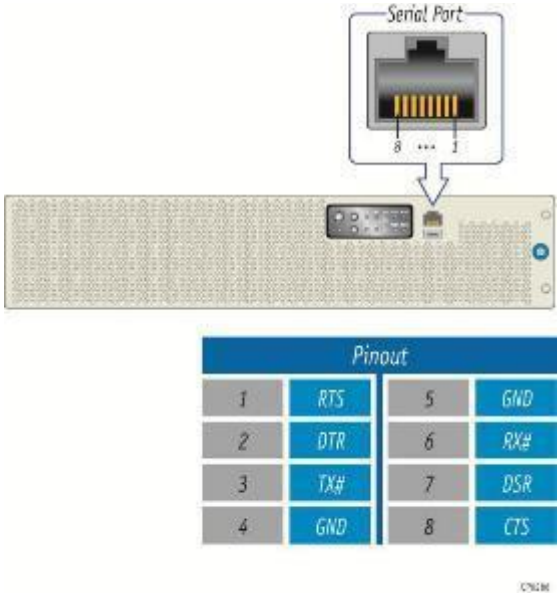
Étape_1	À partir du menu UEFI/BIOS, naviguer jusqu'à l'onglet **Server Mgmt**.	
Étape_2	Sélectionner **BMC network configuration**.	
Étape_3	Le menu **BMC network configuration** s'affiche. **NOTE :** Lorsque la plateforme est démarrée après avoir été éteinte, l'UEFI/BIOS peut se charger avant que le BMC n'ait reçu son adresse IP. Dans ce cas, les informations du menu UEFI/BIOS devront être actualisées en redémarrant le serveur et en entrant à nouveau dans le menu UEFI/BIOS.	

8.3.2.2.2. Accéder au BIOS en utilisant une console série (connexion physique)

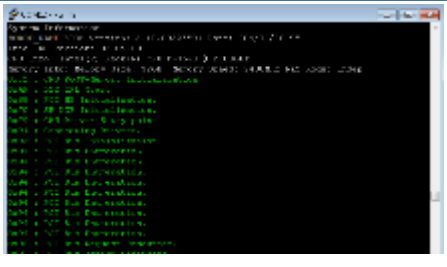
8.3.2.2.2.1. Préalables

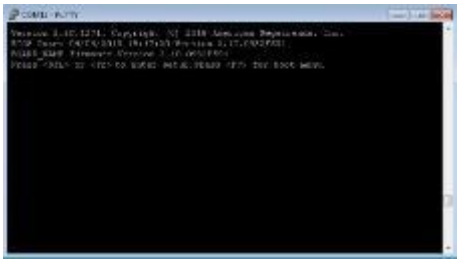
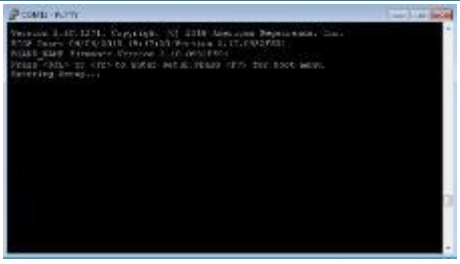
1	Une connexion physique à l'appareil est requise. **NOTE :** Le port de console série est compatible avec le câble 72-3383-01 de Cisco.
2	Un outil de console série est installé sur l'ordinateur distant. Vitesse (baud) : 115200 • Bits d'information : 8 • Bits d'arrêt : 1 • Parité : Aucune • Contrôle de flux : Aucun • Mode émulation recommandé : VT100+ **NOTE :** PuTTY est recommandé.

8.3.2.2.2.2. Emplacement du port

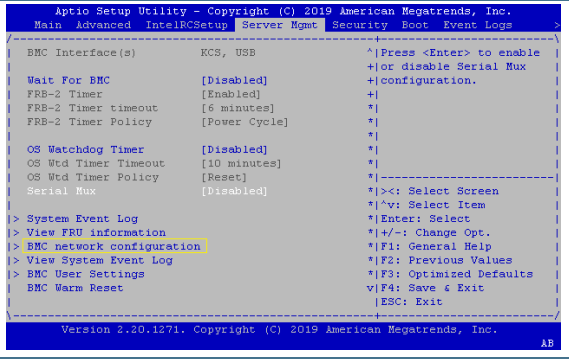


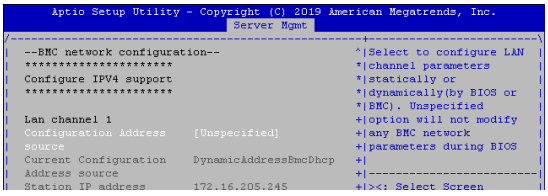
8.3.2.2.2.3. Procédure d'accès

Étape_1	À partir d'un ordinateur disposant d'une connexion physique au port série, ouvrir un outil de console série et démarrer la communication entre la console et le port auquel le système est connecté.	
Étape_2	Réinitialiser le serveur (raccourci-clavier **Ctrl-Pause** [Ctrl-Break]). **NOTE :** Si un système d'exploitation est installé, le raccourci-clavier pourrait ne pas fonctionner correctement. Si c'est le cas, réinitialiser le serveur en suivant les recommandations propres au système d'exploitation. **NOTE :** Lorsqu'une commande de réinitialisation du serveur est lancée, quelques secondes peuvent s'écouler avant que l'écran d'accueil du BIOS ne s'affiche.	

Étape_3	Lorsque l'écran d'accueil du BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration du BIOS. **NOTE :** Il peut s'écouler quelques secondes avant que l'écran d'accueil du BIOS n'affiche le message de confirmation "Entering Setup...".	
Étape_4	L'écran d'accueil du BIOS affiche **"Entering Setup..."**. **NOTE :** L'affichage et l'entrée dans le menu de configuration du BIOS prendront quelques secondes.	
Étape_5	Le menu de configuration du BIOS s'affiche.	

8.3.2.2.2.4. Accéder au menu BMC network configuration

Étape_1	À partir du menu UEFI/BIOS, naviguer jusqu'à l'onglet **Server Mgmt**.	
Étape_2	Sélectionner **BMC network configuration**.	

Étape_3	Le menu **BMC network configuration** s'affiche. **NOTE :** Lorsque la plateforme est démarrée après avoir été éteinte, l'UEFI/BIOS peut se charger avant que le BMC n'ait reçu son adresse IP. Dans ce cas, les informations du menu UEFI/BIOS devront être actualisées en redémarrant le serveur et en entrant à nouveau dans le menu UEFI/BIOS.	

8.4. Mappage PCI

La carte KMB-IXS100 peut être équipée d'un ou de deux CPU. Le nombre de CPU a une incidence sur la manière dont les numéros de bus PCI sont attribués lors de l'initialisation de l'UEFI et sur les emplacements PCIe disponibles.

CPU – présence	CPU	Plage de numéros de bus PCI	Numéros des emplacements PCIe (sur la carte mère KMB-IXS100 elle-même)	Numéros d'emplacement indiqués sur le châssis du CG2400 (arrière)
1 CPU seulement	CPU1	0-255 (0xFF)	Emplacement 5 - x16 (n'accepte pas les cartes adaptatrices de connexion PCIe) Emplacement 6 - x16 (accepte les cartes adaptatrices de connexion PCIe)	Emplacement 5 (carte mère) → Emplacement 5 (châssis) Emplacement 6 (carte mère) → Emplacements 6 et 7 (châssis)
2 CPU présents	CPU1	0-127 (0x7F)	Emplacement 5 - x16 (n'accepte pas les cartes adaptatrices de connexion PCIe) Emplacement 6 - x16 (accepte les cartes adaptatrices de connexion PCIe)	Emplacement 5 (carte mère) → Emplacement 5 (châssis) Emplacement 6 (carte mère) → Emplacements 6 et 7 (châssis)
	CPU2	128-255 (0x80-0xFF)	Emplacement 2 (accepte les cartes adaptatrices de connexion PCIe) Emplacement 3 - x16 (n'accepte pas les cartes adaptatrices de connexion PCIe) Emplacement 4 - x16 (n'accepte pas les cartes adaptatrices de connexion PCIe)	Emplacement 2 (carte mère) → Emplacements 1 et 2 (châssis) Emplacement 3 (carte mère) → Emplacement 3 (châssis) Emplacement 4 (carte mère) → Emplacement 4 (châssis)

Pour obtenir le Mappage PCI de la plateforme, utiliser la commande **lspci -nn**. Vous devrez peut-être mettre à jour la base de données de description lspci avec la commande **update-pciids**.

8.5. Plateforme, modules et accessoires

8.5.1. Éléments remplaçables (pièces de rechange)

8.5.1.1. Ventilateurs

Numéro de pièce Kontron	Description
CG2200-FANSET	Ensemble de ventilateurs (6 ventilateurs)

Numéro de pièce Kontron	Description
	

8.5.1.2. Support pour disque dur/disque SSD

Numéro de pièce Kontron	Description
NSNSASHDDCARQ 	SAS HDD/SATA SSD carrier Contents: Carrier, black plastic filler, screws (4)

8.5.1.3. Panneau frontal

Numéro de pièce Kontron	Description
CG2100-BEZEL01 	Panneau frontal du châssis

8.5.1.4. Capot supérieur

Numéro de pièce Kontron	Description
1067-1312	Ensemble de capot supérieur pour le châssis Contenu : capot supérieur et étiquette de sécurité

Numéro de pièce Kontron	Description
	

8.5.1.5. Blocs d'alimentation

Numéro de pièce Kontron	Description
1056-8389	Bloc d'alimentation CA 850 W
1056-8385	Bloc d'alimentation CC 850 W
K00837-001	Panneau de remplissage pour l'emplacement d'un bloc d'alimentation
1061-0410	Cordon d'alimentation européen CA CEE 7/7 à C13, 10 A/250 VCA, 1,8 m de long
1-340000-0	Cordon d'alimentation CA NEMA 5-15P à C13, 10 A/125 VCA, 2 m de long
1059-8642	Ensemble pour connecteur homologue de bloc d'alimentation CC
1064-4226	Cosse de mise à la terre à angle droit, calibre AWG no 8

8.5.2. Configurations PCIe et cartes adaptatrices de connexion PCIe

8.5.2.1. Emplacements PCIe

La plateforme dispose de 3 emplacements PCIe qui prennent en charge 3 cartes simple largeur, demi-hauteur, demi-longueur ou pleine longueur. Ces cartes peuvent être de type x16, x8, x4, x2 ou x1. Les cartes PCIe branchées dans les emplacements 3 et 4 se connectent au CPU2, tandis que la carte PCIe de l'emplacement 5 se connecte au CPU1.

Le tableau suivant donne les caractéristiques des 3 emplacements PCIe.

	Emplacement 3	Emplacement 4	Emplacement 5
Toutes les cartes PCIe demi-hauteur, sauf RAID	Non	Oui	Oui
RAID	Oui	Non	Non

8.5.2.2. Emplacements des cartes adaptatrices de connexion PCIe

La plateforme dispose également de deux emplacements pour cartes adaptatrices de connexion PCIe :

- Emplacement PCIe 2 (côté gauche si on fait face à la plateforme)
- Emplacement PCIe 6 (côté droit si on fait face à la plateforme)

Chacun de ces emplacements PCIe peut prendre en charge une carte adaptatrice de connexion PCIe x16 à emplacement simple ou une carte adaptatrice de connexion PCIe x8 à emplacement double.

La carte adaptatrice de connexion PCIe branchée dans l'emplacement 2 se connecte au CPU2, tandis que la carte adaptatrice de connexion PCIe dans l'emplacement 6 se connecte au CPU1.

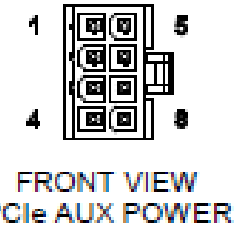
Toutes les cages d'extension PCIe peuvent prendre en charge des cartes allant jusqu'à pleine hauteur et pleine longueur.

Le tableau suivant identifie les configurations possibles et le nombre maximum de cartes PCIe pouvant être connectées au moyen de cartes adaptatrices de connexion PCIe.

Configuration des cartes adaptatrices de connexion PCIe	Cartes PCIe
2 cartes adaptatrices à emplacement simple	2 cartes x16 à simple ou double largeur
1 carte adaptatrice à emplacement simple 1 carte adaptatrice à emplacement double	1 carte x16 à simple ou double largeur 2 cartes x8 à largeur simple
2 cartes adaptatrices à emplacement double	4 cartes x8 à largeur simple

NOTES :

- Toutes les cartes installées dans les cages d'extension PCIe peuvent avoir des E/S.
- Une seule carte PCIe nécessitant une alimentation auxiliaire peut être connectée.
    - Pour avoir une telle connexion, utiliser le câble avec un connecteur à 8 broches disponible dans le support du faisceau de câbles (plateau en plastique au-dessus des blocs d'alimentation).
    - Vérifier le brochage de la carte PCIe pour confirmer qu'il correspond à celui du connecteur d'alimentation auxiliaire de la plateforme.

Broche	Signal	Couleur	Image
1	Masse	Noir	
2	Masse	Noir	
3	Masse	Noir	
4	Masse	Noir	
5	+12V	Jaune	
6	+12V	Jaune	
7	+12V	Jaune	
8	+12V	Jaune	

8.5.2.3. Cartes adaptatrices de connexion PCIe

Numéro de pièce Kontron	Description
CG2200-RISER2SX8R	Carte adaptatrice de connexion à emplacement double pour PCIe x8, Gen 3, pour l'emplacement 6 (côté droit)
CG2200-RISER1SX16R	Carte adaptatrice de connexion à emplacement simple pour PCIe x16, Gen 3, pour l'emplacement 6 (côté droit)
CG2200-RISER2SX8L	Carte adaptatrice de connexion à emplacement double pour PCIe x8, Gen 3, pour l'emplacement 2 (côté gauche)
CG2200-RISER1SX16L	Carte adaptatrice de connexion à emplacement simple pour PCIe x16, Gen 3, pour l'emplacement 2 (côté gauche)
CG2200-RISER2SPCIX*	Carte adaptatrice de connexion à emplacement double pour PCI-X, pour l'emplacement 6 (côté droit)
1065-8218*	Carte adaptatrice de connexion à emplacement triple pour PCIe x4 et x8, Gen 3, pour l'emplacement 5 (côté gauche)

* Les cartes adaptatrices de connexion PCIe CG2200-RISER2SPCIX et 1065-8218 sont des produits spécialisés. Contactez votre représentant Kontron si vous souhaitez les utiliser ou obtenir des informations complémentaires.

8.5.3. Ensemble pour montage en étagère

Code du produit	Description	Rails coulissants avec verrouillage (oui/non)	Quantité minimum de commande
TMLCMOUNT21	Ensemble pour montage d'un serveur dans une étagère de 19 po de largeur à 2 montants	Non	10
TMLPMOUNT41	Ensemble pour montage d'un serveur dans une étagère de 19 po de largeur à 2 ou 4 montants **NOTES :** • Accès aux vis par le côté pour l'installation à 2 montants • Non compatible avec les étagères HP Mulan	Non	10
TMLPMOUNT51	Ensemble pour montage d'un serveur dans une étagère de 19 po de largeur à 2 ou 4 montants **NOTES :** • Finition avec Xylan®	Oui	1
TMLPMOUNT52	Ensemble pour montage d'un serveur dans une étagère de 23 po de largeur à 2 ou 4 montants **NOTES :** • Finition avec Xylan® • Conforme à l'espacement des trous ETSI	Oui	1
TMLPSLIDE01	Supports de montage universels pour l'avant Les rails coulissants 305A-LR de 22 po d'Accuride nécessiteraient les pièces TMLPSLIDE01. Chaque ensemble contient deux supports de montage universels pour l'avant qui permettent de fixer le serveur à l'avant de l'étagère.	S. O.	1
1059-8187	Ensemble d'extension de rails de 19 po • Profondeur maximale de l'étagère lors de l'utilisation : TMLPMOUNT41 –> 36 po • TMLPMOUNT51 –> 34 po	S. O. voir le modèle des rails	1
1061-2890	Ensemble d'extension de rails de 23 po À utiliser avec TMLPMOUNT52	S. O.	1

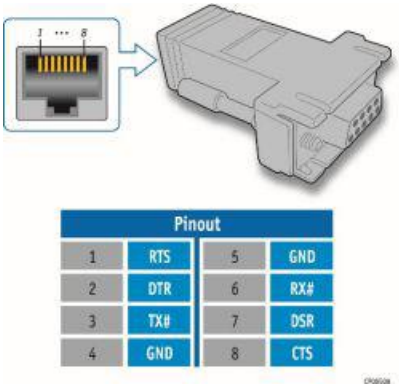
8.5.4. Accessoires

Numéro de pièce Kontron	Description
1066-0224	Sonde thermique
K00740-001	Support de montage pour le module de sauvegarde à batterie
1065-5409	Module TPM 2.0

8.6. Matériel, information et logiciels nécessaires

8.6.1. Matériel et information nécessaires

8.6.1.1. Adaptateur optionnel

Élément_1	Adaptateur série RJ45 vers DB9 (numéro de pièce Kontron : 1015-9404) 

8.6.1.2. Installation et assemblage des composants

Section pertinente :

Installation et assemblage des composants

Élément_1	Tournevis Phillips no 1 (cruciforme) (ou tournevis à embouts interchangeables avec embouts Phillips no 1 et no 2)
Élément_2	Tournevis Phillips no 2 (cruciforme) (ou tournevis à embouts interchangeables avec embouts Phillips no 1 et no 2)
Élément_3	Un tournevis Torx T30
Élément_4	Un tournevis à tête plate de 5 mm
Élément_5	Dispositif personnel de mise à la terre, tel qu'un bracelet antistatique et un tapis antistatique mis à la terre

8.6.1.3. Cordons d’alimentation et outils

Sections pertinentes :

Câblage

Installation dans une étagère

Élément_1	Fil noir toronné de calibre AWG no 12 pour fabriquer le cordon d'alimentation en fonction de la longueur requise
Élément_2	Fil rouge toronné de calibre AWG no 12 pour fabriquer le cordon d'alimentation en fonction de la longueur requise
Élément_3	Un connecteur homologue Positronic pour l’entrée du bloc d'alimentation CC (comprend un assemblage de décharge de traction)
Élément_4	Trois cosses à sertir de calibre 16 Positronic
Élément_5	Deux vis de décharge de traction
Élément_6	Une plaque de décharge de traction
Élément_7	Deux vis Phillips à tête plate
Élément_8	Une pince à sertir manuelle, DMC AF8

Élément_9	Un outil d'extraction manuelle
Élément_10	Un câble de mise à la terre de calibre AWG nº 8 en fonction de la longueur requise
Élément_11	Une cosse de mise à la terre à angle droit, calibre AWG nº 8 (numéro de pièce Kontron 1064-4226)
Élément_12	Clé de 10 mm ou outil équivalent
Élément_13	Une pince à sertir manuelle, Panduit CT-1700

8.6.1.4. Matériel d'installation dans l'étagère

Section pertinente :

Installation dans une étagère

Élément_1	Ensemble de rails (en fonction des exigences d'installation)

8.6.1.5. Câbles et modules réseau

Élément_1	Un câble Ethernet RJ45 pour le plan de gestion
Élément_2	Deux câbles Ethernet RJ45 pour le plan des données
Élément_3	Un câble de connexion série RJ45

8.6.1.6. Infrastructure réseau

Adresses IP :

- Une adresse IP pour le plan de gestion
- Jusqu'à 2 adresses IP pour le plan des données

8.6.2. Logiciels nécessaires

Élément_1	Une version de la communauté d'**ipmitool** est installée sur un ordinateur distant pour permettre la surveillance à distance – il est recommandé d'utiliser la version 1.8.18 d'ipmitool.
Élément_2	Un émulateur de terminal tel que **puTTY** est installé sur un ordinateur distant.
Élément_3	Un outil de détection des périphériques tel que **pciutils** est installé sur le serveur local pour visualiser des informations sur les périphériques connectés aux bus PCI du serveur.

8.7. Liste de compatibilité matérielle

8.7.1. CPU

Fournisseur	Description	Cœurs	Fréquence	Puissance	État	Numéro de pièce Kontron
Intel	Xeon® Silver 4114T, Skylake	10	2,2 GHz	85 W	Actif	1061-9790
Intel	Xeon® Gold 5218T, Cascade Lake	16	2,1 GHz	105 W	Actif	1065-4808
Intel	Xeon® Gold 6230T, Cascade Lake	20	2,1 GHz	125 W	Actif	1065-5295
Intel	Xeon® Silver 4209T, Cascade Lake	8	2,2 GHz	70 W	Actif	1066-7572

Le CG2400 offre des performances optimales lorsqu'un CPU avec une consommation maximale de 125 W par socket est utilisé.

NOTES :

- Les processeurs Silver 4114T et Gold 5218T font partie de la famille de produits « Embedded » d'Intel et figurent sur la feuille de route à long terme. Ils sont recommandés avec le CG2400 pour des performances optimales et une disponibilité et un support de longue durée. Ces deux CPU ont été testés avec succès selon les normes de température de fonctionnement NEBS.
- Les processeurs capables de tirer une puissance supérieure à 105 W conviennent aux applications qui ne nécessitent pas spécifiquement un soutien de longue durée ou une conformité aux exigences strictes NEBS (température de fonctionnement).
- Tous les processeurs décrits ci-dessus nécessitent une solution de dissipation thermique passive. Deux dissipateurs thermiques sont inclus dans le système de base, il n'est pas nécessaire de les commander séparément. Le dissipateur thermique du CPU1 et celui du CPU2 sont différents (le nombre d'ailettes diffère) afin d'optimiser la circulation de l'air dans le système. Il est important de respecter la séquence d'installation.

AVERTISSEMENT :

Des configurations particulières pourraient être viables avec des CPU consommant plus de 125 W (par exemple 150 W, 165 W), si le système est configuré et exploité dans des conditions définies telles que :

- Configuration à un seul CPU
- Environnement/conditions étroitement contrôlés (ex. température ambiante maximale = 20 °C)
- Déflecteurs d'air sur mesure dans le système

Les conséquences possibles de l'utilisation d'un CPU à très haute puissance dans des conditions non adaptées sont les suivantes :

- Grave dégradation de la performance de l'application causée par un étranglement fréquent du processeur
- Haut niveau acoustique
- Réduction de la durée moyenne de fonctionnement avant défaillance (MTBF)

Veuillez contacter votre représentant Kontron si vous souhaitez utiliser un CPU consommant plus de 125 W (c.-à-d. 140 W, 150 W ou 165 W). La plateforme CG2400 ne prend pas en charge les CPU de 200 W et de 205 W (qu'il s'agisse d'une configuration à un ou deux CPU).

8.7.2. Module de mémoire RDIMM ECC

Fournisseur	Numéro de pièce du fournisseur	Type	Taille	État	Numéro de pièce Kontron
Samsung	M393A2K40CB2-CVF	DDR4-2933	16 Go	Actif	1065-6019
Micron	MTA18ASF2G72PDZ-2G9E1	DDR4-2933	16 Go	Actif	
Micron	MTA36ASF8G72PZ-2G9B2	DDR4-2933	64 Go*	Actif	1066-9555
Samsung	M393A8G40MB2-CVF	DDR4-2933	64 Go*	Actif	
Samsung	M393A1K43DB1	DDR4-2933	8 Go	Actif	1069-5684
Micron	MTA9ASF1G72PZ-3G2R1	DDR4-2933	8 Go	Actif	

* Prise en charge uniquement avec les CPU Cascade Lake

8.7.3. Disque SSD M.2 (SATA ou NVMe)

Fournisseur	Numéro de pièce du fournisseur	Type	Taille	Dimension	Écritures complètes de disque par jour (DWPD)	État	Numéro de pièce Kontron
Intel	SSDSCKKB240G801	SATA	240 Go	2280	1,9	Actif	1065-5634
Intel	SSDSCKKB480G801	SATA	480 Go	2280	1,3	Actif	1065-5635
Intel	SSDPEKKA256G801	NVMe	256 Go	2280		Actif**	1065-5636
Intel	SSDPEKKA512G801	NVMe	512 Go	2280		Actif**	1065-5632
Transcend	TS128GMTE652TI	NVMe	128 Go	2280		Actif	1068-6586

** Le module se comporte et fonctionne de manière adéquate à toutes les températures de la plage spécifiée pour le système, mais la température interne renvoyée par le module lui-même est inexacte.

8.7.4. Disque SSD de 2.5 po (SATA)

Fournisseur	Numéro de pièce du fournisseur	Écritures complètes de disque par jour (DWPD)	Taille	Température de fonctionnement	État	Numéro de pièce Kontron
Samsung	MZ7LH240HAHQ-00005	1,3 (3 ans)	240 Go	0 °C à 70 °C	Actif	1066-7175
Samsung	MZ7KH240HAHQ-00005	3 (5 ans)	240 Go	0 °C à 70 °C	Actif	1065-6022

8.7.5. Disque dur de 2,5 po (SAS)

Fournisseur	Numéro de pièce du fournisseur	Formatage rapide	Taille	Tours par minute	12 Gbps SAS	Température de fonctionnement	État	Numéro de pièce Kontron
Seagate	ST300MM0048	512n	300 Go	10k	Oui	5 °C à 55 °C	Actif	1061-6231
Toshiba	AL14SEB030N	512n	300 Go	10k	Oui	5 °C à 55 °C	Actif	
Toshiba	AL15SEB030N	512n	300 Go	10k	Oui	5 °C à 55 °C	Actif	
Toshiba	AL14SEB060N	512n	600 Go	10k	Oui	5 °C à 55 °C	Actif	1061-6070
Toshiba	AL15SEB060N	512n	600 Go	10k	Oui	5 °C à 55 °C	Actif	
Seagate	ST600MM0009	512n	600 Go	10k	Oui	5 °C à 55 °C	Actif	
Seagate	ST1800MM0129	512e/4Kn	1,8 To	10k	Oui	5 °C à 55 °C	Actif	1061-7429
Toshiba	AL15SEB18EP	512e/4Kn	1,8 To	10k	Oui	5 °C à 55 °C	Non testé	
Toshiba	AL15SEB24EQ	512e	2,4 To	10k	Oui	5 °C à 55 °C	Non testé	1062-4999

8.7.6. Cartes PCIe SAS et RAID

Fournisseur	Description	Type	État	Numéro de pièce Kontron
LSI/Broadcom	MegaRAID SAS 9361-8i	RAID/SAS	Actif	1069-5357
LSI/Broadcom	CacheVault LSICVM02	Mémoire cache sécurisée	Actif	1069-5358
LSI/Broadcom	SAS 9300-8i Host Bus Adapter	SAS	Actif	1065-7730

8.7.7. Cartes d'interface réseau PCIe

Fournisseur	Description	Type	État	Numéro de pièce Kontron
Intel	4-port Gigabit Ethernet, RJ-45 (copper) NIC card	Interface réseau (10/100/1000 Mbps)	Actif	1059-8279

8.8. Systèmes d'exploitation validés

8.8.1. Description des états

Légende des états	Description
CERTIFIÉ	Le produit est certifié par le fournisseur du système d'exploitation comme matériel conforme.
VALIDÉ	Le produit a été testé à l'interne.
CERT TESTÉE	L'unité a passé les tests de certification, mais le certificat officiel du fournisseur de système d'exploitation n'a pas été publié.
PRÉVUE	La certification est prévue.
EN COURS	La certification est en cours.

8.8.2. État de la certification selon le système d'exploitation

Système d'exploitation	CG2400
Windows Server 2016	CERTIFIÉ
Windows Server 2019	CERTIFIÉ
SUSE SLES 15 (Suse Entreprise)	PRÉVUE
Ubuntu 18.04	VALIDÉ
Ubuntu 16.04	VALIDÉ
RHEL 8.2 - 8.x	CERTIFIÉ
RHEL 7.8 - 7.x	CERTIFIÉ
VMware ESXi 6.7	VALIDÉ
CentOS 7.6 (inclus avec RHEL)	VALIDÉ

8.9. Sécurité

- Établir un plan pour changer les noms d'utilisateur et les mots de passe par défaut. Voir Configuration et gestion des utilisateurs.
- Déterminer les chemins d'accès qui doivent être fermés ou ouverts. Voir Configuration des méthodes d'accès au système.
- La plateforme inclut un module de plateforme sécurisée (TPM). Déterminer vos exigences en matière de fonctions matérielles associées à la sécurité. Voir Configurer le TPM.

Pour plus d'informations sur les caractéristiques de sécurité, contacter Kontron.

9/ Installation

9.1. Installation mécanique et précautions

9.1.1. Protections contre les décharges électrostatiques

Les décharges électrostatiques (ESD) peuvent endommager les composants électroniques (ex. disques et cartes).

Rechercher cet avertissement dans la documentation. Il indique que le dispositif est sensible aux décharges électrostatiques et que des précautions doivent être prises.

Appareil sensible aux ESD!

Cet équipement est sensible à l'électricité statique. Des précautions doivent donc être prises lors de toutes les opérations de manipulation et d'inspection de ce produit afin d'en garantir l'intégrité à tout moment.

Nous vous recommandons d'effectuer toutes les procédures d'installation décrites dans la documentation sur un poste de travail ESD. Si cela n'est pas possible, utiliser des mesures de protection contre les décharges électrostatiques telles que les suivantes :

- Porter un bracelet antistatique relié à la terre (toute surface métallique non peinte) sur l'équipement lors de la manipulation des composants.
- Toucher le châssis métallique avant de toucher un composant électronique (ex. un module DIMM ou une carte).
- Maintenir une partie de votre corps (ex. une main) en contact avec le châssis métallique pour dissiper la charge statique lors de la manipulation du composant électronique.
- Éviter de vous déplacer inutilement.
- Utiliser un bracelet antistatique attaché au panneau avant (avec le panneau frontal retiré).
- Lire et suivre les précautions de sécurité fournies par le fabricant pour un composant spécifique.

9.1.2. Déballage

Lors de la manipulation des composants, suivre les précautions décrites dans la section Protections contre les décharges électrostatiques.

9.1.2.1. Contenu de la boîte

La boîte de la plateforme CG2400 comprend :

- Un serveur pour étagère 2U haute disponibilité CG2400 de 20 pouces de profondeur
- Deux boîtes de dissipateurs thermiques, l'une étiquetée « Avant » (Front) et l'autre « Arrière » (Rear).

9.1.2.2. Étapes de déballage

Étape_1	Ouvrir la boîte de la plateforme et retirer les petites boîtes de dissipateurs thermiques (il y en aura une ou deux selon la commande). Mettre les boîtes de côté jusqu'au moment d'installer les processeurs et les dissipateurs thermiques dans la plateforme. Voir Installation et assemblage des composants pour les instructions d'assemblage. **NOTE :** • Le processeur avec le dissipateur thermique « Avant » (Front) doit être installé sur le socket CPU1. • Le processeur avec le dissipateur thermique « Arrière » (Rear) doit être installé sur le socket CPU2.

Étape_2	Retirer soigneusement la plateforme de la boîte et enlever les deux morceaux de mousse.
Étape_3	Retirer la plateforme du sac ESD.
Étape_4	Retirer la pellicule plastique installée sur la plateforme. Si la pellicule n'est pas retirée, l'efficacité de la circulation de l'air dans la plateforme risque d'être affectée, ce qui se traduirait par une mauvaise capacité de refroidissement.
Étape_5	Remettre tous les éléments d'emballage dans la boîte (deux sachets déshydratants, un sac ESD, deux morceaux de mousse).

9.1.3. Installation et assemblage des composants

Appareil sensible aux ESD!

Cet équipement est sensible à l'électricité statique. Des précautions doivent donc être prises lors de toutes les opérations de manipulation et d'inspection de ce produit afin d'en garantir l'intégrité à tout moment.

Débrancher le ou les cordons d'alimentation avant toute intervention sur le produit afin d'éviter tout risque de choc électrique. Si le produit est équipé de plusieurs cordons d'alimentation, débrancher tous les cordons.

Lors de la manipulation des composants, suivre les précautions décrites dans la section Protections contre les décharges électrostatiques.

⚠WARNING

Les sections suivantes présentent les procédures générales de retrait qui sont nécessaires avant de retirer ou d'installer divers composants internes qui ne sont pas nécessairement remplaçables à chaud.

Avant de manipuler le serveur, il convient d'observer attentivement les consignes de sécurité figurant dans le présent guide.

Toutes les références à la gauche, la droite, l'avant, l'arrière, le haut et le bas supposent que la personne fait face à l'avant du serveur, tel qu'il est positionné pour un fonctionnement normal.

9.1.3.1. Outils et matériel nécessaires

Pour une liste des outils et du matériel nécessaires à l'installation et à l'assemblage des composants, voir Matériel, information et logiciels nécessaires.

9.1.3.2. Pièces et composants compatibles

Pour la liste complète des pièces et composants compatibles pouvant être commandés auprès de Kontron, voir Plateforme, modules et accessoires.

9.1.3.3. Gestion des câbles

Lorsque des composants sont ajoutés, enlevés ou remplacés dans la plateforme, il est important de porter une attention particulière à la gestion des câbles avant de procéder. Les composants de la plateforme sont très serrés dans le châssis et le rebranchement des câbles pourrait être plus complexe que prévu.

Suivre ces conseils pour réduire les difficultés liées à la gestion des câbles :

- Prendre des photos avant de déplacer, d'enlever ou de débrancher des composants.
- Tous les câbles doivent s'insérer parfaitement dans le châssis sans qu'il soit nécessaire de forcer ou de pincer.
- La gestion des câbles ne doit pas nuire à la ventilation adéquate dans la plateforme.
- Les câbles conservent leurs plis et leur orientation une fois déconnectés. Porter attention à ces détails facilitera le rebranchement et la gestion des câbles.

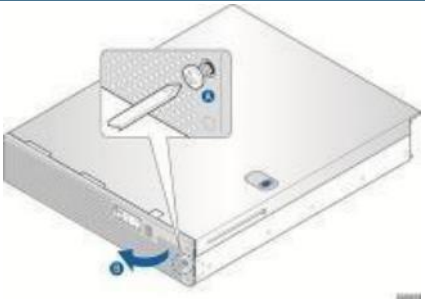
9.1.3.4. Panneau frontal

9.1.3.4.1. Enlever le panneau frontal

Le panneau frontal doit être enlevé pour effectuer des tâches telles que les suivantes :

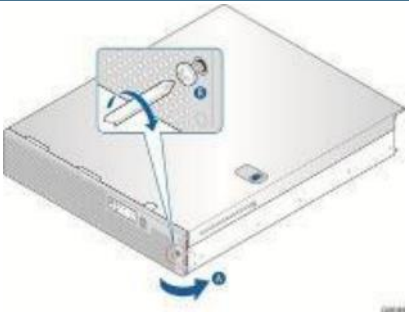
- Installer ou enlever une carte flash SD ou des disques durs remplaçables à chaud.
- Observer les indicateurs d'activité/défaillance des disques durs individuels
- Remplacer le panneau de contrôle des DEL et interrupteurs

NOTE : Il n'est pas nécessaire de mettre le système hors tension simplement pour retirer le panneau frontal.

Étape_1	Desserrer la vis de retenue imperdable du panneau frontal sur le côté droit du panneau frontal (A).	
Étape_2	Faire pivoter le panneau frontal vers la gauche pour le dégager des chevilles du panneau avant (B) et l'enlever.	

9.1.3.4.2. Réinstaller le panneau frontal

NOTE : Il n'est pas nécessaire de mettre le système hors tension simplement pour réinstaller le panneau frontal.

Étape_1	Insérer les languettes du côté gauche du panneau frontal dans les fentes du panneau avant du châssis.	
Étape_2	Déplacer le panneau frontal vers la droite et l'aligner sur les chevilles du panneau avant (A).	
Étape_3	Pousser le panneau frontal en place et serrer la vis de retenue pour le fixer (B).	

9.1.3.5. Capot supérieur du châssis

La consommation électrique en mode veille est active à l'intérieur du châssis lorsque le(s) bloc(s) d'alimentation sont raccordés à une source d'alimentation. Avant de retirer le capot supérieur, toujours mettre le serveur hors tension et débrancher tous les périphériques ainsi que le ou les cordons d'alimentation.

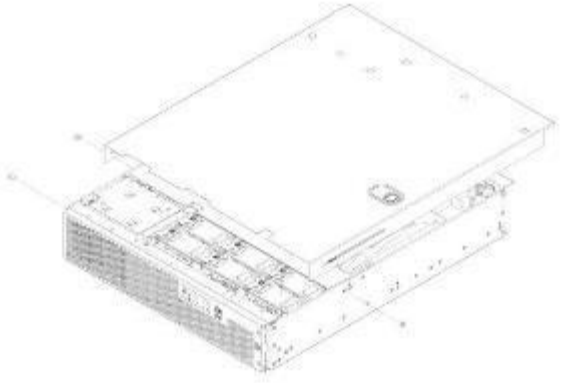
NOTICE

Le CG2400 doit être utilisé avec le capot supérieur en place pour assurer un refroidissement adéquat.

NOTICE

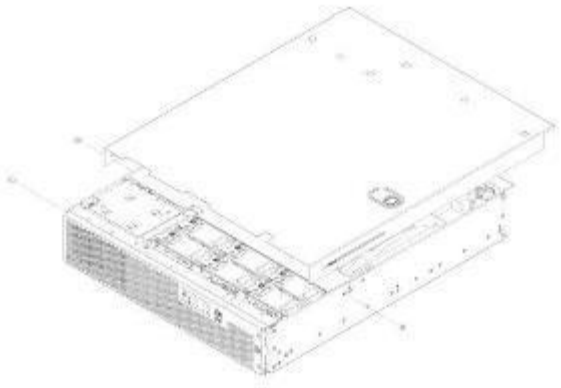
Une surface antidérapante ou une butée derrière le serveur peut être nécessaire pour éviter qu'il ne glisse sur la surface de travail.

9.1.3.5.1. Enlever le capot supérieur du châssis

Étape_1	Retirer la vis d'expédition Phillips à tête hexagonale 6-32 située à l'avant gauche du capot, si elle est encore fixée, et la garder pour une utilisation ultérieure.	
Étape_2	Retirer les deux vis à épaulement (une de chaque côté) du capot.	
Étape_3	Tout en maintenant le bouton bleu de déverrouillage au milieu du capot supérieur, faire glisser le capot vers l'arrière jusqu'à ce qu'il s'arrête et que le bord dégage le support de verrouillage sur le panneau arrière du châssis.	
Étape_4	Soulever le capot vers le haut pour le retirer du châssis.	

9.1.3.5.2. Réinstaller le capot supérieur du châssis

Étape_1	En commençant par l'arrière du châssis, aligner la languette sur le bord arrière droit du couvercle avec le support de verrouillage sur l'extérieur du panneau arrière et déposer le capot sur le châssis avec les bords latéraux à l'extérieur des parois du châssis.	
Étape_2	Faire glisser le capot vers l'avant jusqu'à ce qu'il s'enclenche.	
Étape_3	Installer la vis d'expédition si l'entrée outillée est nécessaire ou si la plateforme doit être expédiée.	
Étape_4	Remettre les deux vis à épaulement en place (une de chaque côté) pour fixer le capot au cadre du châssis. Serrer les vis (couple de 8 lb-po).	

Étape_5	Rebrancher tous les périphériques et le(s) cordon(s) d'alimentation. **ATTENTION :** Le capot doit être installé lorsque la plateforme est en marche afin d'assurer un refroidissement adéquat.	

9.1.3.6. Disques

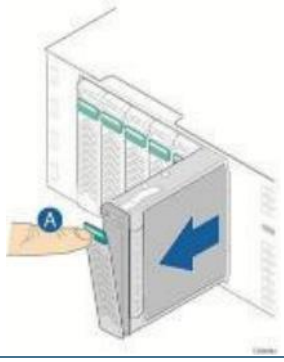
Avant de pouvoir enlever ou installer un disque, il faut enlever (puis réinstaller) :

- Le Panneau avant de la plateforme

NOTICE

Si moins de 6 disques sont installés, pour assurer un refroidissement adéquat, les emplacements de disques inutilisés doivent contenir des supports vides munis de panneaux de remplissage livrés avec la plateforme.

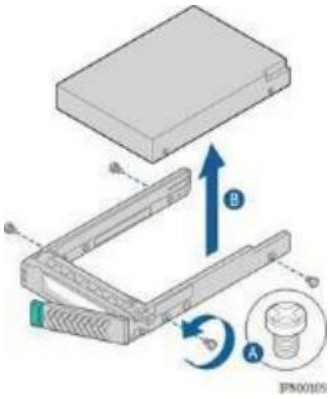
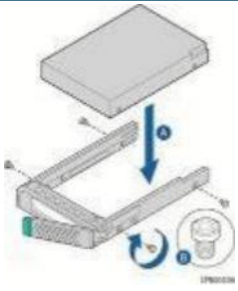
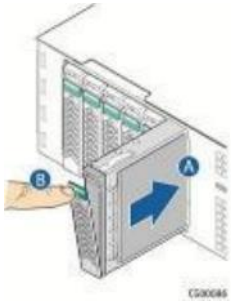
9.1.3.6.1. Enlever un support de disque du châssis

Étape_1	Une fois le panneau frontal enlevé, choisir l'emplacement de disque où un disque sera installé ou remplacé. **NOTE :** L'emplacement de disque 0 doit être utilisé en premier, puis l'emplacement de disque 1, et ainsi de suite. Les numéros d'emplacement sont inscrits sur le panneau avant, sous les emplacements de disque.	
Étape_2	Retirer le support de disque en appuyant sur le bouton vert pour ouvrir le levier qui enclenche le disque sur le fond de panier (A).	
Étape_3	Retirer le support de disque du châssis.	

9.1.3.6.2. Installer un disque dans un support

NOTICE

Les disques doivent être installés dans la bonne orientation dans le support. Ne pas respecter l'orientation risque d'endommager l'équipement.

Étape_1	Si le support de disque est vide (première installation), retirer le panneau de remplissage en plastique noir en dévissant les quatre vis qui le fixent au support (A). Mettre les vis de côté pour les utiliser avec le nouveau disque. OU Si un disque est déjà installé (remplacement de disque), le retirer en dévissant les quatre vis qui le fixent au support (A). Mettre les vis de côté pour les utiliser avec le nouveau disque.	
Étape_2	Soulever le disque (ou le panneau de remplissage) pour le sortir du support (B).	
Étape_3	Installer le nouveau disque dans le support de disque (A) et fixer le disque avec les quatre vis (couple de 4 lb-po maximum) (B). NOTE : S'assurer que l'orientation du disque est bonne. Le connecteur SATA doit être exposé à l'arrière du support. Lorsque le support est dans la position illustrée sur la figure, le connecteur SATA situé à l'arrière du disque ne doit pas être visible. Il doit être en contact avec la surface de travail.	
Étape_4	Avec le levier de verrouillage du support de disque complètement ouvert, pousser le support de disque dans l'emplacement de disque du châssis jusqu'à ce qu'il ne soit plus possible d'aller plus loin (A).	
Étape_5	Appuyer sur le levier de verrouillage jusqu'à ce qu'il s'enclenche et fixe le disque dans l'emplacement (B).	

9.1.3.7. Ventilateurs du système

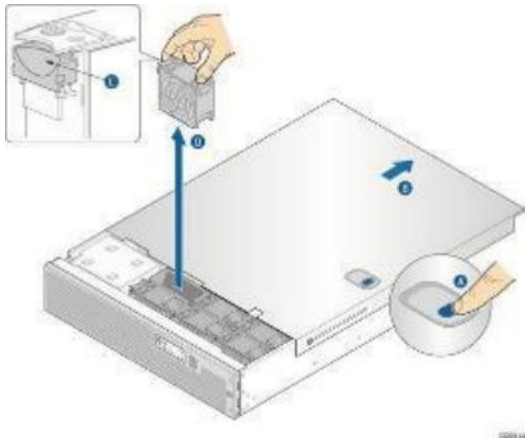
Les ventilateurs sont remplaçables à chaud.

⚠CAUTION

Puisque les ventilateurs sont remplaçables à chaud, il n'est pas nécessaire d'arrêter le serveur et de débrancher l'alimentation et les périphériques externes. Au lieu de retirer le capot du châssis, comme il est d'usage pour travailler sur les composants internes, il suffit d'appuyer sur le bouton bleu de déverrouillage du capot et de faire glisser le capot vers l'arrière sur les vis à épaulement pour accéder à la zone des ventilateurs.

Ne pas retirer complètement le capot supérieur lorsque le système est en marche, car il y a un risque associé à une tension de 12 V dans le serveur lorsqu'il est sous tension. Si le capot supérieur a été enlevé pour accéder à des composants internes du système autres que les ventilateurs remplaçables à chaud, vous devez éteindre le serveur et débrancher les cordons d'alimentation.

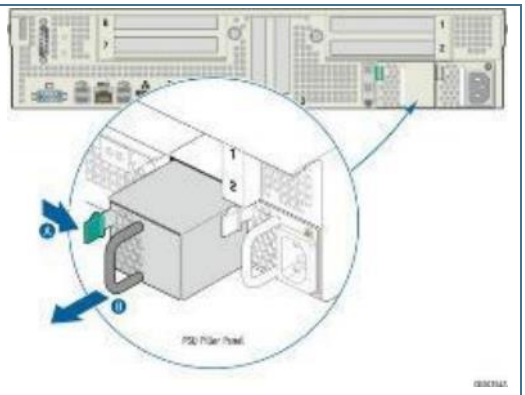
9.1.3.7.1. Remplacer un ventilateur

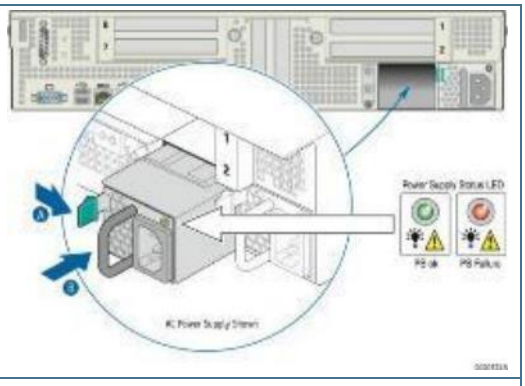
Étape_1	Retirer la vis d'expédition, si elle est utilisée, sur le côté gauche du capot du châssis.	
Étape_2	Tout en maintenant le bouton bleu de déverrouillage (A) au milieu du capot supérieur, faire glisser le capot vers l'arrière (B). Les deux vis à épaulement empêchent le capot de glisser trop loin.	
Étape_3	Déterminer le ventilateur qui a subi une défaillance en trouvant la DEL ambre. (La DEL se trouve à côté de l'œillet bleu sur le dessus de chaque ventilateur.)	
Étape_4	Retirer le ventilateur défaillant en saisissant les deux côtés de l'assemblage du ventilateur, en utilisant le protège-doigts en plastique sur le côté gauche et en tirant le ventilateur hors du boîtier métallique (C et D).	
Étape_5	Remplacer le ventilateur en insérant un nouveau ventilateur dans le même emplacement. Utiliser les bords du boîtier métallique pour aligner correctement le ventilateur et pour veiller à ce que le connecteur d'alimentation soit correctement uni avec l'embase située sur le côté gauche du boîtier métallique.	
Étape_6	S'il s'agit de la dernière manipulation à effectuer, fermer le capot du châssis en le faisant glisser vers l'avant jusqu'à ce qu'il s'enclenche. Remettre la vis d'expédition en place, si elle est utilisée.	

9.1.3.8. Bloc d'alimentation

La plateforme peut fonctionner avec des blocs d'alimentation CA ou CC. Un deuxième bloc d'alimentation peut être ajouté pour assurer la redondance. Les blocs d'alimentation sont remplaçables à chaud. Aucun composant du châssis n'a à être enlevé pour ajouter ou remplacer un bloc d'alimentation. Si le bloc d'alimentation principal est celui à remplacer et qu'il y a un bloc d'alimentation redondant dans le système, l'alimentation basculera sur l'unité redondante pendant le remplacement du bloc principal.

9.1.3.8.1. Insérer ou remplacer un bloc d'alimentation

Étape_1	Deux scénarios sont possibles : <u>Ajouter un bloc d'alimentation</u> Retirer le panneau de remplissage en appuyant sur le mécanisme de verrouillage de sécurité vert et en le maintenant vers le bas (A) et en utilisant la poignée pour tirer le panneau de remplissage hors de l'emplacement (B). **OU** <u>Remplacer un bloc d'alimentation</u> Pour remplacer un bloc d'alimentation (vérifier la DEL d'état du bloc d'alimentation pour confirmer celui qui est défaillant), débrancher le cordon d'alimentation du bloc d'alimentation à remplacer. Retirer le bloc d'alimentation défaillant en appuyant sur le mécanisme de verrouillage de sécurité vert et en le maintenant vers le bas (A) et en utilisant la poignée pour tirer le bloc d'alimentation défaillant hors de l'emplacement (B).	

Étape_2	Insérer le nouveau bloc d'alimentation en appuyant sur le mécanisme de verrouillage de sécurité vert et en le maintenant vers le bas (A) et en utilisant la poignée pour faire glisser le bloc d'alimentation dans l'emplacement jusqu'à ce qu'il s'enclenche (B).	
Étape_3	Brancher le cordon d'alimentation. La DEL du bloc d'alimentation doit être verte fixe.	

9.1.3.9. Cages d'extension PCIe

Avant de pouvoir enlever et réinstaller une cage d'extension PCIe, il faut enlever (puis réinstaller) :

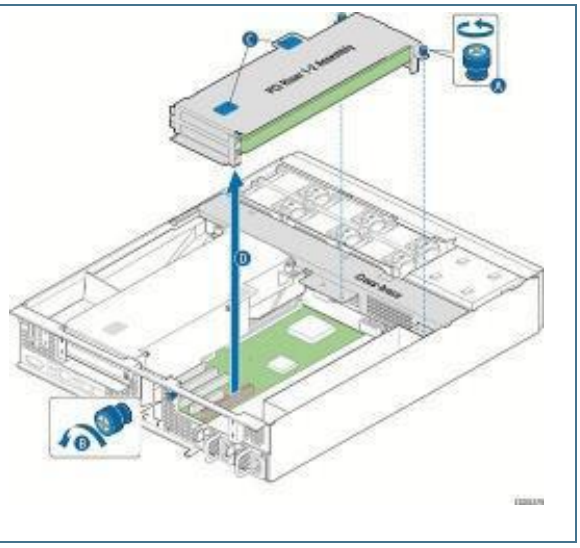
Le capot supérieur du chassis

Il faut enlever du châssis une cage d'extension PCIe ou les deux pour effectuer les tâches suivantes :

- Installer ou remplacer une carte adaptatrice de connexion PCIe ou une carte d'expansion PCIe
- Travailler avec les composants de la carte de la plateforme qui se trouvent à proximité d'une cage d'extension PCIe

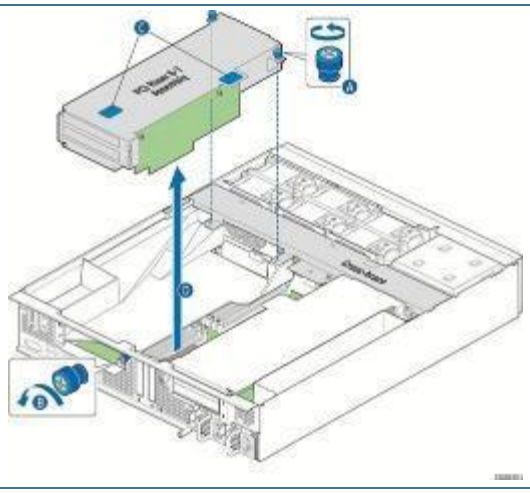
9.1.3.9.1. Enlever une cage d'extension PCIe

9.1.3.9.1.1. Enlever la cage d'extension PCIe de gauche

Étape_1	Desserrer les deux vis de retenue imperdables bleues (A) à l'avant de la cage d'extension PCIe et la vis imperdable bleue à l'arrière du châssis (B).	
Étape_2	En utilisant les deux points de contact bleus (C), soulever la cage d'extension hors du châssis (D).	

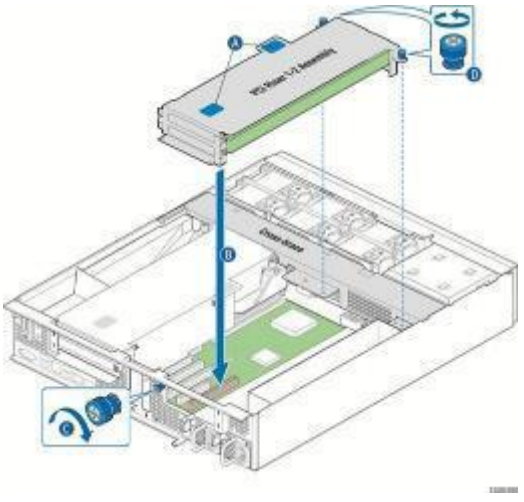
9.1.3.9.1.2. Enlever la cage d'extension PCIe de droite

Étape_1	Desserrer les deux vis de retenue imperdables bleues (A) à l'avant de la cage d'extension PCIe et la vis imperdable bleue à l'arrière du châssis (B).	

Étape_2	En utilisant les deux points de contact bleus (C), soulever la cage d'extension hors du châssis (D).	

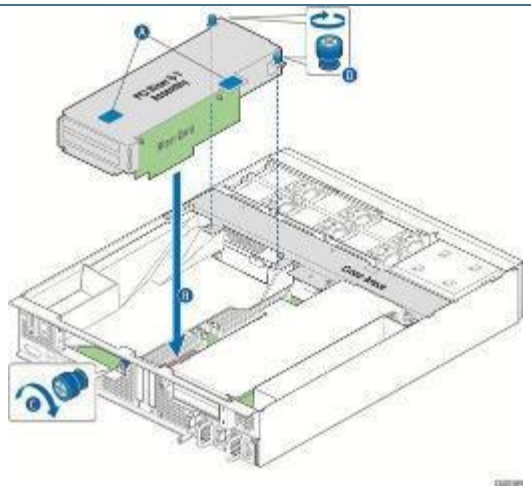
9.1.3.9.2. Réinstaller une cage d'extension PCIe

9.1.3.9.2.1. Réinstaller la cage d'extension PCIe de gauche

Étape_1	Positionner les languettes avant de la cage d'extension au-dessus des trous de la traverse.	
Étape_2	En utilisant les points de contact bleus sur le dessus de la cage (A), appuyer pour unir la carte adaptatrice de connexion au connecteur sur la carte de serveur (B, emplacement 2 pour la cage d'extension de gauche). **NOTES :** • Pour éviter d'endommager le bord de la carte, il faut s'assurer que la carte soit alignée directement avec le connecteur, et non de biais. • Si une carte contrôleur RAID matériel est installée dans l'emplacement PCIe 3, s'assurer de ne pas endommager les broches de diagnostic à l'arrière de la carte, près du panneau arrière du châssis, lors de la réinstallation de la cage d'extension PCIe de gauche.	
Étape_3	Aligner et serrer les vis de retenue imperdable bleues à l'avant de la cage avec les trous sur la traverse (D) et à l'arrière du châssis (C).	

9.1.3.9.2.2. Réinstaller la cage d'extension PCIe de droite

Étape_1	Positionner les languettes avant de la cage d'extension au-dessus des trous de la traverse (par-dessus le conduit d'air des processeurs).	
Étape_2	En utilisant les points de contact bleus sur le dessus de la cage (A), appuyer pour unir la carte adaptatrice de connexion au connecteur sur la carte de serveur (B, emplacement 6 pour la cage d'extension de droite). **NOTE :** Pour éviter d'endommager le bord de la carte, il faut s'assurer que la carte soit alignée directement avec le connecteur, et non de biais.	

Étape_3	Aligner et serrer les vis de retenue imperdable bleues à l'avant de la cage avec les trous sur la traverse (D) et à l'arrière du châssis (C).	

9.1.3.10. Conduit d'air des processeurs

Avant de pouvoir enlever et réinstaller le conduit d'air des processeurs, il faut enlever (puis réinstaller) :

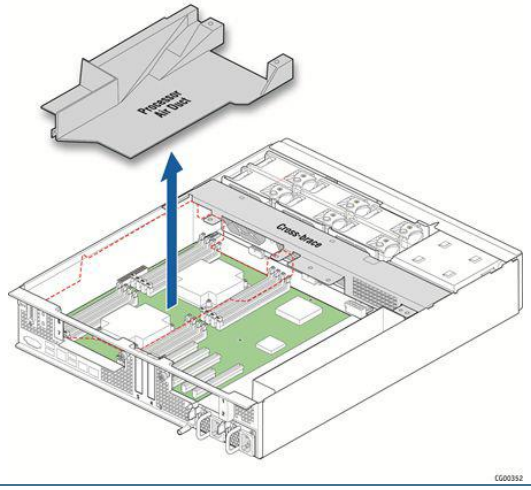
- Le capot supérieur du châssis
- Les cages d'extension PCIe

Le conduit d'air des processeurs en plastique noir doit être retiré pour accéder aux processeurs et aux modules de mémoire DIMM ou pour remplacer la carte de la plateforme.

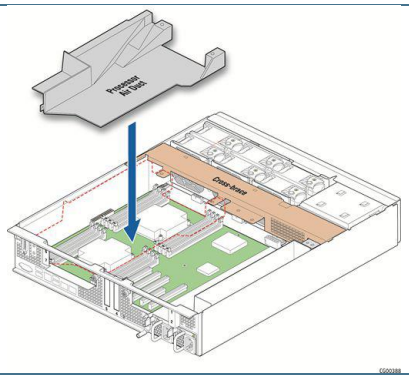
NOTICE

Le conduit d'air est nécessaire pour assurer une bonne circulation de l'air dans le châssis. Il est important de s'assurer qu'il est bien en place avant de réinstaller les cages d'extension PCIe et le capot du châssis.

9.1.3.10.1. Retirer le conduit d'air des processeurs

Étape_1	Pour retirer le conduit d'air des processeurs, il suffit de le soulever vers le haut hors du châssis.	

9.1.3.10.2. Remettre le conduit d'air des processeurs

Étape_1	Placer le conduit d'air des processeurs au-dessus des sockets des processeurs et des modules DIMM. Aligner les languettes avant avec les vis imperdables de la traverse. S'assurer que la goupille située à l'arrière du châssis est insérée dans la rainure moulée à l'arrière du conduit d'air des processeurs. Le conduit d'air est fixé lorsque la cage d'extension PCIe de droite est montée sur la traverse située au-dessus.	

9.1.3.11. Module de sauvegarde à batterie SuperCap

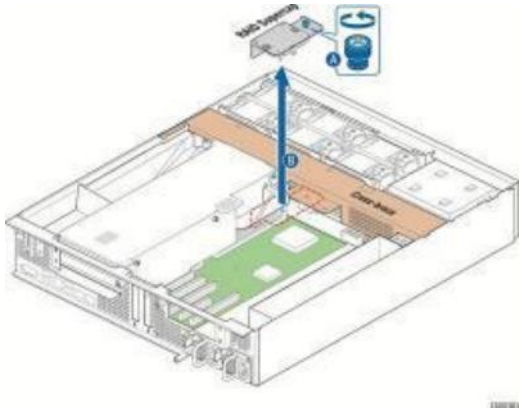
Le module optionnel de sauvegarde à batterie des configurations RAID et son support, s'ils sont installés, doivent être enlevés pour installer ou retirer des composants situés dans cette zone de la carte mère, tels qu'un module M.2. Puisque le module de sauvegarde à batterie SuperCap est fixé à la traverse, il doit être enlevé chaque fois que la traverse est enlevée.

Pour détacher et rattacher le module de sauvegarde à batterie SuperCap de la traverse, il n'est pas nécessaire de le déconnecter ou de le connecter au contrôleur RAID matériel. Pour plus d'informations sur le contrôleur RAID matériel, voir la section Installer un contrôleur RAID matériel.

Avant de pouvoir enlever et réinstaller le module de sauvegarde à batterie SuperCap, il faut enlever (puis réinstaller) :

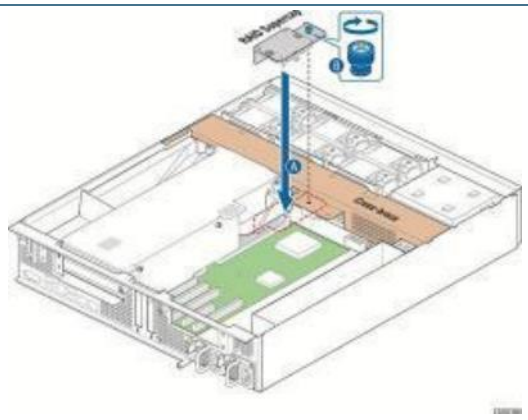
- Le capot supérieur du châssis
- La cage d'extension PCIe de gauche

9.1.3.11.1. Enlever le module de sauvegarde à batterie SuperCap

Étape_1	Desserrer la vis imperdable qui fixe le module de sauvegarde à batterie à la traverse (A).	
Étape_2	Soulever l'unité pour la sortir du châssis (B). **NOTE :** Il n'est pas nécessaire de déconnecter le module de sauvegarde à batterie SuperCap du contrôleur RAID matériel.	

9.1.3.11.2. Réinstaller le module de sauvegarde à batterie SuperCap

Étape_1	Positionner le module de sauvegarde à batterie SuperCap au-dessus de la traverse (A).	

Étape_2	Serrer la vis imperdable qui fixe le module de sauvegarde à batterie à la traverse (B).	

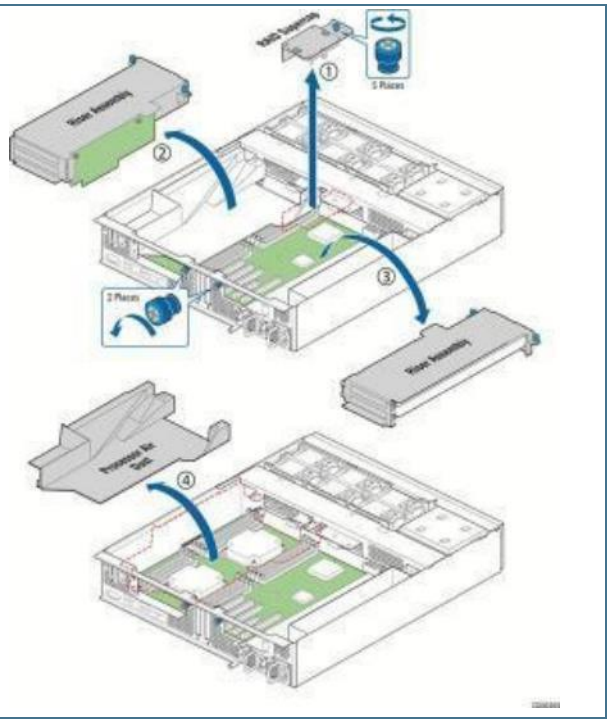
9.1.3.12. Traverse de soutien

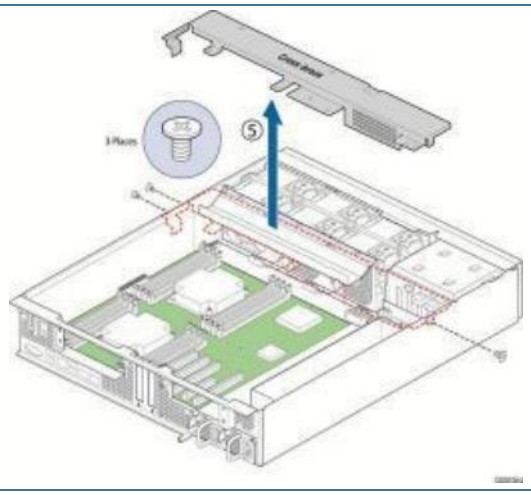
La traverse de soutien permet de fixer plusieurs composants, dont certains sont optionnels. Il s'agit de la séparation entre l'avant et l'arrière. Le capot supérieur peut être repoussé jusqu'à la traverse sans mettre le système hors tension afin d'assurer l'entretien les composants remplaçables à chaud situés à l'avant du châssis. En revanche, certains composants situés à l'avant du châssis, tels que la carte du panneau avant ou la carte de distribution électrique, ne peuvent être remplacés sans que la traverse (ainsi que tous les composants qui y sont attachés) ne soit d'abord retirée. Cette procédure est nécessaire afin de disposer de suffisamment d'espace pour accéder à ces composants avant du châssis.

Avant de pouvoir enlever et réinstaller la traverse, il faut enlever (puis réinstaller) :

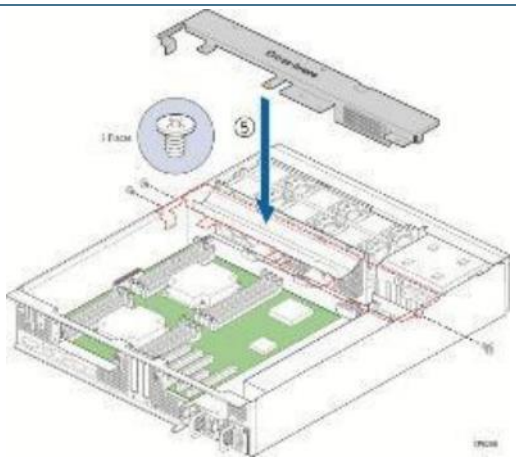
- Le capot supérieur du châssis
- Les cages d'extension PCIe
- Le conduit d'air des processeurs
- Le module de sauvegarde à batterie SuperCap

9.1.3.12.1. Enlever la traverse

Étape_1	S'assurer que tous les composants fixés par les vis de retenue imperdable sont retirés : • Cages d'extension PCIe • Conduit d'air des processeurs • Assemblage du module de sauvegarde à batterie pour le RAID matériel (optionnel)	

Étape_2	Retirer les trois petites vis à tête fraisée qui fixent la traverse aux côtés du châssis : • Une sur le côté gauche • Deux sur le côté droit	
Étape_3	Retirer la traverse du châssis.	

9.1.3.12.2. Réinstaller la traverse

Étape_1	Repositionner la traverse dans le châssis.	
Étape_2	Fixer la traverse avec les trois vis mises de côté : • Une sur le côté gauche • Deux sur le côté droit	

9.1.3.13. Carte de fond de panier (backplane) pour disques remplaçable à chaud (HSBP)

La carte HSBP doit être enlevée pour remplacer la carte HSBP ou la carte de distribution électrique (PDB).

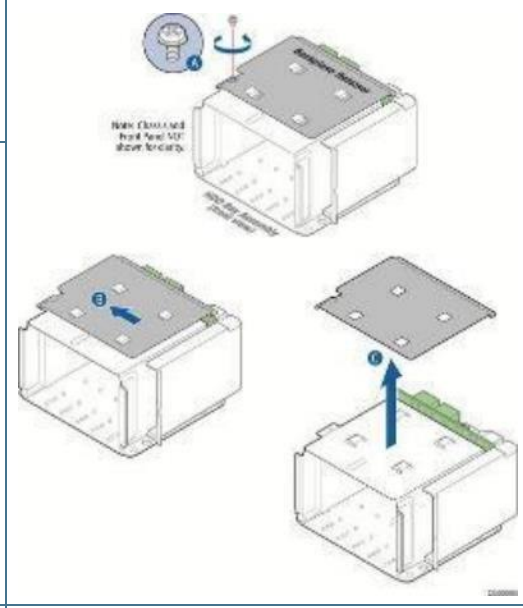
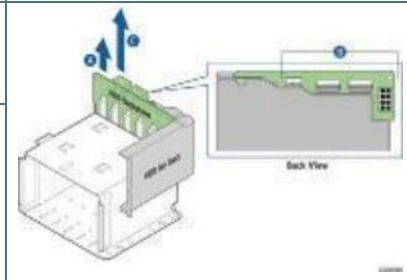
La carte HSBP à six emplacements est située à l'arrière de la cage des disques. Elle est maintenue en place par une plaque de recouvrement située sur le dessus de la cage des disques qui passe par-dessus le bord supérieur de la carte HSBP. Un conduit d'air en plastique noir entoure également la cage des disques sur le côté droit et à l'arrière de l'assemblage.

Avant de pouvoir enlever et réinstaller la carte HSBP, il faut enlever (puis réinstaller) :

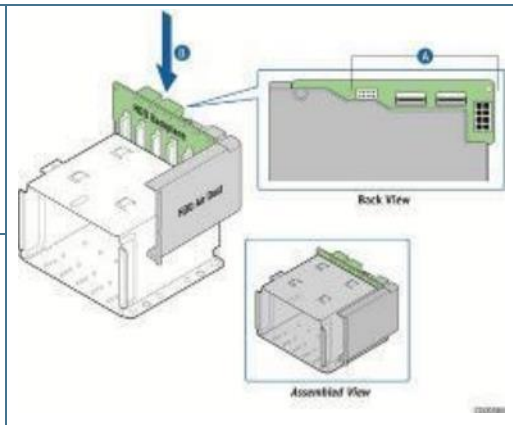
- Le capot supérieur du chassis
- Le panneau frontal

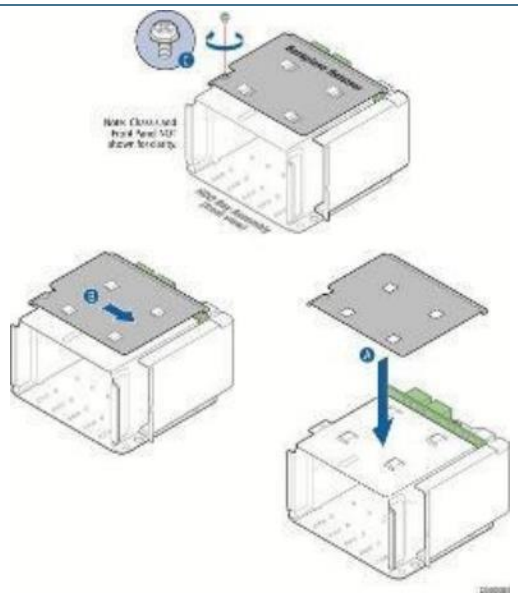
9.1.3.13.1. Enlever la carte HSBP

Étape_1	Faire glisser tous les disques hors des emplacements de la cage des disques pour les désengager du fond de panier.

Étape_2	Retirer la plaque de recouvrement de la cage des disques en desserrant la vis qui la fixe à la cage des disques (A) et en la faisant glisser vers la gauche en direction de la paroi du châssis pour la libérer les languettes (B).	
Étape_3	Soulever la plaque de recouvrement afin de la détacher de la cage des disques (C).	
Étape_4	Soulever la carte HSBP et le conduit d'air des disques pour accéder aux connecteurs situés à l'arrière de la carte (A).	
Étape_5	Débrancher les quatre câbles reliés à la carte HSBP (B) : • Un câble d'alimentation de la carte de fond de panier pour disques • Un câble SAS 1 • Un câble SAS 2 • Un câble de la carte HSBP pour le bus I2C et les DEL d'état des disques	
Étape_6	Soulever la carte de fond de panier et le conduit d'air pour les sortir du châssis (C).	

9.1.3.13.2. Réinstaller la carte HSBP

Étape_1	Rebrancher les quatre câbles reliés à la carte HSBP (A) : • Un câble d'alimentation de la carte de fond de panier pour disques Un câble SAS 1 • Un câble SAS 2 • Un câble de la carte HSBP pour le bus I2C et les DEL d'état des disques	
Étape_2	Réinstaller la carte de fond de panier et le conduit d'air (B).	
Étape_3	Fixer le fond de panier des disques à six emplacements en plaçant la plaque de recouvrement sur la cage des disques, le fond de panier et le conduit d'air (A et B).	

Étape_4	Revisser la vis qui maintient la plaque de recouvrement en place (C).	
Étape_5	Insérer tous les disques de manière à ce qu'ils s'enclenchent dans le fond de panier.	

9.1.3.14. Modules DIMM

Avant de pouvoir enlever ou installer un module DIMM, il faut enlever (puis réinstaller) :

- Le capot supérieur du châssis
- La cage d'extension PCIe de droite
- Le conduit d'air des processeurs

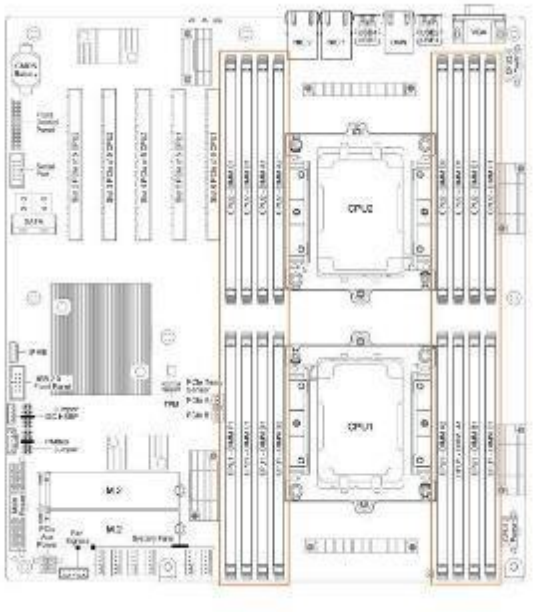
Pour réduire le risque de dommages causés par une décharge électrostatique (ESD) sur le processeur ou les modules DIMM, suivre les procédures suivantes :

- Toucher au châssis métallique avant de toucher le module DIMM ou la carte de serveur.
- Maintenir une partie de votre corps (ex. une main) en contact avec le châssis métallique pour dissiper la charge statique lors de la manipulation du module DIMM.
- Éviter de vous déplacer inutilement.
- Utiliser un bracelet antistatique attaché au panneau avant (avec le panneau frontal retiré).

Pour la liste des modules DIMM testés, voir Liste de compatibilité matérielle.

9.1.3.14.1. Emplacement des modules DIMM

Figure 21. Emplacement des modules DIMM



9.1.3.14.2. Directives d'installation des modules DIMM pour une performance optimale

Il y a 8 emplacements DIMM par CPU, mais seulement 6 canaux par CPU – A1 et A2 sont sur le même canal et D1 et D2 sont sur le même canal. Par conséquent, ne pas remplir les emplacements A2 et D2 à moins d'avoir rempli tous les autres emplacements DIMM.

Pour une performance optimale, les deux CPU devraient avoir la même configuration DIMM, en configuration CPU simple ou double.

Pour chaque CPU, installer les modules DIMM conformément aux directives suivantes pour une performance optimale.

- Pour les configurations avec 1 à 3 modules DIMM – remplir les emplacements A1, B1 et C1, en commençant par A1.
- Pour les configurations avec 4 modules DIMM – remplir les emplacements A1, B1, D1 et E1.
- Les configurations avec 5 modules DIMM ne sont pas recommandées, car elles sont déséquilibrées et produiront une performance moins optimale.
- Pour les configurations avec 6 modules DIMM – remplir les emplacements A1, B1, C1, D1, E1 et F1.
- Les configurations avec 7 modules DIMM ne sont pas recommandées, car elles sont déséquilibrées et produiront une performance moins optimale.
- Pour les configurations avec 8 modules DIMM – remplir tous les emplacements DIMM.

NOTICE

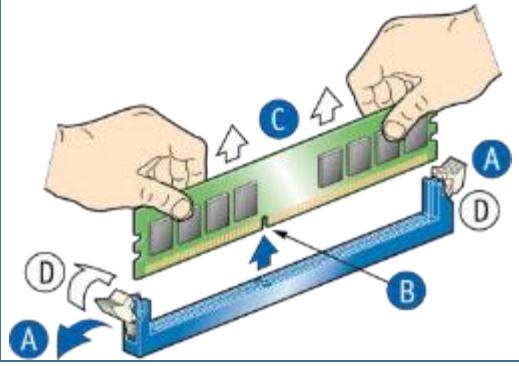
La configuration avec 8 modules DIMM par CPU réduira la vitesse des DIMM à 2933 MHz d'un cran par rapport à la valeur nominale, c'est-à-dire à 2666 MHz.

Si des mémoires à 2666 ou 2400 MHz (8 DIMM par CPU) sont utilisées, la vitesse négociée reste la vitesse nominale des modules DIMM, sauf si la vitesse maximale de la mémoire du CPU est inférieure à la vitesse nominale des modules DIMM.

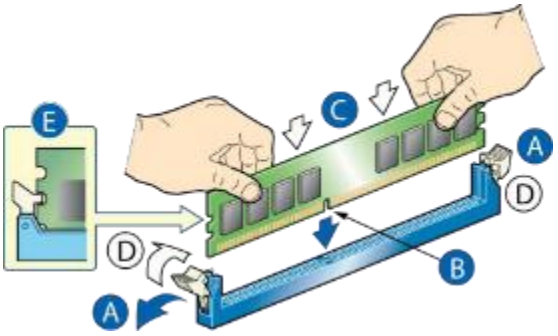
- Exemple 1. Le processeur Xeon Silver 4114T à 2400 MHz négocie des modules DIMM à 2666 MHz à 2400 MHz
- Exemple 2. Le processeur Xeon Gold 5218T à 2666 MHz négocie des modules DIMM à 2666 MHz à 2666 MHz

9.1.3.14.3. Enlever des modules DIMM

Étape_1	Ouvrir les onglets de l'emplacement DIMM pour le module DIMM à enlever (A).	

Étape_2	Avec les deux mains, tenir le module DIMM par les bords et le soulever de l'emplacement. Mettre le module DIMM dans un emballage antistatique.	

9.1.3.14.4. Installer des modules DIMM

Étape_1	Ouvrir les onglets de l'emplacement DIMM. (A)	
Étape_2	Noter l'emplacement de l'encoche d'orientation sur le bord du module DIMM. (B)	
Étape_3	Insérer le module DIMM, en veillant à ce que le bord connecteur du module DIMM s'aligne correctement dans l'emplacement. (E)	
Étape_4	Avec les deux mains, appuyer fermement et uniformément sur les deux côtés du module DIMM jusqu'à ce qu'il s'enclenche et que les onglets se ferment. (C et D)	
Étape_5	Inspecter visuellement chaque onglet pour s'assurer qu'ils sont complètement fermés et correctement enclenchés dans les encoches du bord du module DIMM. (E)	

9.1.3.15. Processeurs et les dissipateurs thermiques

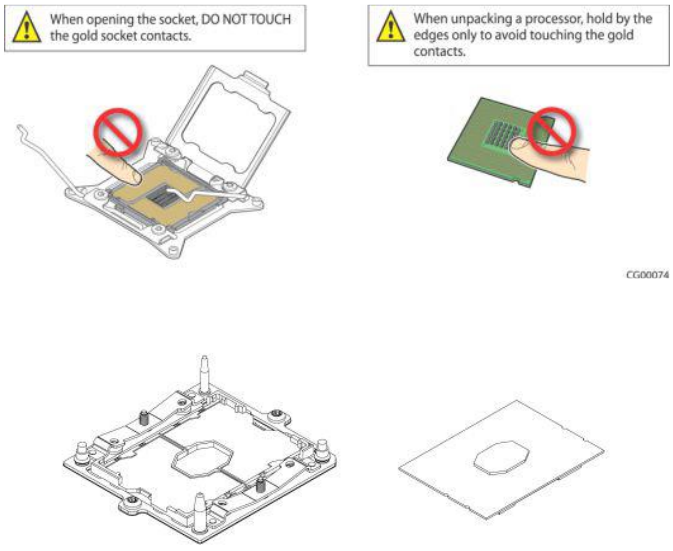
Avant de pouvoir enlever, ajouter ou remplacer un processeur ou un dissipateur thermique, il faut enlever (puis réinstaller) :

- Le capot supérieur du châssis
- La cage d'extension PCIe de droite
- Le conduit d'air des processeurs

9.1.3.15.1. Manipulation des sockets et processeurs et précautions contre les décharges électrostatiques

9.1.3.15.1.1. Précautions pour la manipulation

NOTICE

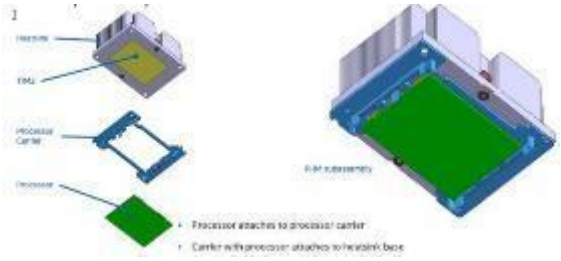


NOTICE

Les contacts des sockets sont fragiles et peuvent être facilement endommagés s'ils sont touchés. Intel a mis au point un sous-ensemble empilé pour assurer des mouvements uniformes et contrôlés lors de l'insertion et du retrait des processeurs des sockets. Kontron attend des utilisateurs et des intégrateurs de systèmes qu'ils utilisent la méthodologie conçue par Intel à tous les points des procédures de cette section où un processeur est retiré ou inséré dans un socket.

Le module dissipateur thermique et processeur (PHM) désigne le sous-ensemble où le dissipateur thermique et le processeur sont clipsés ensemble avant l'installation. Cela permet une installation plus robuste en offrant de meilleures caractéristiques d'alignement et en gardant les doigts à l'écart du champ de contact du socket.

Le sous-ensemble empilé se compose de trois parties.



Source de l'image : Intel Corporation

9.1.3.15.1.2. Précautions contre les décharges électrostatiques

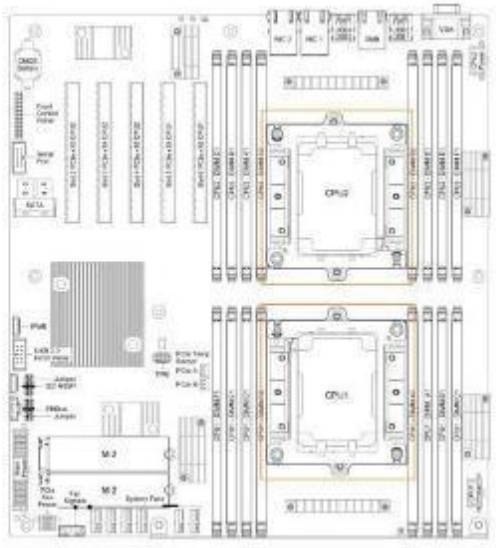
Porter une attention particulière aux points suivants lors de la manipulation des processeurs et des sockets afin de réduire le risque de dommages dus aux décharges électrostatiques (ESD) sur les processeurs :

- **Toucher au châssis métallique avant de toucher le processeur ou la carte de serveur.**

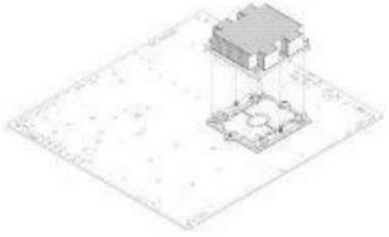
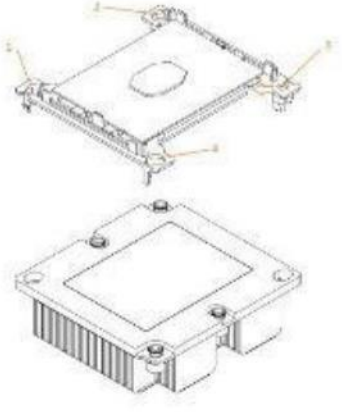
- **Maintenir une partie de votre corps (ex. une main) en contact avec le châssis métallique pour dissiper la charge statique lors de la manipulation du processeur.**
- **Éviter de vous déplacer inutilement.**
- **Utiliser un bracelet antistatique attaché au panneau avant (avec le panneau frontal retiré).**

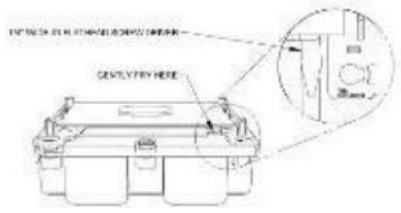
9.1.3.15.2. Emplacement des processeurs

Figure 22. Emplacement des processeurs



9.1.3.15.3. Désassembler le module dissipateur thermique et processeur (PHM)

Étape_1	Desserrer les quatre vis imperdables situées dans les coins du dissipateur thermique à l'aide d'un tournevis Torx T30. Desserrer les vis progressivement en suivant un motif en étoile (c.-à-d. coin 1 un demi-tour, coin 3 un demi-tour, coin 2 un demi-tour, coin 4 un demi-tour; puis revenir au coin 1 et recommencer). Retirer le PHM.	
Étape_2	Détacher le support de processeur (qui contient le processeur) du dissipateur thermique. Pour ce faire, utiliser vos doigts : 1. Déclipser légèrement le coin 1. 2. Déclipser légèrement le coin 3. 3. Déclipser légèrement le coin 2. 4. Déclipser légèrement le coin 4.	

Étape_3	Insérer un tournevis à tête plate no 1 de 1/4 po de largeur à l'endroit indiqué sur la figure (une gravure de tournevis se trouve sur le support de processeur à l'endroit approprié). Tourner légèrement le tournevis pour désengager le support de processeur du dissipateur thermique. **NOTE :** Pour protéger le processeur, placer le support de processeur sur la table dans l'orientation indiquée sur la figure, c'est-à-dire le support sur la table avec le processeur au-dessus.	
Étape_4	En utilisant votre pouce, tirer sur la languette et faire basculer le processeur pour le dégager de son support. Mettre le processeur dans un emballage antistatique.	

9.1.3.15.4. Ajouter ou remplacer un processeur dans un PHM

NOTICE

Le processeur doit être approprié.

L'installation d'un processeur inapproprié pourrait gravement endommager la carte de la plateforme. Voir Liste de compatibilité matérielle pour une liste des composants.

NOTICE

Kontron recommande d'inspecter le socket du CPU avant d'ajouter ou de remplacer un processeur pour s'assurer qu'il n'y a pas de problème avec les broches fragiles du socket.

9.1.3.15.4.1. Préparer le processeur pour l'assemblage dans le PHM

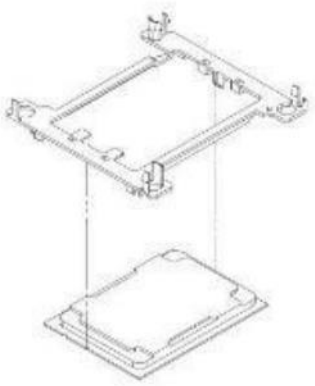
Étape_1	Retirer le couvercle du plateau d'emballage du processeur. Dans cette position, le processeur est prêt à être clipsé au reste des composants du PHM. **ATTENTION :** Ne pas toucher le processeur.

9.1.3.15.4.2. Installer le processeur (nouveau dissipateur thermique et support de processeur)

Section pertinente :

Emplacement des processeurs

Étape_1	Retirer le dissipateur thermique de son emballage. NOTE : Le processeur avec le dissipateur thermique « Avant » (Front) doit être installé sur le socket CPU1 (voir Emplacement des processeurs) Le processeur avec le dissipateur thermique « Arrière » (Rear) doit être installé sur le socket CPU2 (voir Emplacement des processeurs)

Étape_2	Prendre le nouveau PHM (module dissipateur thermique et processeur) et le placer au-dessus du processeur, qui est dans son plateau d'emballage ouvert. Les triangles d'assemblage (indicateur de la broche 1) doivent être dans les positions appropriées avant d'abaisser le PHM. **NOTE :** Sur cette image, le dissipateur thermique a été retiré pour plus de clarté. Seuls le support de processeur et le processeur sont représentés.	
Étape_3	Clipser délicatement le processeur sur le PHM. Soulever l'ensemble. Le processeur doit être clipsé en place.	

9.1.3.15.4.3. Installer un PHM dans la plateforme

Étape_1	Aligner le triangle de la plaque de renfort avec celui du processeur. Poser le PHM sur la plaque de renfort.	
Étape_2	Serrer progressivement (en suivant un motif en étoile) et uniformément chacune des quatre vis selon un schéma diagonal jusqu'à ce que chacune soit fermement serrée (couple de 12,0 lb-po).	

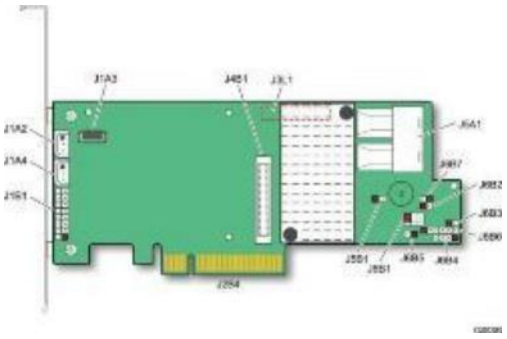
9.1.3.16. Contrôleur RAID

La prise en charge du RAID matériel nécessite un contrôleur RAID/SAS optionnel.

Les composants utilisés à titre d'exemple dans cette section proviennent du matériel Intel® RS3DC080.

La figure suivante illustre la topologie de la carte contrôleur RAID matériel SAS. Le connecteur doré du bord de la carte s'insère dans un connecteur de la carte mère, comme montré dans la section Installer un contrôleur RAID matériel.

Figure 23. Topologie de l'adaptateur RAID matériel

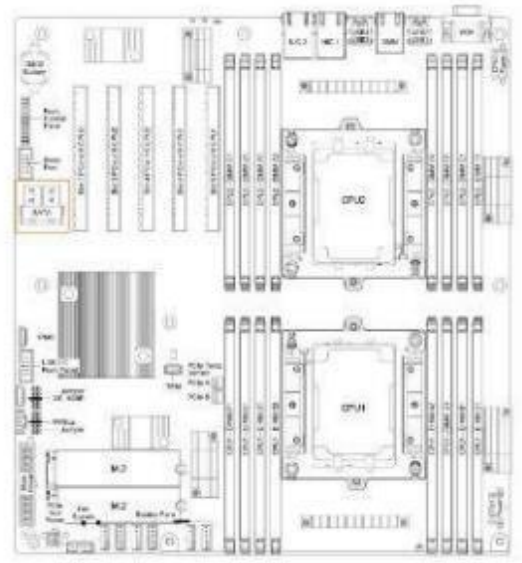


Avant de pouvoir installer ou enlever la carte contrôleur RAID matériel et le module de sauvegarde à batterie SuperCap, il faut enlever (puis réinstaller) :

- Le capot supérieur du châssis
- La cage d'extension PCIe de gauche

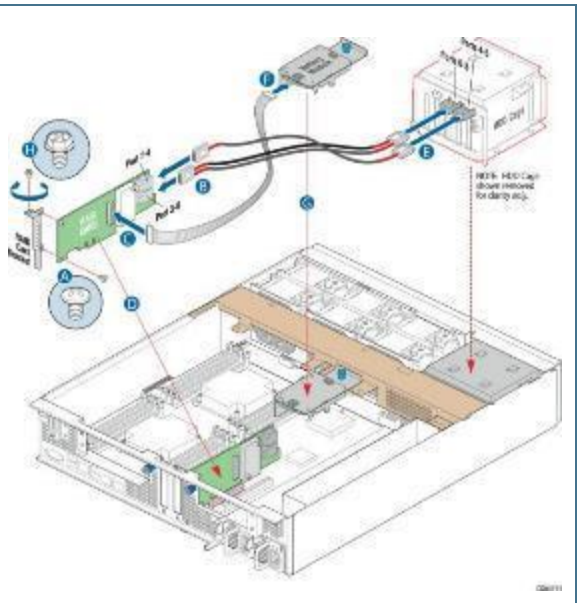
9.1.3.16.1. Débrancher les deux câbles SAS de la carte mère

Figure 24. Emplacement des câbles SAS



Étape_1	Déconnecter les deux câbles SAS (extrémités SFF-8643) de la carte mère.

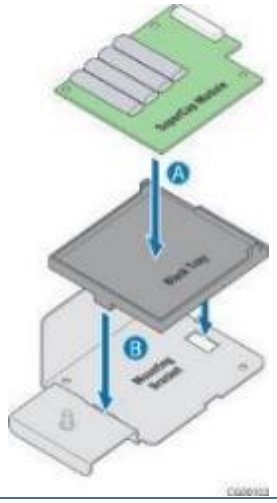
9.1.3.16.2. Installer un contrôleur RAID matériel

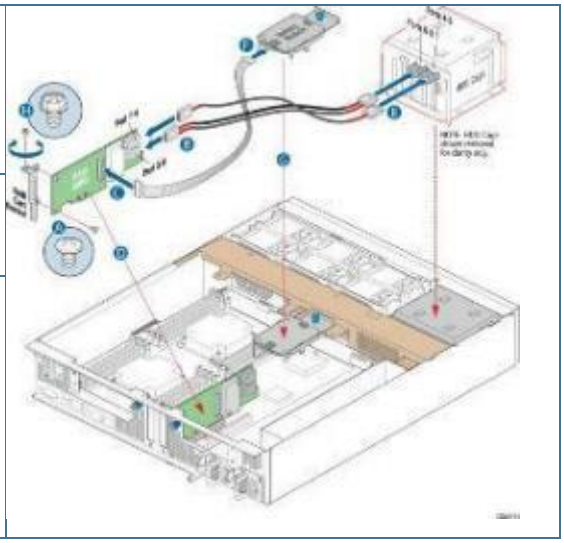
Étape_1	Dévisser la vis qui maintient le support de la carte RAID de l'emplacement 3. Retirer le support du panneau arrière du châssis et le panneau de remplissage de l'emplacement PCIe 4.	
Étape_2	Fixer le support retiré du châssis à la carte contrôleur RAID à l'aide des deux vis du support (A).	
Étape_3	Faire correspondre le câble connecté aux ports 0-3 de la cage du disque dur au port 3-0 de la carte RAID/SAS, en connectant l'extrémité libre à la carte RAID (B). Faire correspondre le câble connecté aux ports 4-5 de la cage du disque dur au port 7-4 de la carte RAID/SAS, en connectant l'extrémité libre à la carte RAID (B). (Optionnel) Si un module de sauvegarde à batterie des configurations RAID SuperCap est utilisé : • Fixer le support du module de sauvegarde à batterie SuperCap sur la traverse du châssis (G). • Connecter le module de sauvegarde à batterie SuperCap à la carte RAID (C et F).	
Étape_4	Réinstaller le panneau de remplissage de l'emplacement PCIe 4 (retiré à l'étape 1), puis insérer la carte contrôleur RAID dans l'emplacement PCIe 3 de la carte mère et appuyer pour l'unir avec le connecteur (D). Le support de l'emplacement 3 est placé directement au-dessus du panneau de remplissage de l'emplacement 4.	
Étape_5	Fixer le panneau de remplissage de l'emplacement 3 avec la vis retirée précédemment (étape 1).	

9.1.3.16.3. Installer le module de sauvegarde à batterie SuperCap

Ce module de sauvegarde à batterie avec mémoire flash sert pour les disques SAS. Elle fait partie de l'ensemble du contrôleur RAID Intel RS3DC080 et pourrait ne pas être compatible avec d'autres produits RAID.

Le support de montage de l'unité doit être commandé séparément, voir Plateforme, modules et accessoires.

Étape_1	Insérer l'unité dans le plateau en plastique noir (A).	
Étape_2	Fixer l'unité et le plateau au support en tôle en insérant les languettes dans les découpes du support (B).	
Étape_3	Faire glisser l'ensemble unité/plateau vers l'arrière (côté avec le connecteur) du support jusqu'à ce qu'il s'enclenche.	

Étape_4	Connecter le câble de signal/alimentation au connecteur approprié sur la carte contrôleur RAID matériel (C) et à l'arrière de l'assemblage du module de sauvegarde à batterie (F).	
Étape_5	Placer le support du module de sauvegarde à batterie sur la traverse, en l'alignant sur le trou central de la plaque d'appui centrale (G).	
Étape_6	Utiliser la vis de retenue bleue pour fixer l'assemblage du module de sauvegarde à batterie à la traverse. **NOTE :** Une fois la plateforme alimentée et fonctionnelle, procéder aux configurations logicielles requises.	

9.1.3.17. Cartes d'expansion PCIe et cartes adaptatrices de connexion PCIe

Seules les cartes adaptatrices de connexion PCIe et les cartes d'expansion PCIe compatibles peuvent être utilisées, voir Plateforme, modules et accessoires pour sélectionner une combinaison carte adaptatrices de connexion/carte d'expansion PCIe appropriée.

⚠CAUTION

En raison du fait que certains fabricants ne respectent pas toujours les spécifications de dimensions appropriées, il existe une possibilité de conflit mécanique avec un dissipateur thermique lorsqu'une carte PCIe est insérée dans l'emplacement 5. Si l'espacement est jugé insuffisant lorsque la carte PCIe est insérée, il est recommandé d'isoler correctement la carte en ajoutant une protection (c.-à-d. du ruban Lexan/Kapton) sur le dissipateur thermique afin d'éviter un court-circuit.

9.1.3.17.1. Cartes d'expansion PCIe dans les emplacements 4 et 5

Deux cartes PCIe demi-hauteur et pleine longueur peuvent être insérées dans les emplacements PCIe 4 et 5 de la carte mère.

Avant de pouvoir installer ou enlever une carte d'expansion PCIe, il faut enlever (puis réinstaller) :

- Le capot supérieur du châssis

9.1.3.17.1.1. Installer une carte d'expansion PCIe

Étape_1	Dévisser la vis qui maintient le panneau de remplissage de l'emplacement PCIe. Retirer le panneau de remplissage vierge et le garder pour une utilisation ultérieure.
Étape_2	Insérer la carte d'expansion PCIe dans l'emplacement PCIe de la carte mère et appuyer pour l'unir au connecteur.
Étape_3	Fixer la carte d'expansion PCIe au châssis avec la vis retirée à l'étape 1.

9.1.3.17.1.2. Enlever une carte PCIe

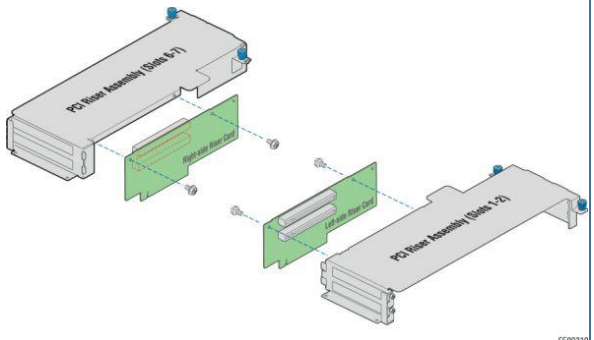
Étape_1	Dévisser la vis qui maintient la carte d'expansion PCIe installée dans l'emplacement.
Étape_2	Retirer la carte d'expansion PCIe de l'emplacement PCIe de la carte mère.
Étape_3	Remettre en place le panneau de remplissage vierge (retiré lors de l'installation de la carte) et le fixer au châssis à l'aide de la vis retirée à l'étape 1. **NOTE :** Le panneau de remplissage est nécessaire pour assurer une bonne circulation de l'air.

9.1.3.17.2. Cartes adaptatrices de connexion PCIe

Les cartes adaptatrices de connexion PCIe ne sont pas incluses avec la plateforme, qui ne contient que les cages en tôle pour loger les cartes adaptatrices de connexion PCIe et les cartes d'expansion. Avant de pouvoir installer une carte adaptatrice de connexion PCIe, il faut enlever (puis réinstaller) :

- Le capot supérieur du châssis
- Les cages d'extension PCIe

9.1.3.17.2.1. Assembler les cartes adaptatrices de connexion PCIe

Étape_1	Fixer la carte adaptatrice de connexion gauche à son support avec les deux vis 6-32 (couple de 8 lb-po).	

La carte adaptatrice de connexion est maintenant prête à recevoir des cartes d'expansion.

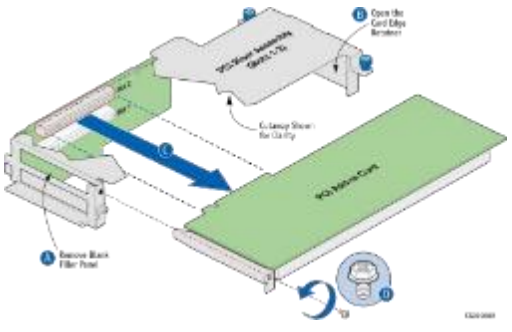
9.1.3.17.3. Ensembles cartes d'expansion et cage d'extension PCIe

Les figures de cette section utilisent la cage d'extension PCIe de gauche (emplacement 2), une carte adaptatrice de connexion PCIe à emplacement double et une carte d'expansion PCIe simple à titre d'exemple.

Avant de pouvoir enlever ou ajouter une carte d'expansion PCIe, il faut enlever (puis réinstaller) :

- Le capot supérieur du châssis

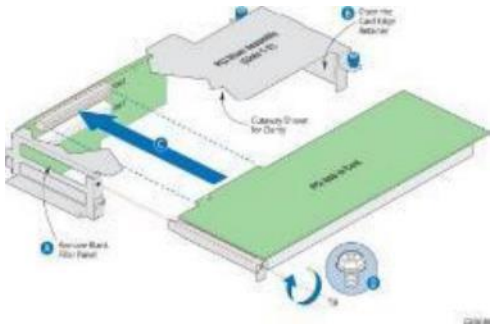
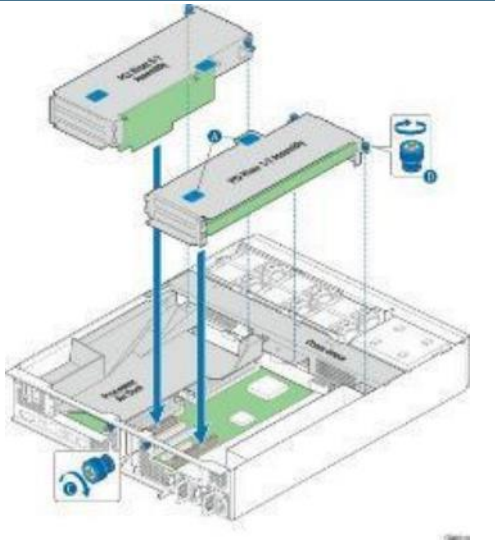
9.1.3.17.3.1. Enlever une carte d'expansion PCIe

Étape_1	Enlever la cage d'extension PCIe. • Desserrer les deux vis de retenue imperdables bleues à l'avant de la cage d'extension PCIe et la vis imperdable bleue à l'arrière du châssis. • En utilisant les deux points de contact bleus, soulever la cage d'extension hors du châssis.	
Étape_2	Dévisser et retirer la vis de retenue arrière (D).	
Étape_3	Pour une carte pleine longueur, avant de retirer la carte de la cage, ouvrir le support d'extrémité de carte à l'avant de la cage en desserrant la vis imperdable bleue (B). Retirer la carte d'expansion PCIe du connecteur de la carte adaptatrice de connexion PCIe (C).	

Étape_4	Installer le panneau de remplissage vierge (A). Fixer la vis (D) pour maintenir le panneau de remplissage en place (couple de 8 lb-po). **NOTE :** Le panneau de remplissage est nécessaire pour assurer une bonne circulation de l'air.	

9.1.3.17.3.2. Installer des cartes d'expansion PCIe

Avant d'installer une carte d'expansion PCIe pour la première fois, la carte adaptatrice de connexion PCIe doit être assemblée. Si une carte d'expansion PCIe est déjà en place, consulter la section Enlever des cartes d'expansion PCIe pour des instructions (faire les étapes 1 à 3 uniquement).

Étape_1	Si une carte d'expansion PCIe est installée pour la première fois, retirer le panneau de remplissage vierge de la cage d'extension (A) en dévissant la vis de l'emplacement sélectionné (D).	
Étape_2	Si une carte d'expansion PCIe est installée pour la première fois, pour une carte pleine longueur, ouvrir le support d'extrémité de carte en desserrant la vis imperdable bleue (B). **NOTE :** Cette étape s'applique uniquement aux cartes pleine longueur (pas aux cartes demi-longueur).	
Étape_3	Joindre la carte d'expansion au connecteur approprié de la carte adaptatrice de connexion (C), en veillant à ce qu'elle soit correctement unie avec le connecteur.	
Étape_4	Fixer la carte d'expansion au support de la cage d'extension avec la vis de retenue arrière (D). Pour les cartes pleine longueur, fixer également la carte dans les rainures du support d'extrémité de carte (B).	
Étape_5	En utilisant les deux points de contact bleus (A), installer la cage d'extension PCIe dans son emplacement (emplacement 2 ou emplacement 6) sur la carte mère.	
Étape_6	Fixer la cage d'extension en serrant les vis imperdables (C et D).	

9.1.3.18. Disques de stockage M.2

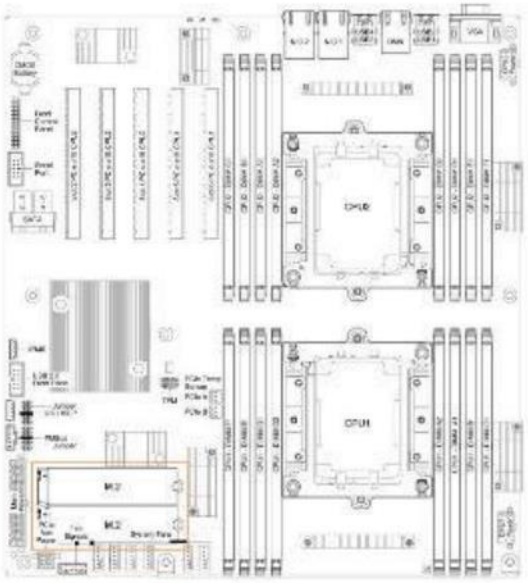
Des disques de stockage M.2 optionnels peuvent fournir un stockage SATA ou NVMe (PCIe). Les disques de stockage M.2 sont installés sur la carte de la plateforme. Avant de pouvoir enlever ou installer un disque de stockage M.2, il faut enlever (puis réinstaller) :

- Le capot supérieur du châssis

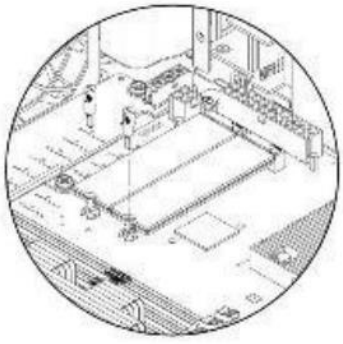
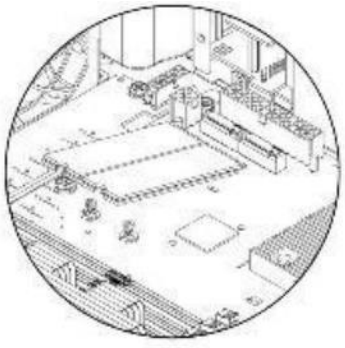
- La cage d'extension PCIe de gauche

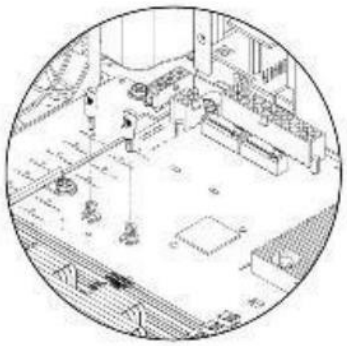
NOTE : La figure montre deux disques de stockage M.2. Les procédures s'appliquent pour chaque disque de stockage M.2.

Figure 25. Emplacement des disques de stockage M.2

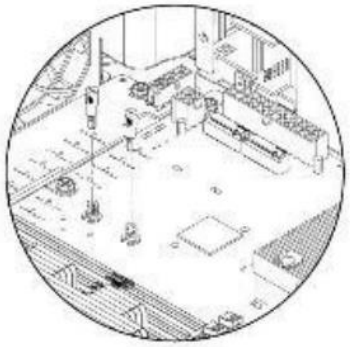
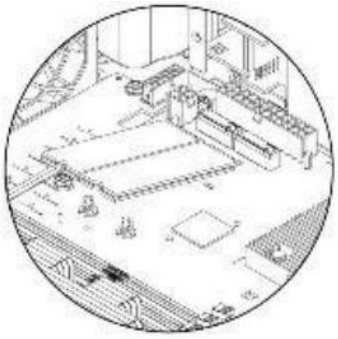
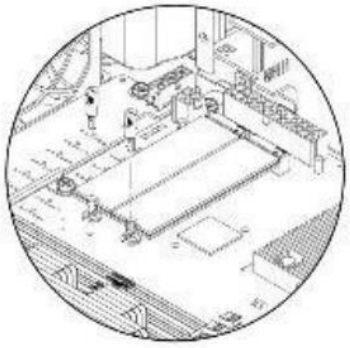


9.1.3.18.1. Enlever le disque de stockage M.2

Étape_1	Retirer le clip du montant pour libérer le disque de stockage M.2.	
Étape_2	Désengager la carte M.2 du connecteur.	

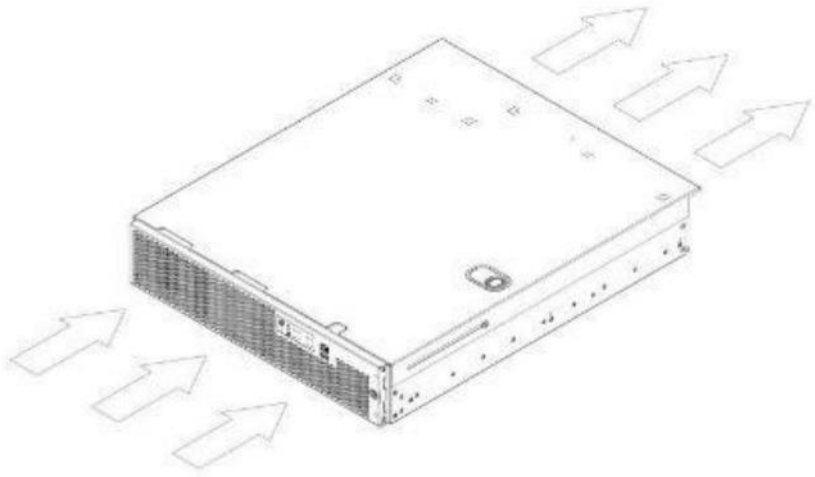
Étape_3	Réinsérer le clip dans le montant qui sert à fixer le disque de stockage M.2.	

9.1.3.18.2. Installer un disque de stockage M.2

Étape_1	Retirer le clip du montant. **NOTE :** Lorsqu'un seul disque de stockage M.2 est ajouté, il est recommandé d'utiliser l'emplacement situé près des ventilateurs.	
Étape_2	Insérer une extrémité de la carte M.2 dans le connecteur et placer l'autre extrémité autour du montant sur la carte mère.	
Étape_3	Fixer le disque de stockage M.2 en insérant le clip dans le montant.	

9.1.4. Circulation de l’air

Figure 26. Direction de la circulation de l’air



9.1.4.1. Considérations pour une bonne circulation de l'air

Section pertinente :

Installation et assemblage des composants

Considération_1	Pour assurer une bonne circulation de l'air, les composants suivants doivent toujours être réinstallés après avoir été retirés pour le remplacement ou l'installation d'un composant : • Conduit d'air des processeurs • Cages d'extension PCIe (gauche et droite) Capot supérieur • Panneau de remplissage en plastique noir du support de disque (lorsqu'un disque n'est pas installé dans un emplacement)
Considération_2	Six ventilateurs doivent être installés en tout temps.
Considération_3	Dans une configuration avec un seul bloc d'alimentation, un panneau de remplissage pour l’emplacement d’un bloc d'alimentation doit être installé dans l'emplacement non utilisé.
Considération_4	Si aucune carte PCIe n'est installée dans les emplacements 4 et 5, des panneaux de remplissage doivent être installés à l'arrière du châssis.

9.1.5. Installation dans une étagère

9.1.5.1. Sélection d’un ensemble de rails

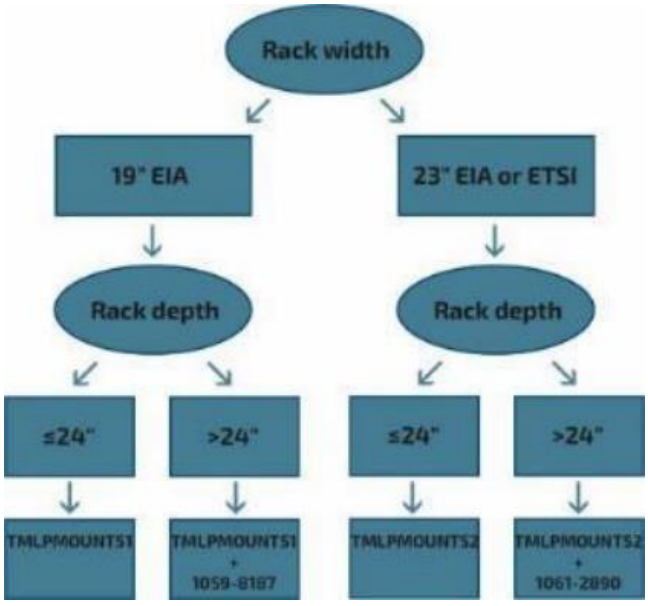
Les ensembles de rails pour montage en étagère proposés pour ce produit sont conçus pour être utilisés avec des étagères à 2 ou 4 montants d'une largeur de 19 po ou 23 po. Tous les ensembles figurant dans le diagramme ci-dessous sont conformes à la norme EIA.

Tous les ensembles présentés dans le diagramme ci-dessous sont fournis avec le matériel approprié pour monter la plateforme dans une étagère 20 à 24 po de profondeur. Pour les étagères d'une profondeur supérieure à 24 po, un ensemble d’extension est également requis.

TMLPMOUNT51 et TMLPMOUNT52 sont conçus avec un système de rails coulissants. Les rails sont conçus pour supporter un serveur monté pendant l'entretien des ventilateurs. TMLCMOUNT21 n'est compatible qu'avec les étagères à 2 montants de 19 po de largeur et ancre le châssis en place. Il est donc recommandé de ne l'utiliser qu'en laboratoire.

Pour choisir entre TMLPMOUNT51 et TMLPMOUNT52, utiliser le diagramme suivant.

Figure 27. Diagramme de sélection de l'ensemble de rails



Code du produit	Description	Rails coulissants avec verrouillage (oui/non)	Quantité minimum de commande
TMLCMOUNT21	Ensemble pour montage en étagère Utilisé pour monter des serveurs sur des étagères de 19 po de largeur, à 2 montants. **NOTE :** Pour une utilisation en laboratoire uniquement.	Non	10
TMLPMOUNT51	Ensemble pour montage en étagère Utilisé pour monter des serveurs sur des étagères de 19 po de largeur, à 2 ou 4 montants. **NOTE :** Finition avec Xylan®	Oui	1
TMLPMOUNT52	Ensemble pour montage en étagère Utilisé pour monter des serveurs sur des étagères de 23 po de largeur, à 2 ou 4 montants. **NOTES :** • Finition avec Xylan® • Supports ETSI inclus	Oui	1
1059-8187	Ensemble d'extension de rails Profondeur maximale de l'étagère lorsqu'utilisé avec TMLPMOUNT51 : 34 po.	S. O.	1
1061-2890	Ensemble d'extension de rails Profondeur maximale de l'étagère lorsqu'utilisé avec TMLPMOUNT52 : 34 po.	S. O.	1

NOTES :

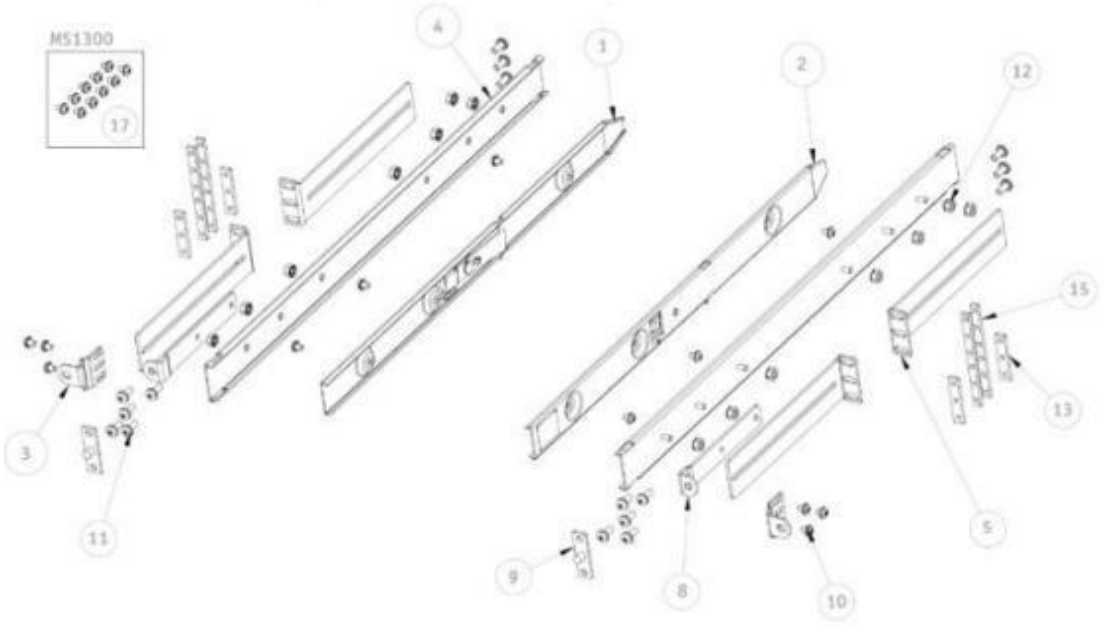
- L'utilisation de rails coulissants pourrait entraîner une non-conformité aux exigences de la zone sismique 4 de NEBS-3.
- Le Xylan® est un revêtement résistant, à faible coefficient de frottement similaire au Téflon.
- L'espacement EIA large ne possède pas le trou interstitiel présent dans l'espacement EIA universel. TMLPMOUNT51 contient un adaptateur large EIA pour résoudre ce problème.

9.1.5.1.1. Ensembles pour montage en étagère

9.1.5.1.1.1. TMLCMOUNT21

Voir Utiliser TMLPMOUNT21 pour plus de détails.

9.1.5.1.1.2. TMLPMOUNT51

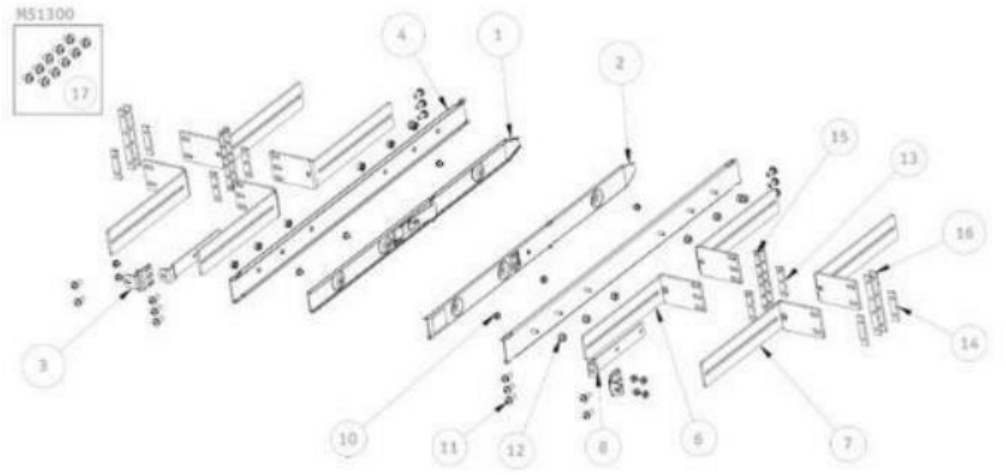


Élément	Qté	Description
1	1	RAIL INTÉRIEUR GAUCHE
2	1	RAIL INTÉRIEUR DROIT
3	2	OREILLE DE MONTAGE
4	2	RAIL EXTÉRIEUR
5	4	SUPPORT EN L 19 PO EIA
8	2	SUPPORT DE MONTAGE À 2 MONTANTS
9	2	ADAPTATEUR LARGE EIA
10	12	VIS « SEM » 8-32 X 1/4
11	16	VIS « SEM » 10-32 X 1/2
12	14	ÉCROU KEPS 8-32
13	4	BARRE AVEC TROUS FILETÉS 1U EIA

Élément	Qté	Description
15	4	BARRE AVEC TROUS FILETÉS 2U EIA
17	12	VIS M4 X 0,7 pour MS1300

NOTE : Les barres avec trous filetés 2U permettent l'installation d'un ensemble de rails dans un emplacement d'étagère 1U lorsque de l'équipement est déjà installé au-dessus et au-dessous de cet emplacement ouvert.

9.1.5.1.1.3. TMLPMOUNT52

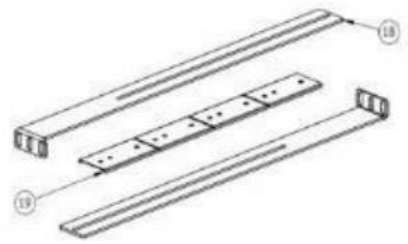


Élément	Qté	Description
1	1	RAIL INTÉRIEUR GAUCHE
2	1	RAIL INTÉRIEUR DROIT
3	2	OREILLE DE MONTAGE
4	2	RAIL EXTÉRIEUR
6	4	SUPPORT EN L 23 PO EIA
7	4	SUPPORT EN L 23 PO ETSI
8	2	SUPPORT DE MONTAGE À 2 MONTANTS
10	12	VIS « SEM » 8-32 X 1/4
11	16	VIS « SEM » 10-32 X 1/2
12	14	ÉCROU KEPS 8-32
13	4	BARRE AVEC TROUS FILETÉS 1U EIA
14	4	BARRE AVEC TROUS FILETÉS 1U ETSI
15	4	BARRE AVEC TROUS FILETÉS 2U EIA
16	4	BARRE AVEC TROUS FILETÉS 2U ETSI
17	12	VIS M4 X 0,7 pour MS1300

NOTE : Les barres avec trous filetés 2U permettent l'installation d'un ensemble de rails dans un emplacement d'étagère 1U lorsque de l'équipement est déjà installé au-dessus et au-dessous de cet emplacement ouvert.

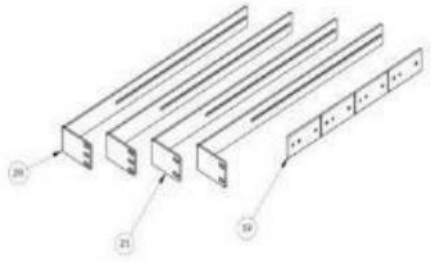
9.1.5.1.2. Ensembles d'extension de rails et supports

9.1.5.1.2.1. Ensemble d'extension 1059 -8187



Élément	Qté	Description
18	2	SUPPORT EN L EIA POUR PASSER DE 24 à 34 PO POUR ÉTAGÈRE DE 19 PO
19	4	SUPPORT DE RETENUE

9.1.5.1.2.2. Ensemble d'extension 1061-2890



Élément	Qté	Description
19	4	SUPPORT DE RETENUE
20	2	SUPPORT EN L EIA POUR PASSER DE 24 à 34 PO POUR ÉTAGÈRE DE 23 PO
21	2	SUPPORT EN L ETSI POUR PASSER DE 24 à 34 PO POUR ÉTAGÈRE DE 23 PO

9.1.5.2. Installation du serveur dans une étagère

⚠CAUTION

Ancrer l'étagère destinée à l'équipement – L'étagère (rack) destinée à l'équipement doit être ancrée à un support impossible à déplacer pour l'empêcher de tomber lorsqu'un ou plusieurs rails coulissants équipés de serveurs sont sortis à l'avant. L'étagère destinée à l'équipement doit être installée conformément aux instructions du fabricant. Il est également requis de tenir compte du poids de tout autre appareil installé dans l'étagère.

Lorsqu'une étagère est utilisée, attendre que le serveur soit correctement monté dans l'étagère avant de brancher le ou les cordons d'alimentation

Dispositif de déconnexion principal **– Les cordons (ou le cordon) d'alimentation sont considérés comme le dispositif de déconnexion principal du serveur et doivent être facilement accessibles une fois installés. Si les cordons (ou le cordon) d'alimentation de chaque serveur ne sont pas accessibles facilement pour permettre leur débranchement, vous êtes responsable d'installer un dispositif de déconnexion électrique pour l'ensemble de l'étagère. Ce dispositif de déconnexion électrique doit être facilement accessible et doit être étiqueté de façon à ce qu'il soit clair qu'il contrôle l'alimentation de l'ensemble de l'étagère, et pas seulement celle du ou des serveurs. Pour couper entièrement l'alimentation, deux cordons d'alimentation doivent être débranchés.**

Mettre à la terre l'étagère destinée à l'équipement – Pour éviter tout risque de choc électrique, si l'alimentation est de type CA, il faut inclure un troisième conducteur de mise à la terre avec l'installation de l'étagère. Pour l'alimentation CC, les deux goujons de mise à la terre du boîtier du châssis doivent être utilisés pour une mise à la terre de sécurité adéquate. Pour une alimentation CA, si le cordon d'alimentation du serveur est branché dans une prise qui fait partie de l'étagère, il faut prévoir une mise à la terre adéquate pour l'étagère elle-même. Si le cordon d'alimentation du serveur est branché dans une prise murale, le conducteur de mise à la terre du cordon d'alimentation assure une mise à la terre adéquate pour le serveur uniquement. Il est requis de prévoir une mise à la terre supplémentaire et appropriée pour l'étagère et les autres périphériques qui y sont installés.

Protection contre les surintensités CA – Lorsqu'une alimentation CA est utilisée, le serveur est conçu pour une source de tension d'entrée avec une protection contre les surintensités allant jusqu'à 20 ampères par cordon d'alimentation. Si le système d'alimentation pour l'étagère destinée à l'équipement est installé sur un circuit de dérivation dont la protection est supérieure à 20 ampères, il est requis de fournir une protection supplémentaire pour le serveur. La consommation de courant nominale totale d'un serveur configuré avec deux blocs d'alimentation est inférieure à 6 ampères.

Voir la section Informations sur la sécurité et la réglementation **pour plus d'informations sur le dispositif de déconnexion principal, la mise à la terre et la protection contre les surintensités CA.**

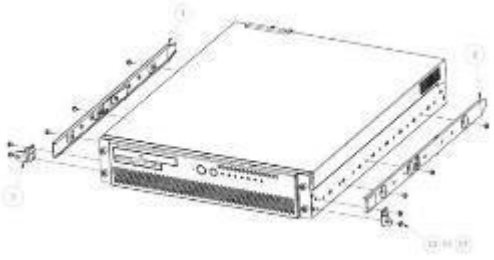
NOTICE

Température – La température de fonctionnement du serveur, lorsqu'il est installé dans une étagère, ne doit pas être inférieure à 5 °C (41 °F) ni supérieure à 40 °C (104 °F). Les fluctuations extrêmes de température peuvent provoquer divers problèmes dans le serveur.

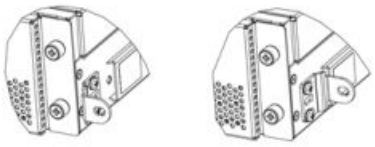
NOTE : La plateforme illustrée dans les instructions d'installation ci-dessous est différente du serveur CG2400 et n'est utilisée qu'à des fins de démonstration.

9.1.5.2.1. Utiliser TMLPMOUNT51 ou TMLPMOUNT52

9.1.5.2.1.1. Installer les rails intérieurs et les oreilles de montage

Étape_1	Fixer le rail intérieur gauche (élément 1) et le rail intérieur droit (élément 2) au châssis avec 3 vis (élément 10) par rail intérieur.	
Étape_2	Fixer les 2 oreilles de montage (élément 3) au châssis à l'aide de 2 vis (élément 10) par oreille de montage.	

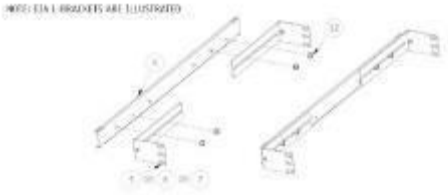
Les oreilles de montage (élément 3) peuvent être retournées pour positionner l'équipement plus en avant dans l'étagère.



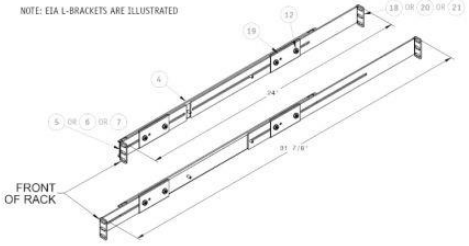
9.1.5.2.1.2. Bâtir l'assemblage des rails extérieurs

- Pour une installation sur 4 montants dans des étagères de moins de 24 po de profondeur, naviguer à la section Installation sur 4 montants – étagères de moins de 24 po de profondeur.
- Pour une installation sur 4 montants dans des étagères de 24 po à 31 ⅞ po de profondeur, naviguer à la section Installation sur 4 montants – étagères de 30 ¼ po à 34 ⅜ po de profondeur.
- Pour une installation sur 4 montants dans des étagères de 30 ¼ po à 34 ⅜ po de profondeur, naviguer à la section Installation sur 4 montants – étagères de 30 ¼ po à 34 ⅜ po de profondeur
- Pour une installation sur 2 montants, naviguer à la section Installation sur 2 montants.

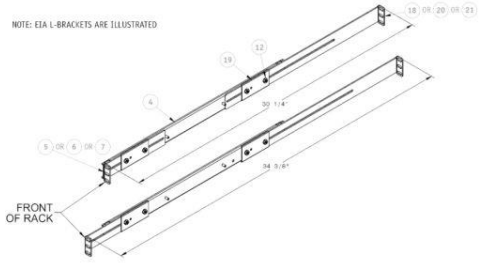
9.1.5.2.1.2.1 Installation sur 4 montants – étagères de moins de 24 po de profondeur

Étape_1	Insérer 2 supports en L (élément 5 pour 19 po EIA, élément 6 pour 23 po EIA ou élément 7 pour 23 po ETSI) sur les tiges filetées d'un rail extérieur (élément 4) comme montré sur la figure.	Assemblage des supports en L (4 montants de moins de 24 po de profondeur) 
Étape_2	Visser sans serrer 2 écrous (élément 12) par support en L.	
Étape_3	Ajuster les supports en L à la longueur requise et serrer les écrous.	
Étape_4	Répéter les étapes 1 à 3 pour bâtir un total de 2 assemblages de rails extérieurs.	

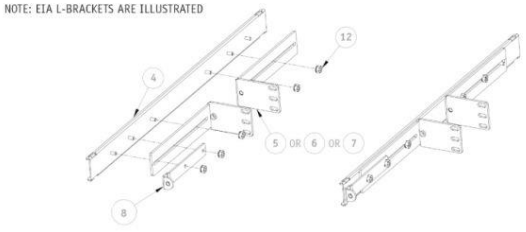
9.1.5.2.1.2.2 Installation sur 4 montants – étagères de 24 po à 31 ⅞ po de profondeur

Étape_1	Insérer 1 support en L (élément 5 pour 19 po EIA, élément 6 pour 23 po EIA ou élément 7 pour 23 po ETSI) et 1 support en L d'extension (élément 18 pour 19 po EIA, élément 20 pour 23 po EIA ou élément 21 pour 23 po ETSI) sur les tiges filetées d'un rail extérieur (élément 4) comme montré sur la figure.	Assemblage des supports en L à l'aide d'un ensemble d'extension (étagères à 4 montants de 24 po à 31 ⅞ po de profondeur) 
Étape_2	Insérer 2 supports de retenue (élément 19) sur les tiges filetées comme montré sur la figure.	
Étape_3	Visser sans serrer 2 écrous (élément 12) par support en L.	
Étape_4	Ajuster les supports en L à la longueur requise et serrer les écrous.	
Étape_5	Répéter les étapes 1 à 4 pour bâtir un total de 2 assemblages de rails extérieurs.	

9.1.5.2.1.2.3 Installation sur 4 montants – étagères de 30 ¼ po à 34 ⅜ po de profondeur

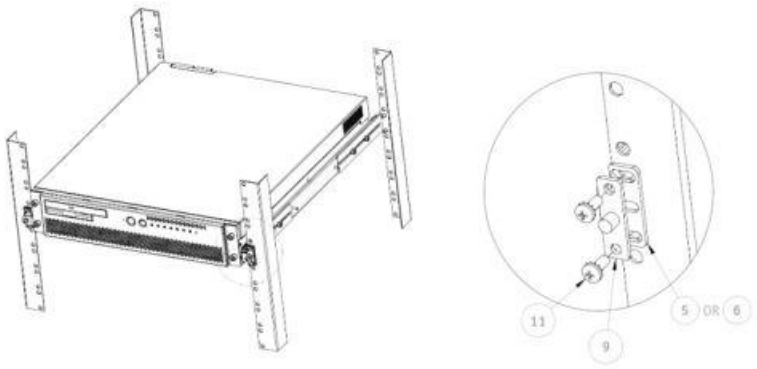
Étape_1	Insérer 1 support en L (élément 5 pour 19 po EIA, élément 6 pour 23 po EIA ou élément 7 pour 23 po ETSI) et 1 support en L d'extension (élément 18 pour 19 po EIA, élément 20 pour 23 po EIA ou élément 21 pour 23 po ETSI) sur les tiges filetées d'un rail extérieur (élément 4) comme montré sur la figure.	Assemblage des supports en L à l'aide d'un ensemble d'extension (étagères à 4 montants de 30 ¼ po à 34 ⅜ po de profondeur) 
Étape_2	Insérer 2 supports de retenue (élément 19) sur les tiges filetées comme montré sur la figure.	
Étape_3	Visser sans serrer 2 écrous (élément 12) par support en L.	
Étape_4	Ajuster les supports en L à la longueur requise et serrer les écrous.	
Étape_5	Répéter les étapes 1 à 4 pour bâtir un total de 2 assemblages de rails extérieurs.	

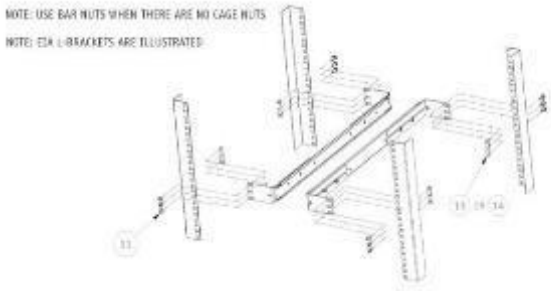
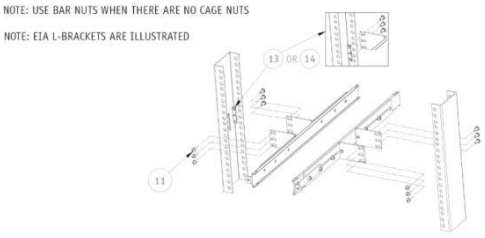
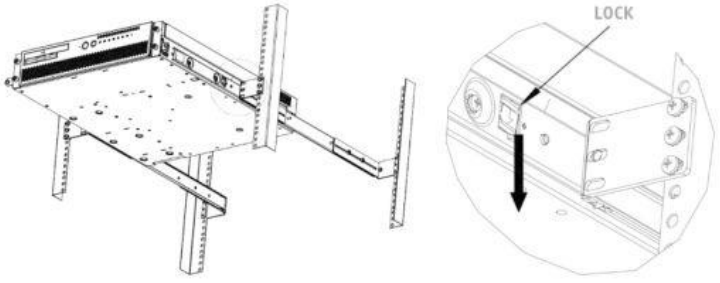
9.1.5.2.1.2.4 Installation sur 2 montants

Étape_1	Insérer 2 supports en L (élément 5 pour 19 po EIA, élément 6 pour 23 po EIA ou élément 7 pour 23 po ETSI) sur les tiges filetées d'un rail extérieur (élément 4) comme montré sur la figure.	Assemblage des supports en L (2 montants) 
Étape_2	Insérer un support de montage pour 2 montants (élément 8) sur les tiges filetées comme montré sur la figure.	
Étape_3	Visser sans serrer un total de 5 écrous (élément 12) pour les deux supports en L.	
Étape_4	Ajuster les supports en L à la longueur requise et serrer les écrous.	
Étape_5	Répéter les étapes 1 à 4 pour bâtir un total de 2 assemblages de rails extérieurs.	

9.1.5.2.1.3. Fixer les assemblages de rails extérieurs aux montants de l'étagère

Lors d'une installation dans une étagère à 4 montants avec un espacement de trous EIA large, l'adaptateur large EIA (élément 9) doit être installé sur le dessus des supports en L avant avec 2 vis (élément 11) par support en L comme montré sur la figure.



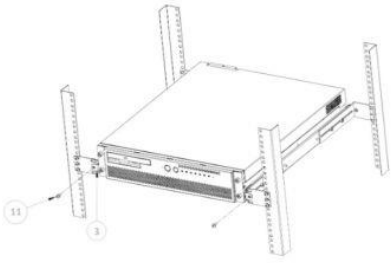
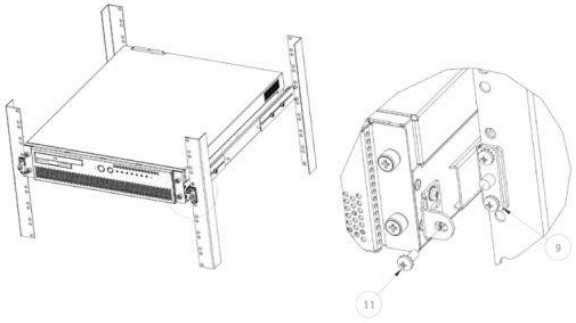
Étape_1	Fixer les assemblages de rails extérieurs (tels qu'ils ont été bâtis au cours de la phase Bâtir l'assemblage des rails extérieurs) à l'étagère avec 8 ou 12 vis (élément 11). Si l'étagère est conçue pour utiliser des écrous à cage, aucune barre avec trous filetés ne sera requise. Si l'étagère a des trous ronds, des barres avec trous filetés (élément 13 pour EIA et élément 14 pour ETSI) doivent être utilisées. S'assurer que le schéma des trous de la barre avec trous filetés correspond au schéma des trous du support en L. **NOTE :** Si l'étagère n'est pas conçue pour des écrous à cage et que plusieurs systèmes 1U doivent être installés immédiatement l'un au-dessus de l'autre, des barres avec trous filetés 2U (élément 15 pour EIA et élément 16 pour ETSI) doivent être utilisées pour des raisons de commodité.	Assemblage des rails extérieurs dans une étagère à 4 montants  Assemblage des rails extérieurs dans une étagère à 2 montants 
Étape_2	Faire glisser l'équipement dans l'étagère, en s'assurant que les rails intérieurs s'emboîtent dans les rails extérieurs. Soutenir le poids du système jusqu'à ce que le mécanisme de verrouillage s'enclenche dans les rails extérieurs. **NOTE :** Pour retirer l'équipement, le faire glisser vers l'avant jusqu'à ce que vous puissiez accéder aux mécanismes de verrouillage. Appuyer sur les mécanismes de verrouillage des deux côtés et continuer à sortir l'équipement, tout en supportant entièrement le poids du système.	Libération du mécanisme de verrouillage 

9.1.5.2.1.4. Fixer l'équipement

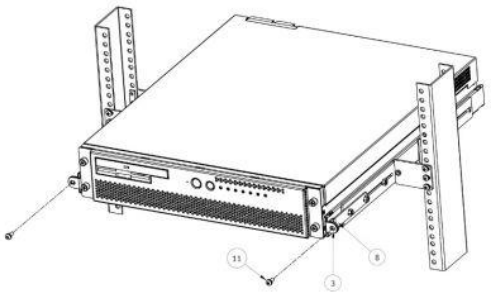
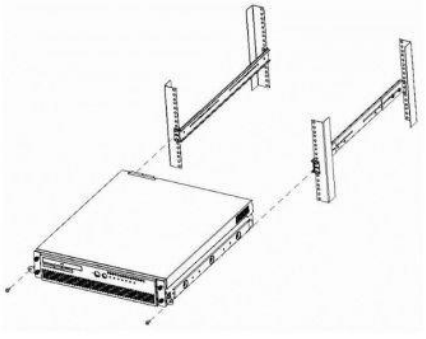
- Pour une étagère à 4 montants, voir Fixer l'équipement dans une étagère à 4 montants

- Pour une étagère à 2 montants, voir Fixer l'équipement dans une étagère à 2 montants

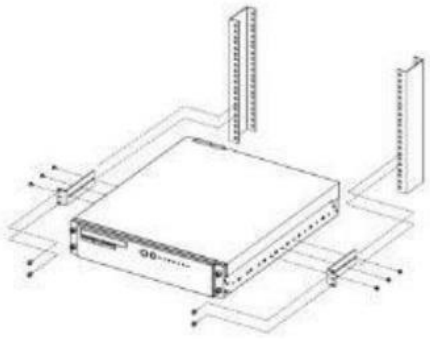
9.1.5.2.1.4.1 Fixer l'équipement dans une étagère à 4 montants

Étape_1	Fixer chaque oreille de montage (élément 3) à un support en L avant avec un total de 2 vis (élément 11) comme montré sur les figures.	Fixer l'équipement dans une étagère à 4 montants (EIA standard)  Fixer l'équipement dans une étagère à 4 montants (norme EIA large) 

9.1.5.2.1.4.2 Fixer l'équipement dans une étagère à 2 montants

Étape_1	Fixer chaque oreille de montage (élément 3) à un support de montage pour 2 montants (élément 8) avec un total de 2 vis (élément 11) comme montré sur la première figure.	 

9.1.5.2.2. Utiliser TMLPMOUNT21

Étape_1	Fixer chaque support de montage à la plateforme avec un total de 3 vis comme montré sur la figure.	
Étape_2	Fixer chaque support de montage à l'étagère avec un total de 2 vis comme montré sur la figure.	

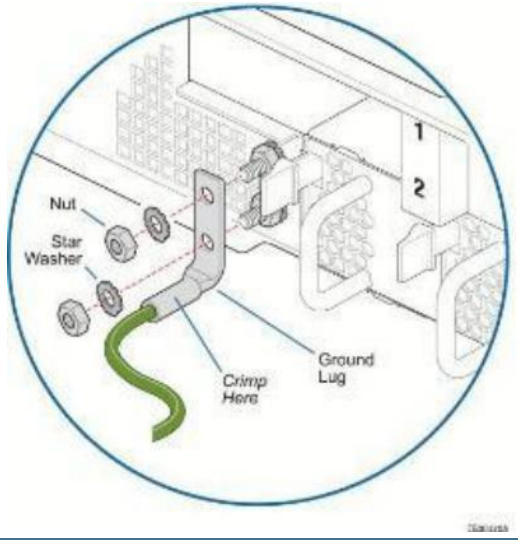
9.1.5.3. Mise à la terre

Sections pertinentes :

Plateforme, modules et accessoires

Matériel, information et logiciels nécessaires

Informations sur la sécurité et la réglementation

Étape_1	Si une cosse de mise à la terre est installée, retirer les 2 écrous et rondelles des goujons de la cosse de mise à la terre. Retirer la cosse de mise à la terre.	
Étape_2	Dénuder 19 mm (0,75 po) du câble de mise à la terre de calibre AWG nº 8.	
Étape_3	Insérer le câble de mise à la terre de calibre AWG no 8 dans la cosse de mise à la terre. Sertir la cosse sur le câble à l'aide d'une pince à sertir manuelle appropriée (ex. l'outil de sertissage Panduit CT-1700 ajusté comme suit : code de couleur = rouge; numéro de matrice = P21).	
Étape_4	Installer la cosse de mise à la terre sur les goujons, en la fixant à l'aide des 2 écrous et rondelles.	

9.1.6. Câblage

9.1.6.1. Alimentation CA

Si un cordon d'alimentation CA n'a pas été fourni avec votre produit, vous pouvez en acheter un dont l'utilisation est approuvée dans votre pays.

⚠WARNING

Pour éviter tout risque de choc électrique ou d'incendie :

- Ne pas tenter de modifier ou d'utiliser le ou les cordons d'alimentation CA s'ils ne sont pas du type exact requis pour s'insérer dans les prises électriques mises à la terre.
- Chaque cordon d'alimentation doit avoir des caractéristiques électriques supérieures ou égales à celles du courant électrique nominal indiqué sur le produit.

- Chaque cordon d'alimentation doit être équipé d'une broche ou d'un contact de mise à la terre adapté à la prise électrique.
- Les cordons (ou le cordon) d'alimentation sont considérés comme le dispositif de déconnexion principal de l'alimentation CA. Les prises (ou la prise) de courant doivent se trouver à proximité de l'équipement et être facilement accessibles pour le débranchement.
- Les cordons (ou le cordon) d'alimentation doivent être branchés dans des prises de courant dotées d'une mise à la terre appropriée.

9.1.6.1.1. Directives sur l'utilisation des cordons d'alimentation

Les directives suivantes peuvent aider à déterminer le jeu de cordons approprié. Le jeu de cordons d'alimentation utilisé doit être conforme aux codes électriques locaux du pays. Pour les États-Unis et le Canada, homologué UL et/ou certifié CSA (UL signifie Underwriters' Laboratories, Inc. et CSA signifie Association canadienne de normalisation).

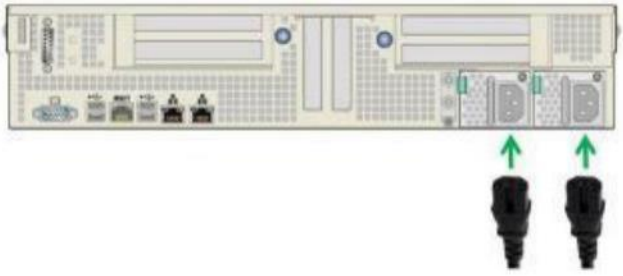
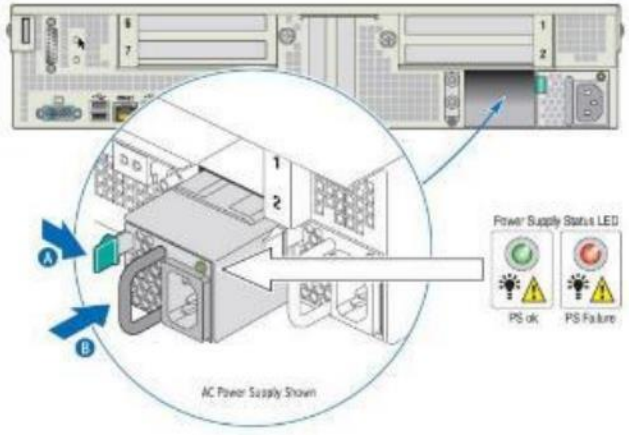
En dehors des États-Unis et du Canada, les cordons doivent être certifiés conformément aux codes électriques locaux, avec trois conducteurs de 0,75 mm classifiés pour une tension de 250 VCA. Connecteur d'extrémité de la prise murale :

- L'extrémité des cordons doit être une fiche mâle avec mise à la terre conçue pour être utilisée dans votre région.
- Le connecteur doit porter des marques d'homologation attestant d'une certification par un organisme reconnu dans votre région.

Les connecteurs d'extrémité de la plateforme sont des connecteurs femelles de type IEC 320 C13.

La longueur maximale du cordon est de 2 m.

9.1.6.1.2. Branchement de l'alimentation CA

Étape_1	Brancher un cordon avec une classification appropriée d'une source d'alimentation externe dans chaque bloc d'alimentation situé à l'arrière de la plateforme.	
Étape_2	Vérifier que la DEL de chaque bloc d'alimentation est verte clignotante (charge utile désactivée) ou verte fixe (charge utile activée). Si ce n'est pas le cas, voir Composants de la plateforme pour une description du comportement des DEL.	

9.1.6.2. Alimentation CC

NOTICE

Avant de travailler avec ce produit ou d'exécuter les instructions décrites dans la section Guide de démarrage ou dans d'autres sections, lire la section Informations sur la sécurité et la réglementation propre au produit. Les instructions d'assemblage contenues dans cette documentation doivent être suivies pour garantir et maintenir la conformité avec les certifications et approbations existantes associées au produit. Utiliser uniquement les composants décrits et réglementés spécifiés dans cette documentation. L'utilisation d'autres produits/composants annulera la certification CSA et les autres approbations réglementaires du produit et entraînera très probablement une non-conformité avec les réglementations relatives au produit dans la ou les régions dans lesquelles le produit est vendu.

9.1.6.2.1. Connecteur d'entrée du bloc d'alimentation CC

Le connecteur d'entrée du bloc d'alimentation CC est un Positronic à 3 broches. Ce connecteur est conçu pour supporter 20 A par broche. Une broche de mise à la terre n'est pas nécessaire, car la plateforme est équipée de deux goujons de mise à la terre sur son panneau arrière.

Figure 28. Connecteur d'entrée du bloc d'alimentation CC

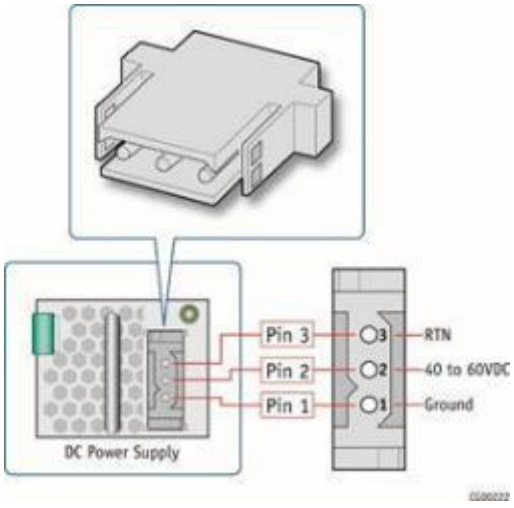
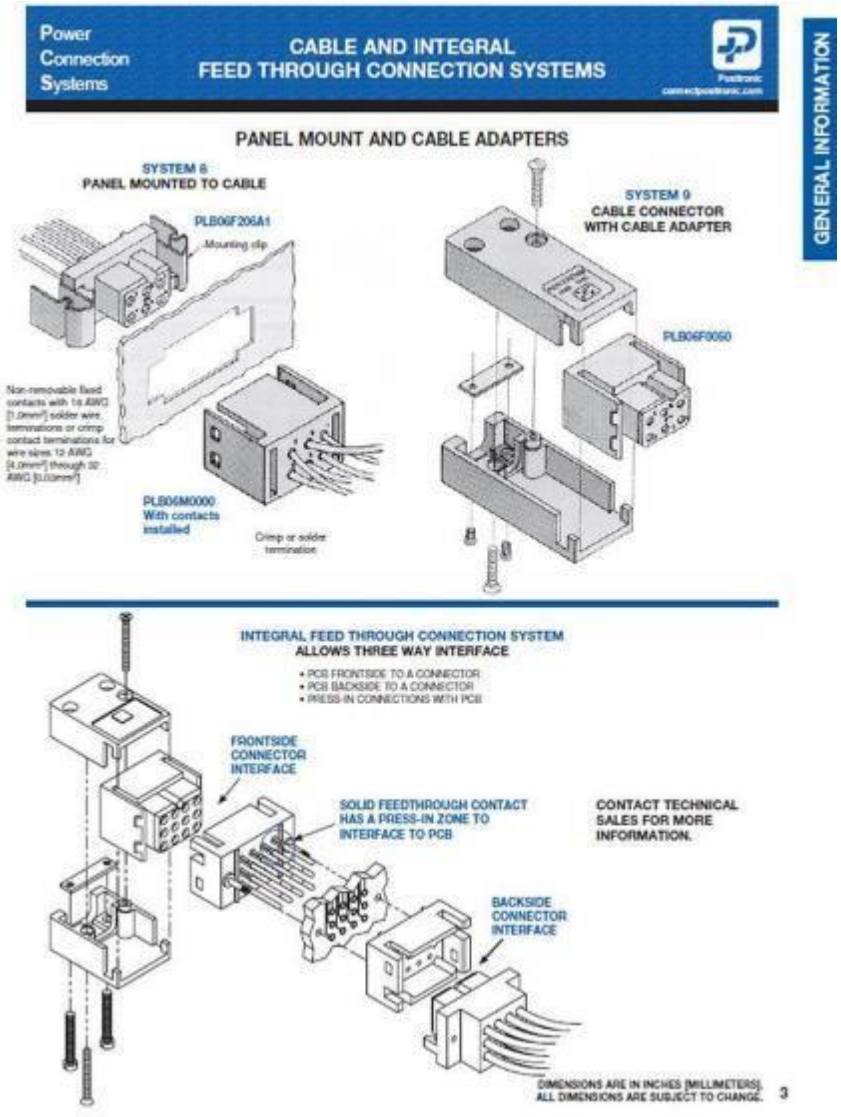


Figure 29. Processus d'assemblage du connecteur



9.1.6.2.2. Fabrication des cordons d'alimentation

⚠WARNING **L'installation de ce produit doit être effectuée conformément aux codes de câblage nationaux et aux réglementations locales.**

Pour fabriquer les cordons d'alimentation (extrémités qui seront branchées dans le CG2400), le matériel, les outils et les fils spécifiés ci-dessous sont nécessaires.

NOTE : Les autres extrémités des cordons devront être fabriquées conformément aux codes de câblage nationaux et aux réglementations locales, en plus de tenir compte des exigences de l'installation d'alimentation électrique de votre centre de données.

Description	Quantité	Numéro de pièce du fabricant	Lien
Fil noir toronné de calibre AWG nº 12 pour fabriquer le cordon d'alimentation en fonction de la longueur requise	Longueur requise		
Fil rouge toronné de calibre AWG nº 12 pour fabriquer le cordon d'alimentation en fonction de la longueur requise	Longueur requise		
Connecteur homologue Positronic pour l'entrée du bloc d'alimentation CC (comprend un assemblage de décharge de traction)	1 (fourni avec le module d'alimentation CC)	PLA03F7050/AA	Catalogue Positronic
Cosse à sertir de calibre 16 Positronic	3 (fourni avec le module d'alimentation CC)	FC112N2/AA-14	Catalogue Positronic
Vis de décharge de traction	2 (fourni avec le module d'alimentation CC)	Fait partie de l'ensemble 1059-8642 Voir Plateforme, modules et accessoires	
Plaque de décharge de traction	1 (fourni avec le module d'alimentation CC)	Fait partie de l'ensemble 1059-8642 Voir Plateforme, modules et accessoires	
Vis Phillips à tête plate	2 (fourni avec le module d'alimentation CC)	Fait partie de l'ensemble 1059-8642 Voir Plateforme, modules et accessoires	
Pince à sertir manuelle DMC AF8	1	AF8	• Catalogue des pinces à sertir manuelle DMC • Fiche technique – DMC AF8
Outil d'extraction manuelle	1	9081-0-0-0	• Catalogue des outils d'extraction Molex • Spécifications

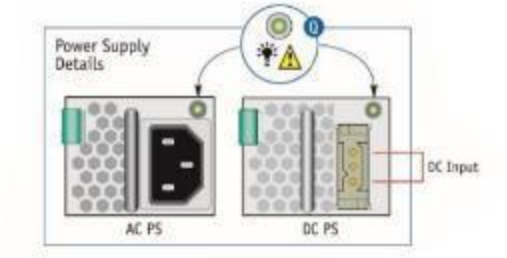
Voici un lien vers une vidéo montrant comment sertir les broches et les assembler dans le connecteur : CG2300DC Power Supply Cable instruction.

NOTE : Cette procédure est valable pour les connecteurs du CG2300 et du CG2400.

Étape_1	Dénuder l'extrémité d'un fil noir toronné de calibre AWG nº 12 sur une longueur de 6,6 mm (0,26 po).
Étape_2	Dénuder l'extrémité d'un fil rouge toronné de calibre AWG nº 12 sur une longueur de 6,6 mm (0,26 po).
Étape_3	Insérer chaque fil dans une cosse à sertir. Suivre la procédure du fabricant de la cosse à sertir, en utilisant la pince à sertir manuelle appropriée, comme spécifié dans la fiche technique du AF8 de DMC.
Étape_4	Insérer le fil rouge serti et le fil noir serti dans les douilles appropriées du boîtier de la prise.
Étape_5	Insérer la plaque de décharge de traction dans la partie appropriée de l'assemblage de décharge de traction.

Étape_6	Insérer le connecteur avec les fils dans le sous-ensemble de l'assemblage de décharge de traction.
Étape_7	Placer le couvercle pour compléter l'assemblage de décharge de traction.
Étape_8	Insérer et serrer les 2 vis Phillips à tête plate (une de chaque côté) pour bien fermer l'assemblage.
Étape_9	Insérer et serrer les 2 vis de décharge de traction pour fixer la plaque de décharge de traction.

9.1.6.2.3. Branchement de l’alimentation CC

Étape_1	Brancher un cordon avec une classification appropriée d'une source d'alimentation externe dans chaque bloc d'alimentation situé à l'arrière de la plateforme.	
Étape_2	Vérifier que la DEL de chaque bloc d'alimentation est verte clignotante (charge utile désactivée) ou verte fixe (charge utile activée). Si ce n’est pas le cas, voir Composants de la plateforme pour une description du comportement des DEL.	

9.2. Installation et déploiement de logiciels

9.2.1. Préparation de l'installation du système d'exploitation

Étape_1	Choisir le système d'exploitation nécessaire en fonction des exigences de votre application (CentOS 7.6 ou la version la plus récente est recommandé).
Étape_2	Confirmer que la version du système d'exploitation à installer inclut ou est compatible avec le pilote d'interface réseau suivant : **i40e**.
Étape_3	Si requis, télécharger le fichier ISO du système d'exploitation à installer.

Pour une liste des systèmes d'exploitation compatibles connus, voir Systèmes d’exploitation validés.

Pour de l'information sur les composants, voir Mappage PCI.

9.2.2. Installation d'un système d'exploitation sur un serveur

Le système d'exploitation peut être installé :

- En utilisant le KVM
- En utilisant PXE (Boot from LAN)
- En utilisant une unité de stockage USB

Pour un système d'exploitation hérité, voir Installer un système d'exploitation hérité.

9.2.2.1. Installer un système d'exploitation sur un serveur en utilisant le KVM

Section pertinente :

Accéder au BMC

9.2.2.1.1. Préalables

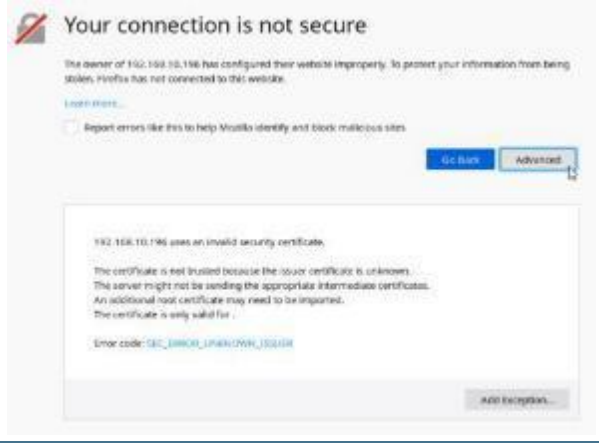
1	L'adresse IP du BMC est connue (voir la section Configuration > Contrôleur de gestion de carte mère – BMC pour obtenir le paramètre IP_GESTION_BMC).
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.

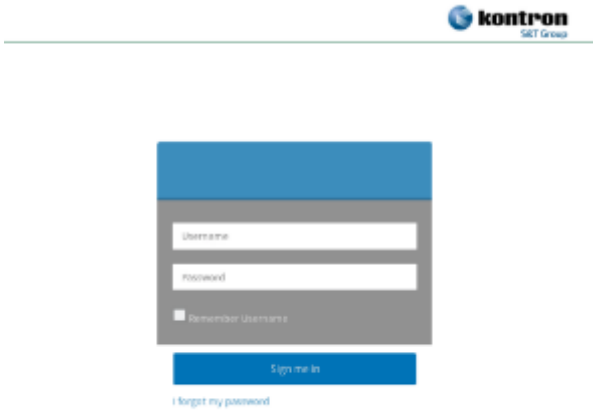
9.2.2.1.2. Considérations relatives au navigateur

HTML5	Pour établir une communication avec l'interface utilisateur Web, un navigateur Web prenant en charge HTML5 est nécessaire.
Certificat auto-signé HTTPS	Lors de l'établissement d'une connexion à l'interface Web, il est obligatoire d'accepter le certificat auto-signé HTTPS. Pour plus d'information sur l'acceptation des certificats auto-signés HTTPS, se reporter à la documentation du navigateur Web.
Autorisation de téléchargement de fichiers	Le téléchargement de fichiers à partir du site doit être autorisé. Pour plus d'information sur les autorisations de téléchargement de fichiers, se reporter à la documentation du navigateur Web.
Témoins	Les témoins doivent être activés pour pouvoir accéder au site Web. Pour plus d'information sur l'activation des témoins, se reporter à la documentation du navigateur Web.

NOTE : La procédure peut varier selon le navigateur utilisé. Les exemples fournis utilisent Firefox.

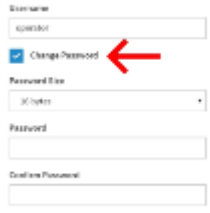
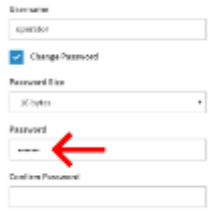
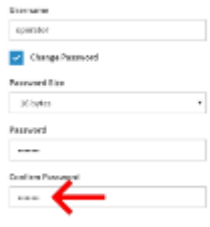
9.2.3. Établir la communication avec l'interface utilisateur Web du BMC

Étape_1	À partir d'un ordinateur distant ayant accès au réseau de gestion, ouvrir une fenêtre de navigateur et entrer l'adresse IP découverte pour le BMC. NOTE : Le préfixe HTTPS est obligatoire. *https://[IP_GESTION_BMC]*	
Étape_2	Cliquer sur **Advanced** pour lancer le processus d'acceptation du certificat auto-signé HTTPS. De l'information sur le message d'erreur s'affichera.	

Étape_3	Cliquer sur **Add Exception...** La fenêtre contextuelle Add Security Exception s'affichera. Cliquer sur **Confirm Security Exception** pour autoriser le navigateur à accéder à l'interface utilisateur Web de gestion de cette interface.	
Étape_4	Ouvrir une session dans l'interface utilisateur Web du BMC à l'aide des données d'accès appropriées. **NOTE :** Le nom d'utilisateur et le mot de passe par défaut de l'interface utilisateur Web sont admin/admin.	
Étape_5	Vous avez maintenant accès à l'interface utilisateur Web de gestion du BMC. Vous pouvez utiliser l'interface.	

9.2.3.1.1. Changer le nom d'utilisateur et le mot de passe

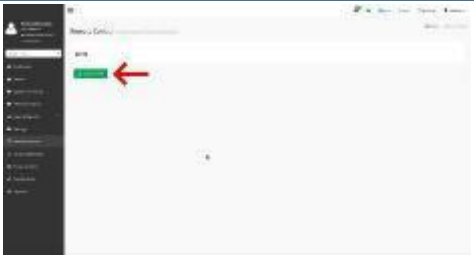
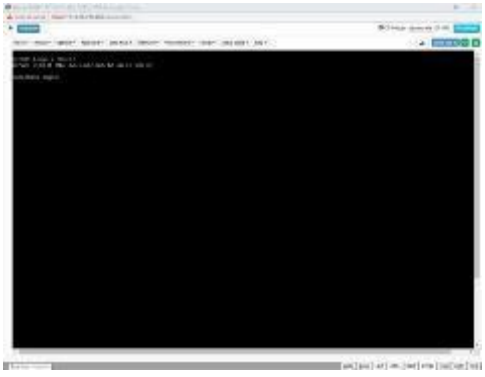
Noter que le champ du mot de passe est obligatoire, **qu'il doit comporter un minimum de 8 caractères et qu'il ne doit pas contenir de mots du dictionnaire.** Il est recommandé, mais pas obligatoire, de saisir un mot de passe fort composé d'au moins une lettre majuscule, d'un caractère alphanumérique et d'un caractère spécial. **Ne pas utiliser les symboles du code ASCII étendu, car ils ne sont pas gérés par l'outil IPMI.**

Étape_1	Cliquer sur **Settings** dans le menu de gauche puis cliquer sur **User Management**.	
Étape_2	Sélectionner l'utilisateur à gérer. **NOTE :** Le premier et le deuxième utilisateur sont des champs réservés, leurs noms d'utilisateur ne peuvent donc pas être modifiés.	
Étape_3	Modifier le champ **Username** si nécessaire.	
Étape_4	Cocher la case **Change Password**.	
Étape_5	Créer un nouveau mot de passe. **NOTE :** Il est recommandé, mais pas obligatoire, de saisir un mot de passe fort composé d'au moins une lettre majuscule, d'un caractère alphanumérique et d'un caractère spécial**. Ne pas utiliser les symboles du code ASCII étendu, car ils ne sont pas gérés par l'outil IPMI.** Noter que le champ du mot de passe est obligatoire et qu'il doit comporter un minimum de 8 caractères lorsque le service SNMP est activé.	
Étape_6	Confirmer le mot de passe.	

Étape_7	Cliquer sur **Save**.	

9.2.3.1.2. Lancer le KVM

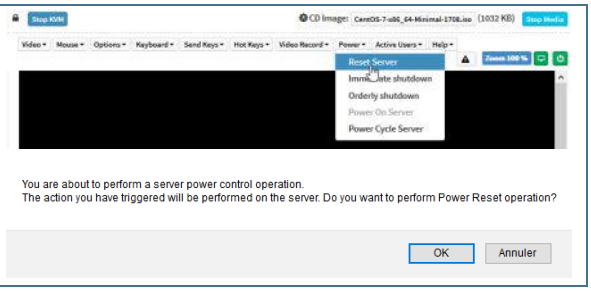
L'interface utilisateur Web permet de contrôler le serveur à distance via une interface KVM (écran-clavier-souris).

Étape_1	Dans le menu de gauche, cliquer sur **Remote Control**.	
Étape_2	Dans le menu **Remote Control**, cliquer sur le bouton **Launch KVM**.	
Étape_3	Une nouvelle fenêtre de navigateur s'ouvre et affiche l'écran du serveur. **NOTE :** Si un système d'exploitation est installé, l'image affichée pourrait être celle du système d'exploitation.	

9.2.3.1.3. Monter l'image du système d'exploitation via un support virtuel

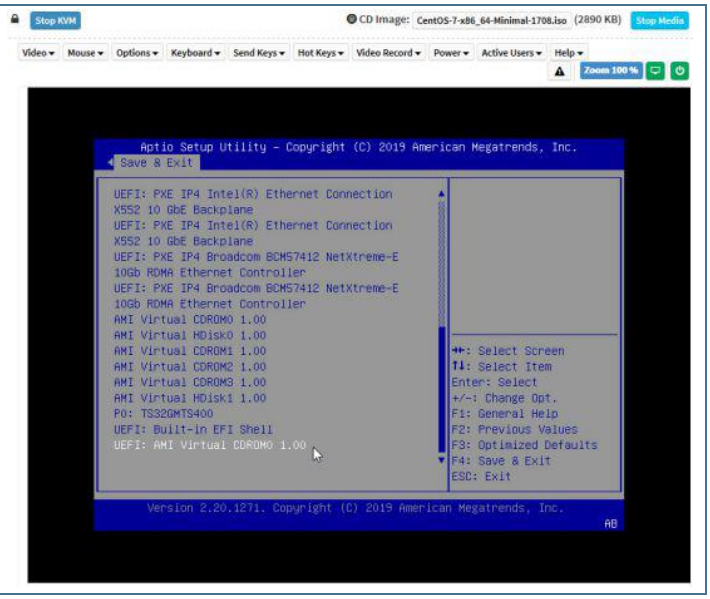
Étape_1	Dans la vue du KVM de l'écran du serveur, cliquer sur **Browse File** en haut à droite de l'écran. Sélectionner le fichier ISO à monter et cliquer sur **Open**.	
Étape_2	Une fois le fichier ISO chargé, cliquer sur **Start Media** en haut à droite de l'écran. **NOTE :** Une fois cliqué, le bouton Start Media devient le bouton **Stop Media**.	

9.2.3.1.4. Accéder au menu de configuration du BIOS

Étape_1	Dans le menu déroulant **Power**, sélectionner **Reset Server** pour accéder au menu BIOS. Cliquer sur **OK** pour confirmer l'opération. **NOTE :** Lorsqu'une commande de réinitialisation du serveur est lancée, quelques secondes peuvent s'écouler avant que l'écran d'accueil du BIOS ne s'affiche.	

Étape_2	Lorsque l'écran d'accueil du BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration du BIOS. **NOTE :** Il peut s'écouler quelques secondes avant que l'écran d'accueil du BIOS n'affiche le message de confirmation "Entering Setup…". **Conseil :** Certains utilisateurs appuient plusieurs fois et très rapidement sur Échap/F2 (DEL/F2) pour s'assurer que le serveur attrape la touche et entre dans le menu de configuration du BIOS. Cela peut entraîner l'affichage du message suivant sur l'écran du KVM : **HID Queue is about to get full. Kindly hold on a second(s)...** Kontron suggère de modifier le paramètre **Setup Prompt Timeout** pour donner aux utilisateurs plus de temps pour réagir. Maintenir l'attention (monotâche) sur la fenêtre KVM est également une bonne pratique pour entrer dans le menu de configuration du BIOS chaque fois que c'est nécessaire. Le paramètre **Setup Prompt Timeout** se trouve dans l'onglet **Boot** du menu de configuration du BIOS. La valeur par défaut est de 1 seconde. La changer pour une valeur comprise entre 3 et 10 secondes constitue une bonne cible.	
Étape_3	L'écran d'accueil du BIOS affiche **"Entering Setup..."**. NOTE : L'affichage et l'entrée dans le menu de configuration du BIOS prendront quelques secondes.	
Étape_4	Le menu de configuration du BIOS s'affiche.	

9.2.3.1.5. Sélectionner l'ordre de démarrage dans le menu Boot Override

Étape_1	Dans le menu de configuration du BIOS et à l'aide des flèches du clavier, sélectionner le menu **Save & Exit**. Dans la section **Boot Override**, sélectionner **UEFI: AMI Virtual CDROM0 1.00** et appuyer sur **Entrée**. Le serveur redémarrera et la procédure d'installation des supports démarrera.	

> Vous avez maintenant tout ce qu'il faut pour terminer l'installation du système d'exploitation en fonction des exigences de votre application.

9.2.3.1.6. Compléter l'installation du système d'exploitation

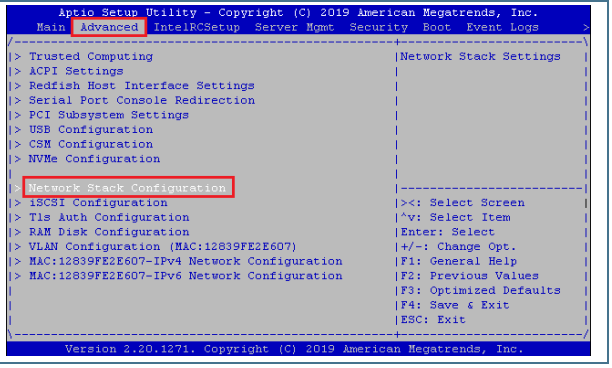
Étape_1	Terminer l'installation en suivant les invites à l'écran du système d'exploitation installé.

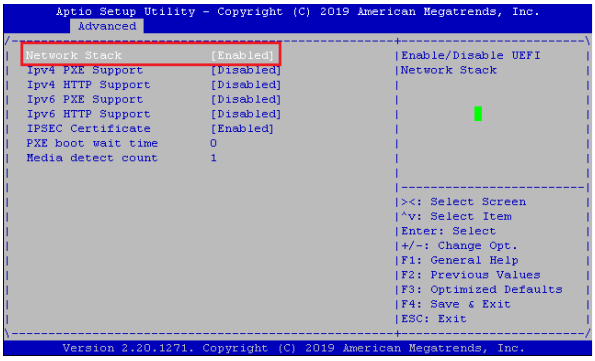
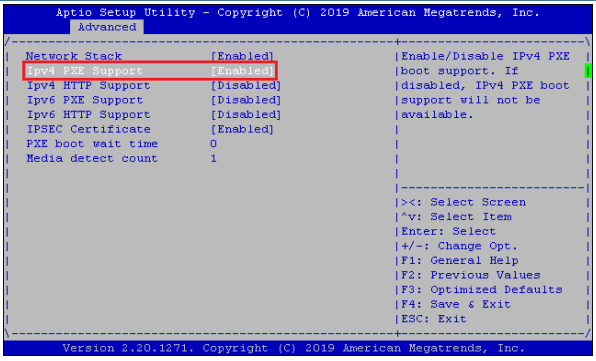
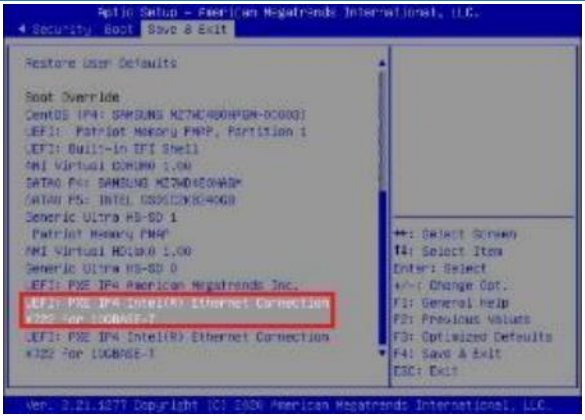
9.2.3.2. Installer un système d'exploitation sur un serveur en utilisant PXE (Boot from LAN)

Section pertinente :

Accéder au BIOS

NOTE : L'utilisation de la fonctionnalité Boot from LAN nécessite une infrastructure de serveur PXE.

Étape_1	Accéder au menu BIOS. Voir la section Accéder au BIOS.	
Étape_2	Sélectionner l'onglet **Advanced**, puis le sous-menu **Network Stack Configuration**.	

Étape_3	Mettre **Network Stack** à **Enabled**.	
Étape_4	Selon l'application, mettre **IPv4 PXE Support** ou **IPv6 PXE Support** à **Enabled**.	
Étape_5	Redémarrer le système et accéder à nouveau au menu de configuration du BIOS.	
Étape_6	Naviguer jusqu'au menu **Save & Exit** et ensuite jusqu'à la section **Boot Override**.	
Étape_7	Choisir l'option PXE souhaitée.	

> Vous avez maintenant tout ce qu'il faut pour terminer l'installation du système d'exploitation en fonction des exigences de votre application.

9.2.3.2.1. Compléter l'installation du système d'exploitation

Étape_1	Terminer l'installation en suivant les invites à l'écran du système d'exploitation installé.

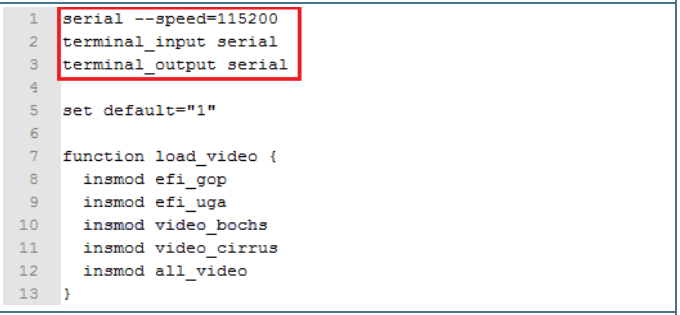
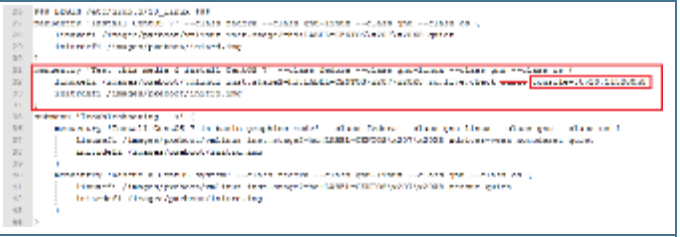
9.2.3.3. Installer un système d'exploitation sur un serveur en utilisant une unité de stockage USB

Sections pertinentes :

Accéder au BIOS

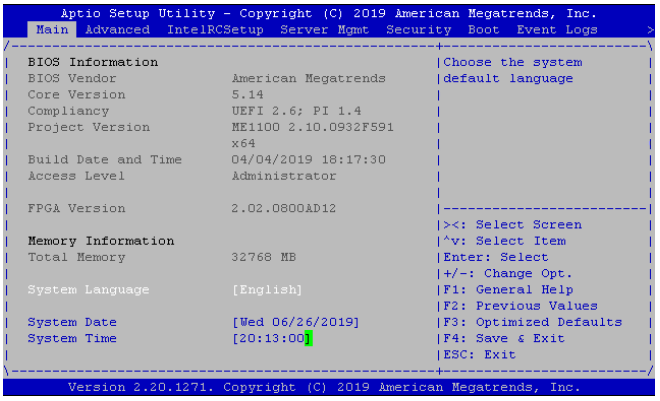
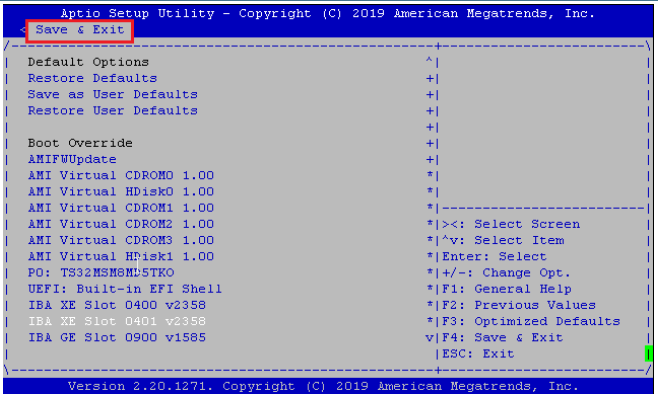
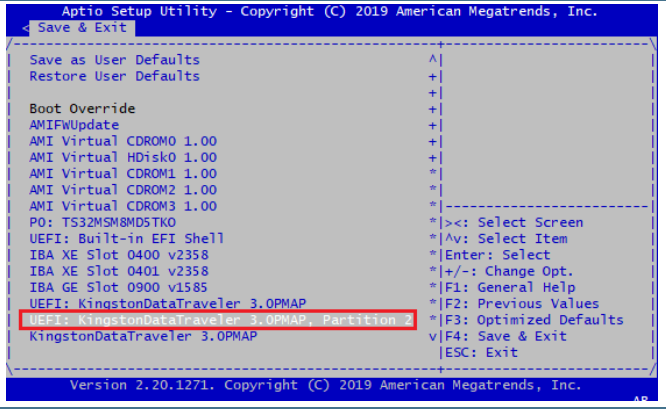
Gestion de l'alimentation de la plateforme

9.2.3.3.1. Préparer l'unité de stockage USB

Étape_1	Créer une clé USB amorçable avec le logiciel approprié. **NOTE :** RUFUS est recommandé.	
Étape_2	Ouvrir le répertoire USB sur un ordinateur distant.	
Étape_3	Naviguer jusqu'à EFI > BOOT (ex. E:/EFI/BOOT/).	
Étape_4	Ouvrir le fichier grub.cfg avec n'importe quel éditeur de texte.	
Étape_5	Modifier le fichier en ajoutant les lignes suivantes en haut pour activer l'installation série : serial --speed=115200 terminal_input serial terminal_output serial	
Étape_6	Dans la ligne « **Test this media & install CentOS 7** », remplacer l'argument « **quiet** » par « **console=ttyS0,115200n81** ».	
Étape_7	Enregistrer le fichier et éjecter la clé USB.	

9.2.3.3.2. Configurer Boot Override

Étape_1	Connecter l'unité de stockage USB à la plateforme.
Étape_2	Démarrer la plateforme. Voir la section Gestion de l'alimentation de la plateforme.

Étape_3	Accéder au menu de configuration du BIOS. Voir la section Accéder au BIOS.	
Étape_4	Naviguer jusqu'au menu **Save & Exit** et ensuite jusqu'à la section **Boot Override**.	
Étape_5	Choisir votre unité de stockage USB. **NOTE :** L'unité de stockage USB doit être nommée comme suit : « **UEFI : monNomUSB, Partition X** ».	

> Vous avez maintenant tout ce qu'il faut pour terminer l'installation du système d'exploitation en fonction des exigences de votre application.

9.2.3.3.3. Compléter l'installation du système d'exploitation

Étape_1	Terminer l'installation en suivant les invites à l'écran du système d'exploitation installé.

9.2.3.4. Installer un système d'exploitation hérité

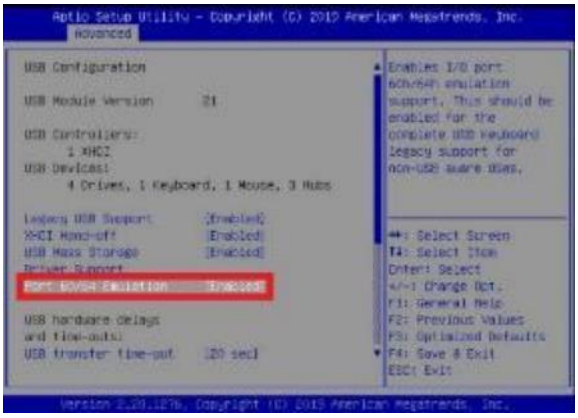
9.2.3.4.1. Installer RHEL/Cent OS 7.3 et se préparer à l'installation du pilote AST

9.2.3.4.1.1. Préalables

1	Une image de RHEL/CentOS 7.3 (ou une version inférieure) est disponible sur le support d'installation.

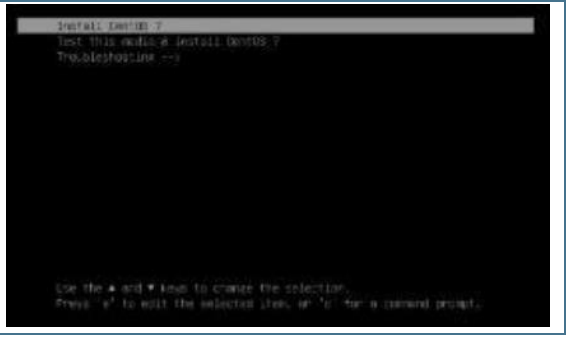
9.2.3.4.1.2. Activer le clavier USB pour une utilisation dans le chargeur d'amorçage en mode hérité (legacy)

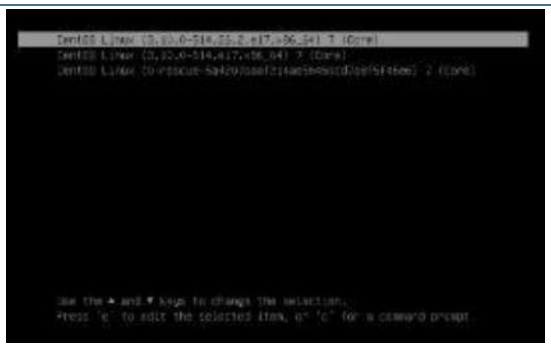
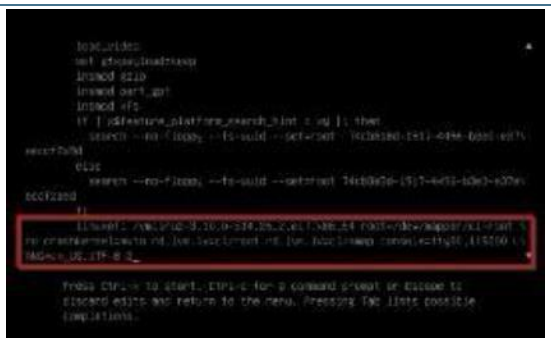
Voir Accéder au BIOS pour les instructions d'accès.

Étape_1	Dans le menu de configuration du BIOS, sélectionner le menu **Advanced** et naviguer à la section **USB Configuration**. Mettre **Port 60/64 Emulation** à **Enabled**.	
Étape_2	Appuyer sur **F4** pour enregistrer et quitter.	

9.2.3.4.1.3. Installer RHEL/Cent OS 7.3 et se préparer à l'installation du pilote AST

La procédure décrite ci-dessous s'applique aux versions 7.3 ou inférieures.

Étape_1	Démarrer à partir du support d'installation choisi.	
Étape_2	Modifier l'option de démarrage : (UEFI) Appuyer sur « **Tab** » pour modifier l'option d'installation en mode UEFI. **OU** (Hérité) Appuyer sur « **e** » pour modifier l'option d'installation en mode hérité.	

Étape_3	Ajouter un paramètre (**modprobe.blacklist=ast**) dans la ligne de commande affichée comme montré dans l'image. Le paramètre est inséré avant le paramètre « quiet » à la fin de la ligne « **linuxefi** ».	
Étape_4	Lancer l'installation du système d'exploitation en appuyant sur **Ctrl+X** ou **F10**.	
Étape_5	Le serveur redémarre une fois l'installation terminée. Pendant le démarrage, appuyer sur « **Tab** » en mode UEFI ou sur « **e** » en mode hérité pour modifier l'élément sélectionné.	
Étape_6	Ajouter le chiffre « **2** » à la fin de la ligne qui commence par « **linuxefi** » en mode UEFI ou « linux16 » en mode hérité. NOTE : Cette modification est nécessaire pour démarrer le système en « **runlevel 2** » pour l'installation du pilote AST.	
Étape_7	Appuyer sur **Ctrl+X** ou **F10** pour démarrer le système d'exploitation.	

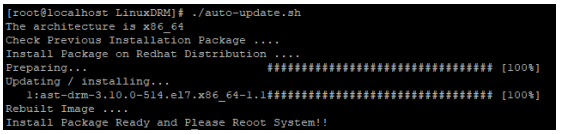
9.2.3.4.2. Installer le pilote AST

Liens pertinents :

L'ensemble de pilotes peut être téléchargé au https://www.aspeedtech.com/support.php .

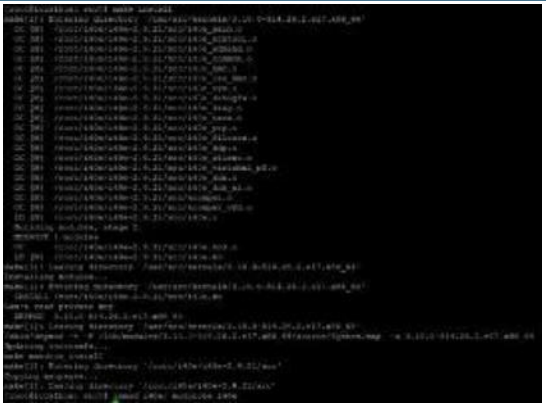
La version de l'ensemble de pilotes utilisé dans cette procédure est la suivante : https://upload.aspeedtech.com/BIOS/v11003_linux.zipx.

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur (via SSH, RDP, etc.), entrer la commande pour télécharger et copier l'ensemble de pilotes. InviteSE_ServeurLocal:~# **wget** https://downloadmirror.intel.com/29072/eng/ASPEED_v11003_linux.zip
Étape_2	Extraire le contenu. InviteSE_ServeurLocal:~# **unzip ASPEED_v11003_linux.zip**
Étape_3	Changer de répertoire. InviteSE_ServeurLocal:~# **cd LinuxDRM/**
Étape_4	Extraire le contenu. InviteSE_ServeurLocal:~# **tar xvzf lxdrm.tar.gz**

Étape_5	Installer le pilote. InviteSE_ServeurLocal:~# **./auto-update.sh**	
Étape_6	Redémarrer la plateforme. InviteSE_ServeurLocal:~# **reboot**	
Étape_7	(Optionnel) Si la version du noyau n'est pas 3.10.0-514.el7.x86_64, il est possible que le message d'erreur suivant s'affiche : *The kernel version is not in RPMs support list, Please try SRPMS instead!!* Ce problème est dû au résultat de la commande uname -r, qui ne correspond pas à 100 % à la structure des noms de fichiers du pilote AST. Il est possible de modifier le script ou le nom du fichier. InviteSE_ServeurLocal:~# **uname -r** 3.10.0-514.26.2.el7.x86_64 InviteSE_ServeurLocal:~# **sed -e "s/kver=\`uname -r\`/kver=\`uname -r | sed 's\/26.2.\/\/'\`/" ./auto-update.sh**	
Étape_8	(Optionnel) Après avoir mis à jour le fichier auto-update avec le bon noyau, faire la mise à jour. InviteSE_ServeurLocal:~# **./auto-update.sh**	

9.2.3.4.3. Installer le pilote réseau dans RHEL/CentOS 7.3

Le pilote réseau i40e doit être installé pour les ports 10GbE.

Étape_1	Télécharger la plus récente version du pilote i40e à partir de Sourceforge. InviteSE_ServeurLocal:~# **wget -nc --random-file /root/.bashrc --content-disposition** http://sourceforge.net/projects/e1000/files/i40e%20stable/2.9.21/i40e-2.9.21.tar.gz/download	
Étape_2	Extraire le contenu du fichier tar. InviteSE_ServeurLocal:~# **tar xvzf i40e-2.9.21.tar.gz**	
Étape_3	Installer les outils de la version. InviteSE_ServeurLocal:~# **yum groupinstall 'Development Tools' -y**	
Étape_4	Changer de répertoire. InviteSE_ServeurLocal:~# **cd ./i40e-2.9.21/src**	
Étape_5	Compiler la source. InviteSE_ServeurLocal:~# **make** InviteSE_ServeurLocal:~# **make install**	
Étape_6	Supprimer l'ancienne version du pilote et charger la nouvelle. InviteSE_ServeurLocal:~# **rmmod i40e** InviteSE_ServeurLocal:~# **modprobe i40e**	

9.2.3.4.4. Empêcher yum de mettre à niveau le noyau dans RHEL/CentOS 7.3

Étape_1	Si vous n'avez pas de source locale/répertoire local disponible et que vous devez empêcher yum d'installer/mettre à niveau la dernière version du noyau. **#! /bin/bash** **mkdir /etc/yum.repos.d/.disabled** **mv /etc/yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/.disabled/** **cat <<EOT >> /etc/yum.repos.d/CentOS-7.3.repo** **[base-7.3]** **name=CentOS-7.3 – Base** **baseurl=http://vault.centos.org/centos/7.3.1611/os/\$basearch/** **gpgcheck=1** **gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7** **[updates-7.3]** **name=CentOS-7.3 - Updates baseurl=http://vault.centos.org/centos/7.3.1611/updates/\$basearch/** **gpgcheck=1** **gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7** **EOT** **yum repolist** **yum clean all** **rm -rf /var/cache/yum yum update** **cat /etc/centos-release**

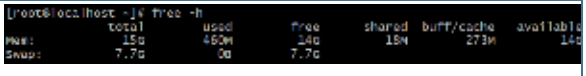
9.2.4. Vérification de l'installation

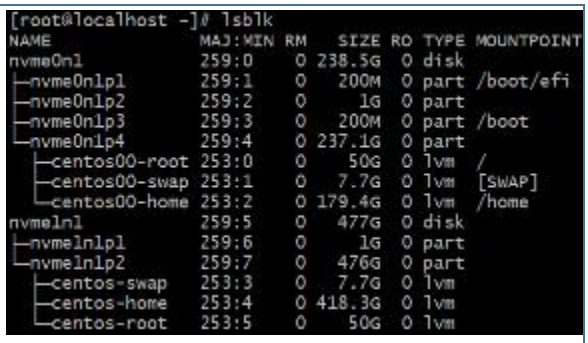
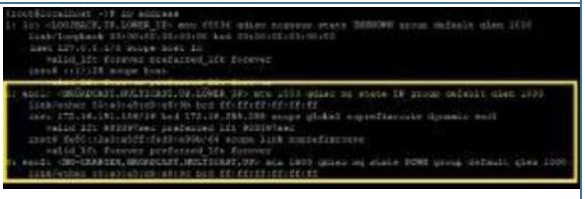
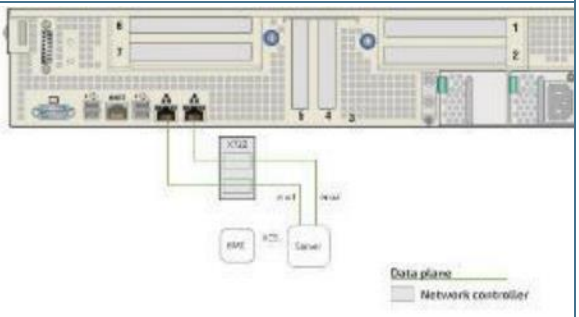
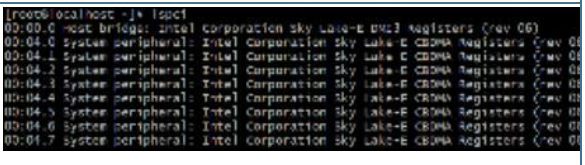
Sections pertinentes :

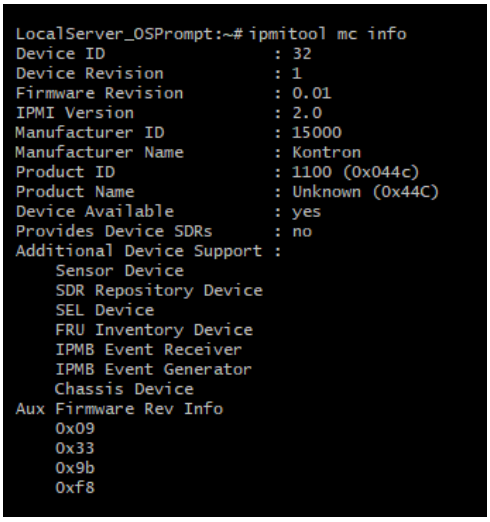
Mappage PCI

Installation des logiciels courants

Tous les résultats et toutes les commandes peuvent varier en fonction du système d'exploitation et des périphériques ajoutés.

Étape_1	Redémarrer le système d'exploitation comme recommandé, puis accéder à l'invite de commande du système d'exploitation.	
Étape_2	Vérifier qu'aucun message d'erreur ou d'avertissement n'est affiché dans **dmesg** à l'aide des commandes suivantes. InviteSE_ServeurLocal:~# **dmesg | grep -i fail** InviteSE_ServeurLocal:~# **dmesg | grep -i Error** InviteSE_ServeurLocal:~# **dmesg | grep -i Warning** InviteSE_ServeurLocal:~# **dmesg | grep -i "Call trace"** **NOTE :** Si des messages ou des avertissements s'affichent, consulter la documentation du système d'exploitation pour y remédier.	
Étape_3	Vérifier que les modules DIMM sont détectés. InviteSE_ServeurLocal:~# **free -h**	

Étape_4	Vérifier que toutes les unités de stockage sont détectées. InviteSE_ServeurLocal:~# **lsblk**	
Étape_5	Confirmer que les contrôleurs d'interfaces réseau du plan des données sont chargés par le pilote i40e. InviteSE_ServeurLocal:~# **dmesg | grep i40e** **NOTE :** Deux CIR 10GbE devraient être découverts.	
Étape_6	Confirmer que toutes les interfaces réseau sont détectées. InviteSE_ServeurLocal:~# **ip address** **NOTE :** Deux interfaces réseau devraient être détectées.	
Étape_7	Configurer les contrôleurs d'interfaces réseau en fonction de vos exigences. **NOTE :** Les noms des interfaces pourraient différer selon le système d'exploitation installé. Cependant, les paramètres « Bus:Device.Function » restent les mêmes pour l'interface, quel que soit le système d'exploitation.	
Étape_8	Installer **ipmitool** et **pciutils** à l'aide du gestionnaire de paquets et mettre à jour les paquets du système d'exploitation. La version recommandée d'ipmitool est la 1.8.18. Exemple : InviteSE_ServeurLocal:~# **yum update** InviteSE_ServeurLocal:~# **yum install ipmitool** InviteSE_ServeurLocal:~# **yum install pciutils** **NOTE :** La mise à jour des paquets peut prendre quelques minutes.	
Étape_9	(Optionnel) Si des cartes d'expansion PCIe ou d'autres composants matériels sont installés, vérifier qu'ils sont détectés. InviteSE_ServeurLocal:~# **lspci | grep [MOT-CLÉ]** **NOTE :** Le mot-clé est un mot unique qui permet d'identifier le composant matériel. Le Mappage PCI du produit pourrait aider avec cette validation.	

Étape_10	Vérifier la communication entre le système d'exploitation et le BMC. InviteSE_ServeurLocal:~# **ipmitool mc info**	

9.2.5. Installation des logiciels courants

Les commandes peuvent varier en fonction du système d'exploitation et du gestionnaire de paquets.

Certains outils pourraient ne pas être nécessaires selon les fonctionnalités prises en charge par la plateforme.

9.2.5.1. Outils logiciels requis

Outil	Description	Installation
ipmitool	Utilitaire IPMI pour contrôler et surveiller des périphériques via les interfaces IPMI de la plateforme.	À partir d'une invite de commande : InviteSE_ServeurLocal# **sudo apt install ipmitool**
pciutils	Outil utilisé pour gérer les cartes PCIe connectées à la plateforme	À partir d'une invite de commande : InviteSE_ServeurLocal# **sudo apt install pciutils**
hdparm	Programme de ligne de commande pour Linux	À partir d'une invite de commande : InviteSE_ServeurLocal# **sudo apt install hdparm**
nvme-cli	Outils en espace utilisateur (userspace) pour contrôler les disques NVMe	À partir d'une invite de commande : InviteSE_ServeurLocal# **sudo apt install nvme-cli**
snmpd	Démon SNMP	À partir d'une invite de commande : InviteSE_ServeurLocal:~# **yum install ./ kontron-snmp-agent-1.2.2-1.x86_64.rpm**
ksnmpd	Sous-agent Linux de Kontron.	NOTE : Ce logiciel est fourni par Kontron.
snmp	Paquet par défaut Net-SNMP.	À partir d'une invite de commande : InviteSE_OrdinateurDistant:~# **yum install snmp**
snmp-mibs-downloader	Outil utilisé pour installer et gérer les fichiers MIB (base d'information de gestion)	À partir d'une invite de commande : InviteSE_OrdinateurDistant:~# **yum install snmp-mibs-downloader**

9.2.5.2. Outils logiciels recommandés

Outil	Description
PuTTY	Outil de console série recommandé dans la documentation
jq	Outil de ligne de commande utilisé pour analyser les données JSON brutes afin de rendre la réponse de l'API Redfish lisible en clair.
cURL	Outil client HTTP/FTP utilisé pour naviguer dans l'API Web à l'aide d'un outil de ligne de commande.
Extension de navigateur pour interpréter JSON (JSON viewer)	Si l'API Redfish est utilisée via un navigateur Internet, il est recommandé d'utiliser JSON viewer pour rendre le résultat lisible en clair

9.2.5.3. Outils logiciels propres aux produits

Outil	Description	Installation
net-snmp-utils	Ensemble d'utilitaires SNMP	À partir d'une invite de commande : InviteSE_ServeurLocal:~# **yum install wget unzip net-snmp- utils net-snmp**

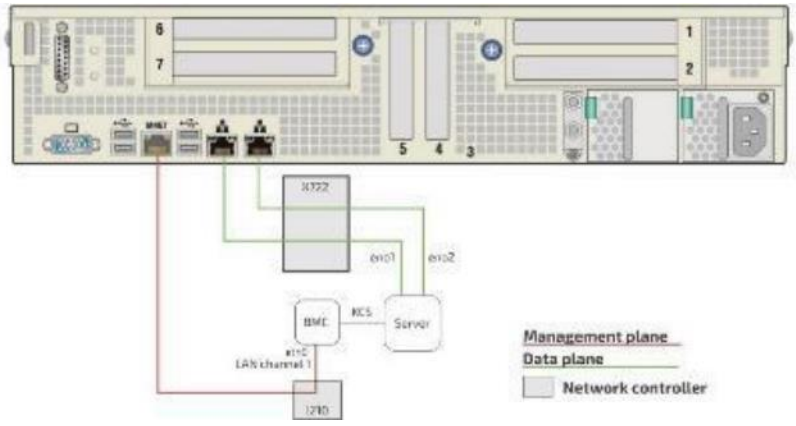
10/ Configuration

10.1. Configuration des méthodes d'accès au système

10.1.1. Considérations générales et avertissements concernant la configuration du réseau

L'architecture de la plateforme CG2400 offre de nombreux points d'entrée, y compris un canal LAN vers le BMC.

Faites preuve de prudence lors de la configuration des accès au réseau. Votre accès au système pourrait être interrompu si vous désactivez le point d'accès par lequel vous êtes entré. Par exemple, si vous accédez au canal LAN 1 du BMC via IOL pour désactiver IOL sur le canal LAN 1, votre connexion sera interrompue et vous vous serez bloqué l'accès au BMC puisque le seul canal LAN sera désormais désactivé. Pour accéder au BMC, il faut établir une connexion à un système d'exploitation sur le serveur et utiliser KCS pour réactiver l'accès LAN.



10.1.2. Désactiver IOL sur un canal LAN

Les procédures décrites ci-dessous doivent être effectuées pour une interface à la fois. Si l'application nécessite plusieurs interfaces, les configurer séparément. Sur un canal LAN, IOL peut être désactivé :

- En utilisant IPMI

NOTE : Il n'est actuellement pas possible de désactiver un canal LAN à l'aide du menu de configuration du BIOS.

10.1.2.1. Désactiver IOL sur un canal LAN en utilisant IPMI

10.1.2.1.1. Accéder au BMC

Le BMC est accessible par deux méthodes IPMI.

- Si un système d'exploitation est installé (adresse IP du BMC connue ou non), IPMI via KCS peut être utilisé. Voir Accéder au BMC en utilisant IPMI via KCS.
- Si l'adresse IP du BMC est connue (système d'exploitation installé ou non), IPMI sur LAN peut être utilisé. Voir Accéder au BMC en utilisant IPMI sur LAN (IOL).

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL. Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

10.1.2.1.2. Désactiver IOL sur un canal LAN

NOTE : Le canal LAN 1 correspond au port MNGT du CIR.

Étape_1	Désactiver l'accès LAN. InviteSE_ServeurLocal:~# **ipmitool lan set [CANAL_LAN] access off**	`[root@localhost ~]# ipmitool lan set 1 access off` `Set Channel Access for channel 1 was successful.`

10.1.3. Activer IOL sur un canal LAN

Les procédures décrites ci-dessous doivent être effectuées pour une interface à la fois. Si l'application nécessite plusieurs interfaces, les configurer séparément. Sur un canal LAN, IOL peut être activé :

- En utilisant IPMI

NOTE : Il n'est actuellement pas possible d'activer un canal LAN à l'aide du menu de configuration du BIOS.

10.1.3.1. Activer IOL sur un canal LAN en utilisant IPMI

10.1.3.1.1. Accéder au BMC

Le BMC est accessible par deux méthodes IPMI.

- Si un système d'exploitation est installé (adresse IP du BMC connue ou non), IPMI via KCS peut être utilisé. Voir Accéder au BMC en utilisant IPMI via KCS.
- Si l'adresse IP du BMC est connue (système d'exploitation installé ou non), IPMI sur LAN peut être utilisé. Voir **Erreur! Source du renvoi introuvable.**.

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL. Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

10.1.3.1.2. Activer IOL sur un canal LAN

NOTE : Le canal LAN 1 correspond au port MNGT du CIR.

Étape_1	Activer l'accès LAN. InviteSE_ServeurLocal:~# **ipmitool lan set [CANAL_LAN] access on**	`[root@localhost ~]# ipmitool lan set 1 access on` `Set Channel Access for channel 1 was successful.`

10.1.4. Configurer les paramètres série sur LAN en utilisant IPMI

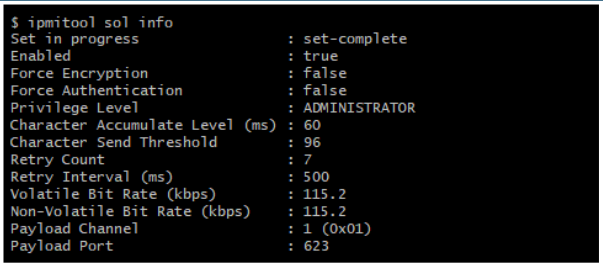
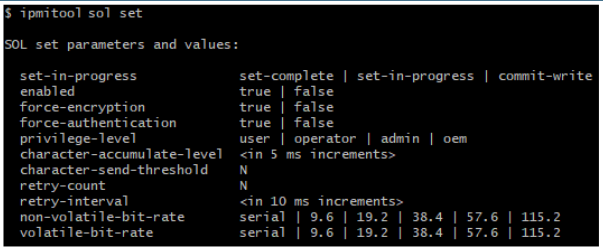
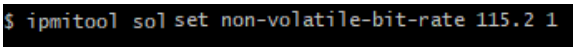
10.1.4.1. Accéder au BMC

Le BMC est accessible par deux méthodes IPMI.

- Si un système d'exploitation est installé (adresse IP du BMC connue ou non), IPMI via KCS peut être utilisé. Voir Accéder au BMC en utilisant IPMI via KCS.
- Si l'adresse IP du BMC est connue (système d'exploitation installé ou non), IPMI sur LAN peut être utilisé. Voir **Erreur! Source du renvoi introuvable.**.

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL. Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

10.1.4.2. Visualiser et configurer les paramètres SOL

Étape_1	Afficher des paramètres SOL. InviteSE_ServeurLocal:~# **ipmitool sol info**	
Étape_2	Afficher les paramètres SOL configurables. InviteSE_ServeurLocal:~# **ipmitool sol set**	
Étape_3	Définir les paramètres souhaités. InviteSE_ServeurLocal:~# **ipmitool sol set [PARAMÈTRE] [VALEUR_PARAMÈTRE] [CANAL_LAN]**	

10.1.5. Créer l'URL racine Redfish

10.1.5.1. Préalables

1	L'adresse IP du BMC est connue (voir la section Configuration > Contrôleur de gestion de carte mère – BMC pour obtenir le paramètre IP_GESTION_BMC).
2	Un outil client HTTP est installé sur l'ordinateur distant.
3	Un outil de ligne de commande pour analyser le JSON, tel que jq, est installé.

Sections pertinentes :

Contrôleur de gestion de carte mère – BMC

Installation des logiciels courants

Noms d'utilisateur et mots de passe par défaut

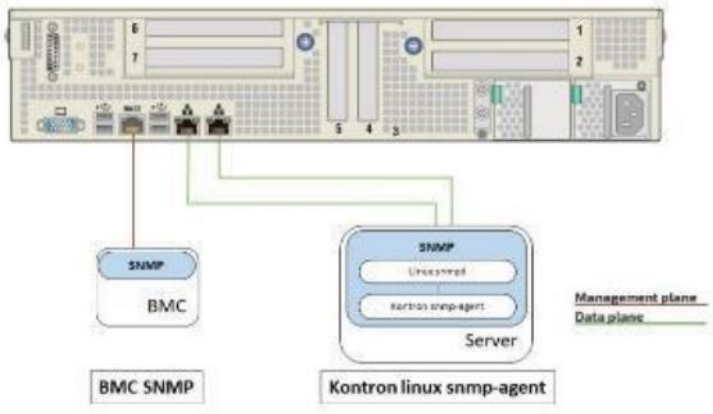
10.1.5.2. Procédure

Étape_1	Commencer l'URL par le préfixe https.	https://
Étape_2	Ajouter le nom d'utilisateur et le mot de passe Redfish, séparés par le deux-points.	https://Administrator:superuser
Étape_3	Ajouter **@** à l'URL puis l'adresse IP de gestion du BMC.	https://Administrator:superuser@172.16.205.245
Étape_4	Ajouter le suffixe de l'API Redfish à l'URL.	https://Administrator:superuser@172.16.205.245/redfish/v1

Étape_5	Accéder à l'API à l'aide d'un client HTTP et vérifier que l'URL est valide.	$ curl -k -s https://Administrator:superus$er@172.16.205.245/redfish/v1/ {"@odata.context":"/redfish/v1/$metadata#ServiceRoot.ServiceRoot","@odata.etag": "W/\"1563368478\"","@odata.id":"/redfish/v1/","@odata.type":"#ServiceRoot.v1_2_0 .ServiceRoot","AccountService":{"@odata.id":"/redfish/v1/AccountService"},"Chass is":{"@odata.id":"/redfish/v1/Chassis"},"CompositionService":{"@odata.id":"/redf ish/v1/CompositionService"},"Description":"The service root for all Redfish requ ests on this host","EventService":{"@odata.id":"/redfish/v1/EventService"},"Id": "RootService","JsonSchemas":{"@odata.id":"/redfish/v1/JsonSchemas"},"Links":{"Se ssions":{"@odata.id":"/redfish/v1/SessionService/Sessions"}},"Managers":{"@odata .id":"/redfish/v1/Managers"},"Name":"Root Service","Oem":{"Ami":{"@odata.type":" AMIServiceRoot.v1_0_0.AMIServiceRoot","Configurations":{"@odata.id":"/redfish/v1 /configurations"},"RtpVersion":"1.2.1"},"Dre":{"@odata.type":"#AMIDynamicExtensi on.v1_0_0.AMIDynamicExtension","DynamicExtension":{"@odata.id":"/redfish/v1/Dyna micExtension"}}},"RedfishVersion":"1.2.1","Registries":{"@odata.id":"/redfish/v1 /Registries"},"SessionService":{"@odata.id":"/redfish/v1/SessionService"},"Syste ms":{"@odata.id":"/redfish/v1/Systems"},"Tasks":{"@odata.id":"/redfish/v1/TaskSe rvice"},"TelemetryService":{"@odata.id":"/redfish/v1/TelemetryService"},"UUID":" 00a0a5d6-332a-c503-0010-debfa0af8f6b","UpdateService":{"@odata.id":"/redfish/v1/ UpdateService"}}

* Lorsqu'il est requis de changer le mot de passe par défaut, utiliser la commande : curl -u Administrator:superuser -X PATCH -k -H 'Content-Type: application/json' -H 'If-Match: *' -i 'https://[IP_BMC]/redfish/v1/AccountService/Accounts/1' --data '{"Password": "superuser"}'

10.1.6. Configurer SNMP



10.1.6.1. Configurer le service SNMP pour le BMC

Avant de configurer SNMP, le nom d'utilisateur et le mot de passe par défaut doivent être modifiés, car un minimum de 8 caractères est requis pour chacun d'eux. Voir Configurer les noms d'utilisateur et mots de passe du BMC en utilisant l'interface utilisateur Web.

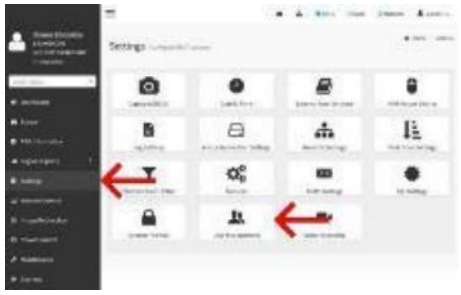
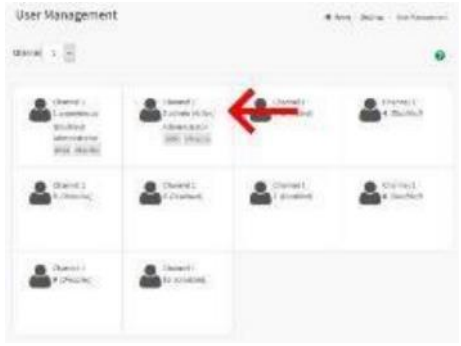
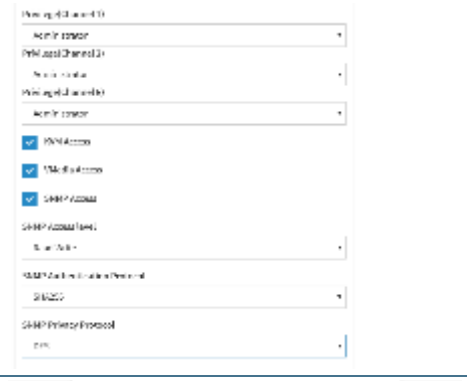
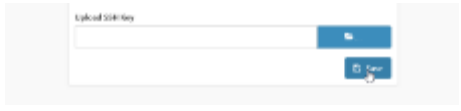
NOTE : La version actuelle prend en charge la version 3 du protocole SNMP. Pour que les commandes fonctionnent, la version 5.8 ou supérieure de snmpwalk doit être installée.

10.1.6.1.1. Activer SNMP pour un utilisateur utilisant l'interface utilisateur Web du BMC

Section pertinente :

Configuration et gestion des utilisateurs

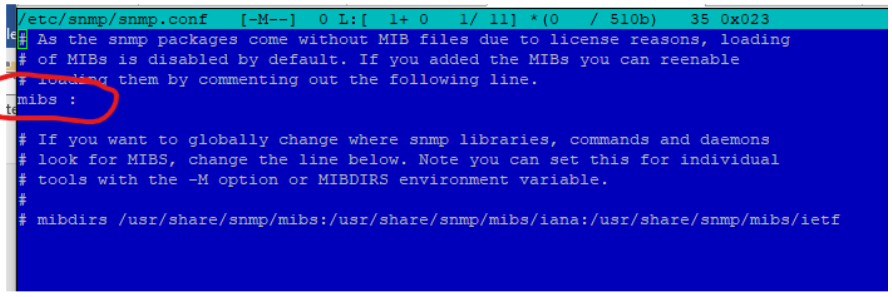
Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

Étape_1	Dans le menu de gauche, cliquer sur **Settings** puis sur **User Management**.	
Étape_2	Sélectionner l'utilisateur.	
Étape_3	Cocher la case **SNMP Access** pour donner à l'utilisateur un accès SNMP.	
Étape_4	Choisir le niveau d'accès dans le menu **SNMP Access Level**. **NOTE :** Une fois l'accès SNMP activé, la sécurité minimale du mot de passe augmente, et un minimum de 8 caractères est requis.	
Étape_5	Choisir le protocole d'authentification dans le menu **SNMP Authentification Protocol**.	
Étape_6	Choisir le protocole de confidentialité dans le menu **SNMP Privacy Protocol**.	
Étape_7	Cliquer sur **Save**.	

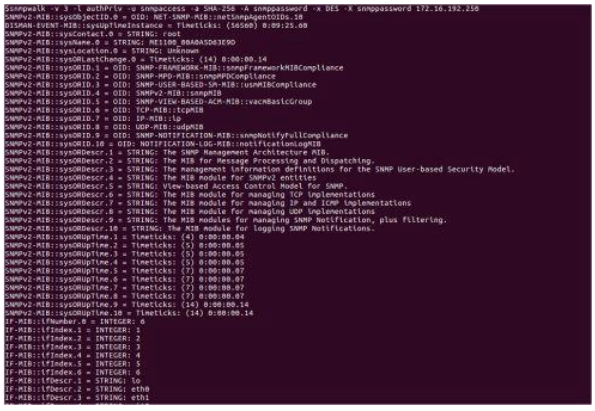
10.1.6.1.2. Installer SNMP sur un ordinateur distant

NOTE : Le gestionnaire de paquets pourrait varier en fonction du système d'exploitation installé.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, installer SNMP. InviteSE_OrdinateurDistant:~# **yum install snmp**

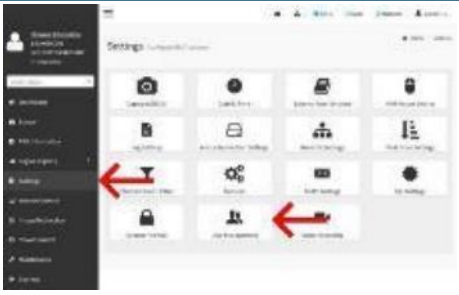
Étape_2	(Optionnel) Pour pouvoir voir la base d'information de gestion (MIB) lisible en clair (au lieu de voir l'identificateur d'objet [OID]), installer également snmp-mibs-downloader. InviteSE_OrdinateurDistant:~# **yum install snmp-mibs-downloader** Ensuite, pour configurer le CLI net-snmp afin d'utiliser la base d'information de gestion (MIB), éditer /etc/snmp/snmp.conf et commenter la ligne suivante : 

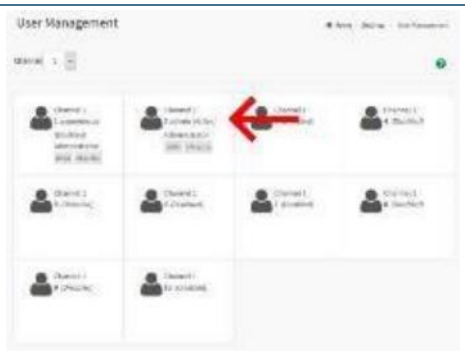
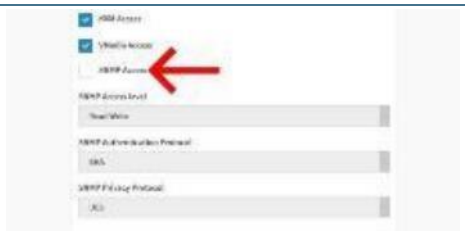
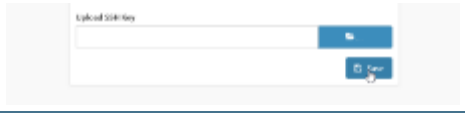
10.1.6.1.3. Vérifier la communication SNMP pour un utilisateur

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, vérifier que le BMC répond correctement à la requête SNMP. InviteSE_OrdinateurDistant:~# **snmpwalk -v 3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] - A [MOT_DE_PASSE_SNMP] -x [PROTOCOLE_PROTECTION] - X [MOT_DE_PASSE_SNMP] [IP_GESTION_BMC]**	

10.1.6.1.4. Désactiver un accès SNMP

Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

Étape_1	Accéder à l'interface utilisateur Web du BMC.	
Étape_2	Dans le menu de gauche, cliquer sur **Settings** puis sur **User Management**.	

Étape_3	Sélectionner l'utilisateur.	
Étape_4	Décocher la case **SNMP Access** pour désactiver l'accès SNMP de l'utilisateur sélectionné.	
Étape_5	Cliquer sur **Save**.	

10.1.6.2. Configurer l'agent SNMP (snmp-agent) de Kontron pour Linux

L'agent SNMP de Kontron pour Linux fonctionne uniquement avec les systèmes d'exploitation Red Hat/CentOS de Linux.

La procédure suivante sera effectuée sous CentOS. Les commandes peuvent varier en fonction du système d'exploitation installé.

10.1.6.2.1. Installer les outils logiciels requis

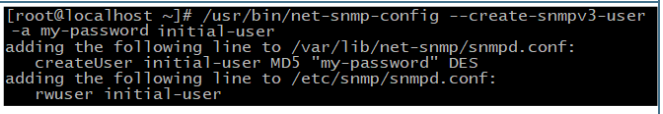
Voir Accéder au système d'exploitation d'un serveur pour les instructions d'accès.

Étape_1	Installer l'agent SNMP fourni par Kontron. InviteSE_ServeurLocal:~# **yum install ./ kontron-snmp-agent-1.2.2-1.x86_64.rpm**
Étape_2	Installer l'outil net-snmp-utils. InviteSE_ServeurLocal:~# **yum install net-snmp-utils**

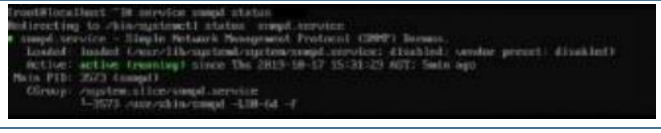
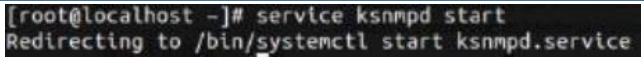
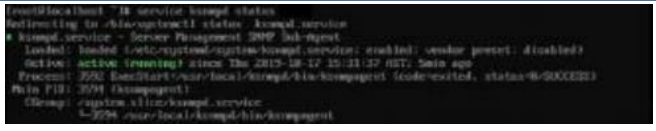
10.1.6.2.2. Configurer l'agent SNMP de Kontron pour Linux

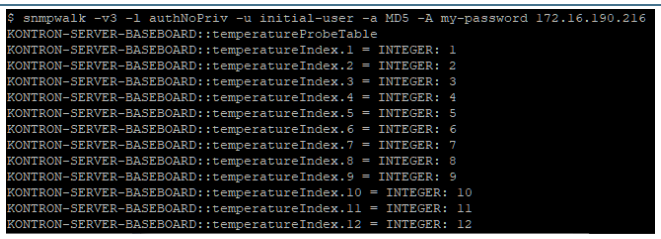
Cette procédure remplacera complètement toutes les configurations snmpd existantes stockées dans le fichier snmpd.conf. S'il y a des configurations snmpd existantes, il suffit d'ajouter les lignes de **rwcommunity** dans **authtrapenable** à la fin du fichier **snmpd.conf**.

Étape_1	Sauvegarder la configuration actuelle. InviteSE_ServeurLocal:~# **mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak**

Étape_2	Créer le fichier snmpd.conf avec la commande suivante : InviteSE_ServeurLocal:~# **nano /etc/snmp/snmpd.conf** L'éditeur nano s'ouvre. Copier le texte suivant : **rwcommunity public** **# Need to define default master agentx socket if net-snmp >=5.4 agentXSocket tcp:localhost:1705** **# turn on agentx master agent support master agentx** **# Enable TRAPs** **trap2sink localhost public** **authtrapenable 1**	
Étape_3	Définir les données d'accès par défaut. InviteSE_ServeurLocal:~# **/usr/bin/net-snmp-config --create-snmpv3-user - a [MOT_DE_PASSE] [NOM_UTILISATEUR]** **NOTE :** Le mot de passe doit comporter au moins 8 caractères. Exécuter la commande à nouveau supprime l'utilisateur précédent et le remplace par les nouvelles données d'accès. Cette méthode n'est pas recommandée pour créer et gérer des utilisateurs SNMP. Elle ne fait qu'initialiser les données d'accès par défaut et il est fortement recommandé de les modifier une fois que l'agent SNMP est opérationnel. Voir Configuration et gestion des utilisateurs pour plus d'instructions.	

10.1.6.2.3. Exécuter l'agent SNMP de Kontron pour Linux et vérifier l'installation et la configuration

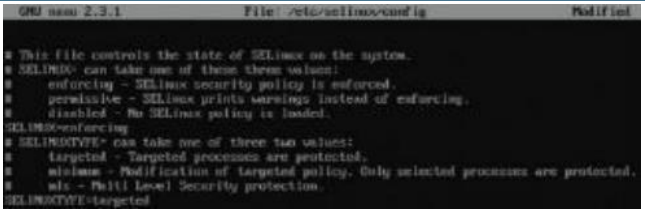
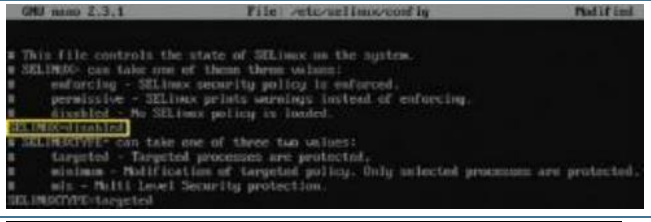
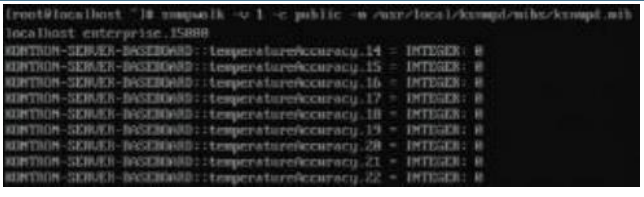
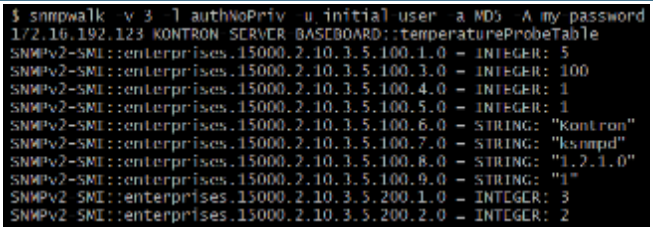
Étape_1	Exécuter snmpd. InviteSE_ServeurLocal:~# **service snmpd start**	
Étape_2	Vérifier que snmpd fonctionne correctement. InviteSE_ServeurLocal:~# **service snmpd status**	
Étape_3	(Optionnel) Si un ou plusieurs services posent problème, cela peut être dû au mécanisme de sécurité SELinux. Voir Désactiver SELinux pour plus d'instructions.	
Étape_4	Exécuter ksnmpd. InviteSE_ServeurLocal:~# **service ksnmpd start**	
Étape_5	Vérifier que ksnmpd fonctionne correctement. InviteSE_ServeurLocal:~# **service ksnmpd status**	

Étape_6	Vérifier que l'agent SNMP fonctionne correctement localement. InviteSE_ServeurLocal:~# **snmpwalk -v 1 -c public -m /usr/local/ksnmpd/mibs/ksnmpd.mib localhost [MIBS]**	
Étape_7	À partir d'un ordinateur distant ayant accès au réseau du serveur, vérifier que le serveur répond correctement à la requête SNMP. InviteSE_OrdinateurDistant:~# **snmpwalk -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] [IP_SERVEUR] [OID]**	

10.1.6.2.4. Désactiver SELinux

(Optionnel) Si un ou plusieurs services posent problème, cela peut être dû au mécanisme de sécurité SELinux (Security-Enhanced Linux) du système d'exploitation. Procéder à la procédure suivante pour résoudre le problème.

NOTE : Au lieu de désactiver complètement le mécanisme de sécurité, la configuration SELinux pourrait être modifiée pour activer SNMP sur les ports 1705, mais cela n'est pas documenté ici.

Étape_1	Ouvrir le fichier de configuration SELinux à l'aide d'un éditeur de texte. InviteSE_ServeurLocal:~# **nano /etc/selinux/config**	
Étape_2	Modifier le fichier en changeant le paramètre SELI UX en le mettant à **Disabled**.	
Étape_3	Enregistrer les modifications et redémarrer le système d'exploitation. InviteSE_ServeurLocal:~# **reboot**	
Étape_4	Ouvrir une session dans le système d'exploitation d'un serveur.	
Étape_5	Vérifier que l'agent SNMP fonctionne correctement localement. InviteSE_ServeurLocal:~# **snmpwalk -v 1 -c public -m /usr/local/ksnmpd/mibs/ksnmpd.mib localhost [MIBS]**	
Étape_6	À partir d'un ordinateur distant ayant accès au réseau du serveur, vérifier que le serveur répond correctement à la requête SNMP. InviteSE_OrdinateurDistant:~# **snmpwalk -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] [IP_SERVEUR] [OID]**	

10.2. Configuration et gestion des utilisateurs

10.2.1. Configurer les utilisateurs du BMC

Les droits d'administrateur sont nécessaires pour gérer les utilisateurs.

10.2.1.1. Configurer les noms d'utilisateur et mots de passe du BMC

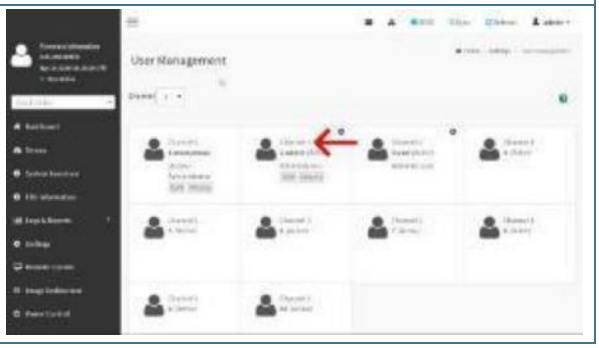
Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut. Les noms d'utilisateur et les mots de passe du BMC peuvent être gérés :

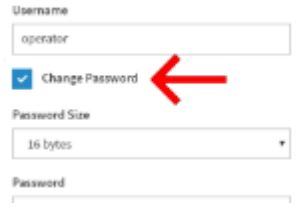
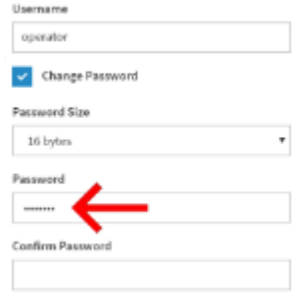
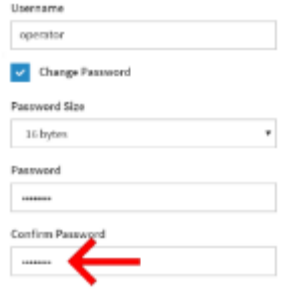
- En utilisant l'interface utilisateur Web
- En utilisant IPMI sur LAN (IOL)
- En utilisant IPMI via KCS

10.2.1.1.1. Configurer les noms d'utilisateur et mots de passe du BMC en utilisant l'interface utilisateur Web

Noter que le champ du mot de passe est obligatoire, qu'il doit comporter un minimum de 8 caractères et qu'il ne doit pas contenir de mots du dictionnaire. Il est recommandé, mais pas obligatoire, de saisir un mot de passe fort composé d'au moins une lettre majuscule, d'un caractère alphanumérique et d'un caractère spécial. Ne pas utiliser les symboles du code ASCII étendu, car ils ne sont pas gérés par l'outil IPMI.

Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

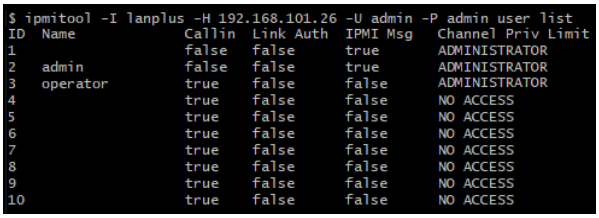
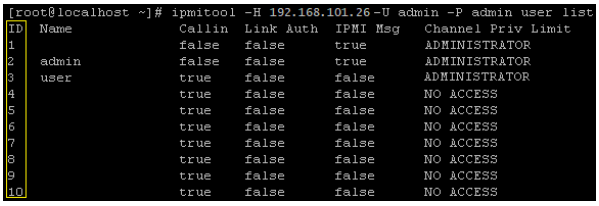
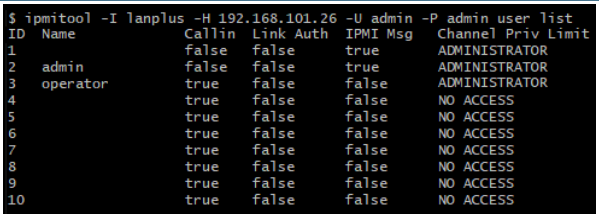
Étape_1	Cliquer sur **Settings** dans le menu de gauche puis cliquer sur **User Management**.	
Étape_2	Sélectionner l'utilisateur à gérer. **NOTE :** Le premier et le deuxième utilisateur sont des champs réservés, leurs noms d'utilisateur ne peuvent donc pas être modifiés.	

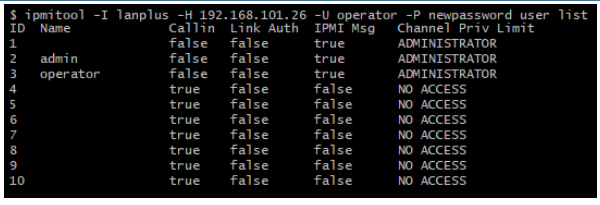
Étape_3	Modifier le champ **Username** si nécessaire.	
Étape_4	Cocher la case **Change Password**.	
Étape_5	Créer un nouveau mot de passe. **NOTE :** Il est recommandé, mais pas obligatoire, de saisir un mot de passe fort composé d'au moins une lettre majuscule, d'un caractère alphanumérique et d'un caractère spécial. Ne pas utiliser les symboles du code ASCII étendu, car ils ne sont pas gérés par l'outil IPMI. Noter que le champ du mot de passe est obligatoire et qu'il doit comporter un minimum de 8 caractères lorsque le service SNMP est activé.	
Étape_6	Confirmer le mot de passe.	
Étape_7	Cliquer sur **Save**.	

10.2.1.1.2. Configurer les noms d'utilisateur et mots de passe du BMC en utilisant IPMI sur LAN (IOL)

Noter que le champ du mot de passe est obligatoire, qu'il doit comporter un minimum de 8 caractères et qu'il ne doit pas contenir de mots du dictionnaire. Il est recommandé, mais pas obligatoire, de saisir un mot de passe fort composé d'au moins une lettre majuscule, d'un caractère alphanumérique et d'un caractère spécial. Ne pas utiliser les symboles du code ASCII étendu, car ils ne sont pas gérés par l'outil IPMI.

Voir Accéder au BMC en utilisant IPMI sur LAN (IOL) pour les instructions d'accès.

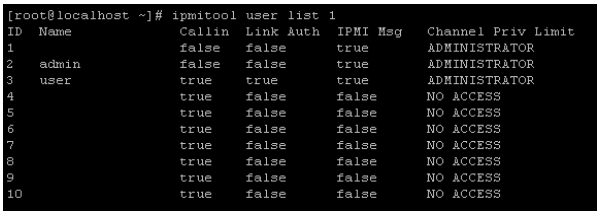
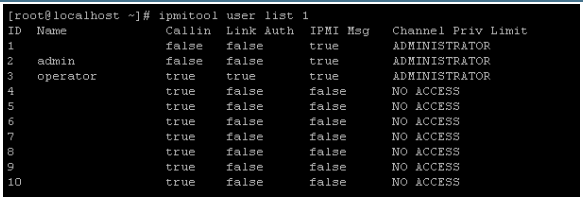
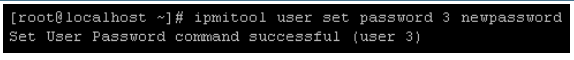
Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, afficher la liste des utilisateurs du BMC. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] user list**	
Étape_2	Identifier le numéro d'identification de l'utilisateur à modifier.	
Étape_3	Modifier le nom d'utilisateur. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] user set name [ID_UTILISATEUR_IPMI] [NOUVEAU_NOM_UTILISATEUR_IPMI]** **NOTE :** Le premier et le deuxième noms d'utilisateur de la liste des utilisateurs sont des champs réservés et ne peuvent donc pas être modifiés.	
Étape_4	Vérifier que le nom d'utilisateur a été correctement mis à jour en affichant la liste des utilisateurs. InviteSE_OrdinateurDistant:~$ ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] user list	

Étape_5	Modifier le mot de passe. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] user set password [ID_UTILISATEUR_IPMI] [NOUVEAU_MOT_DE_PASSE_IPMI]** **NOTE :** Il est recommandé, mais pas obligatoire, de saisir un mot de passe fort composé d'au moins une lettre majuscule, d'un caractère alphanumérique et d'un caractère spécial. **Ne pas utiliser les symboles du code ASCII étendu, car ils ne sont pas gérés par l'outil IPMI.** Noter que le champ du mot de passe est obligatoire et qu'il doit comporter un minimum de 8 caractères lorsque le service SNMP est activé.	
Étape_6	Activer l'utilisateur. InviteSE_OrdinateurDistant:~$ **ipmitool user enable [ID_UTILISATEUR_IPMI]**	
Étape_7	Configurer le niveau de privilège. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] channel setaccess [CANAL_LAN] [ID_UTILISATEUR] privilege=[NIVEAU_DE_PRIVILÈGE]**	
Étape_8	Vérifier que les données d'accès ont été mises à jour correctement en exécutant une commande ipmitool. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOUVEAU_NOM_UTILISATEUR_IPMI] -P [NOUVEAU_MOT_DE_PASSE_IPMI] [COMMANDE_IPMI]** **NOTE :** D'autres paramètres pourraient limiter l'accès de l'utilisateur qui tente de gérer le BMC. Pour plus d'information, voir la documentation d'ipmitool.	

10.2.1.1.3. Configurer les noms d'utilisateur et mots de passe du BMC en utilisant IPMI via KCS

Noter que le champ du mot de passe est obligatoire, qu'il doit comporter un minimum de 8 caractères et qu'il ne doit pas contenir de mots du dictionnaire. Il est recommandé, mais pas obligatoire, de saisir un mot de passe fort composé d'au moins une lettre majuscule, d'un caractère alphanumérique et d'un caractère spécial. Ne pas utiliser les symboles du code ASCII étendu, car ils ne sont pas gérés par l'outil IPMI.

Voir Accéder au BMC en utilisant IPMI via KCS pour les instructions d'accès.

<table>
<tr><td>Étape_1</td><td>À partir d’un ordinateur distant ayant accès au système d’exploitation du serveur via SSH, RDP ou le port série de la plateforme, afficher la liste des utilisateurs du BMC.
InviteSE_ServeurLocal:~# ipmitool user list [CANAL_LAN]</td><td> 
</td></tr>
<tr><td>Étape_2</td><td>Identifier le numéro d'identification de l'utilisateur à modifier.</td><td> 
</td></tr>
<tr><td>Étape_3</td><td colspan="2">Modifier le nom d'utilisateur.
InviteSE_ServeurLocal: ~# ipmitool user set name [ID_UTILISATEUR_IPMI] [NOUVEAU_NOM_UTILISATEUR_IPMI]
NOTE : Le premier et le deuxième noms d'utilisateur de la liste des utilisateurs sont des champs réservés et ne peuvent donc pas être modifiés.</td></tr>
<tr><td>Étape_4</td><td>Vérifier que le nom d'utilisateur a été correctement mis à jour en affichant la liste des utilisateurs. InviteSE_ServeurLocal:~# ipmitool user list [CANAL_LAN]</td><td> 
</td></tr>
<tr><td>Étape_5</td><td>Modifier le mot de passe.
InviteSE_ServeurLocal: ~# ipmitool user set password [ID_UTILISATEUR_IPMI] [NOUVEAU_MOT_DE_PASSE_IPMI]</td><td> 
</td></tr>
<tr><td>Étape_6</td><td colspan="2">Vérifier que les données d’accès ont été mises à jour correctement en utilisant une méthode d'accès qui nécessite d’ouvrir une session.
NOTE : D'autres paramètres pourraient limiter l'accès de l'utilisateur qui tente de gérer le BMC. Voir la documentation d'ipmitool.</td></tr>
</table>

10.2.1.2. Ajouter un utilisateur du BMC

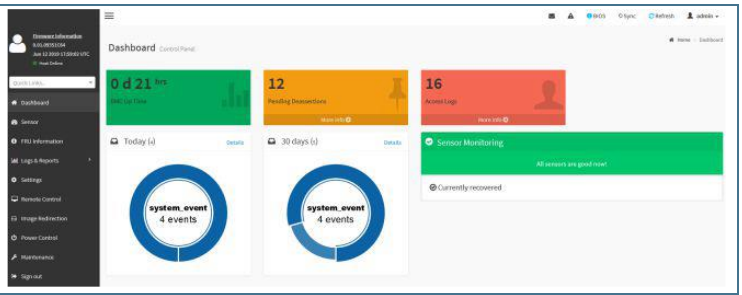
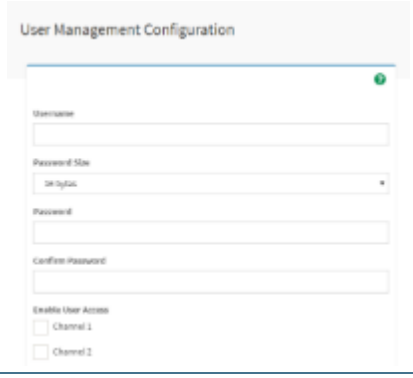
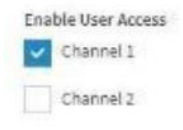
Des utilisateurs du BMC peuvent être ajoutés :

- En utilisant l’interface utilisateur Web
- En utilisant IPMI sur LAN (IOL)
- En utilisant IPMI via KCS

10.2.1.2.1. Ajouter un utilisateur du BMC en utilisant l’interface utilisateur Web

Noter que le champ du mot de passe est obligatoire, qu'il doit comporter un minimum de 8 caractères et qu'il ne doit pas contenir de mots du dictionnaire. Il est recommandé, mais pas obligatoire, de saisir un mot de passe fort composé d'au moins une lettre majuscule, d'un caractère alphanumérique et d'un caractère spécial. Ne pas utiliser les symboles du code ASCII étendu, car ils ne sont pas gérés par l'outil IPMI.

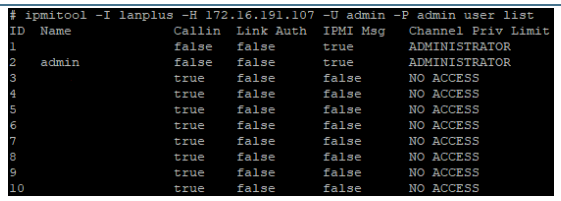
Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

Étape_1	Accéder à l'interface utilisateur Web du BMC du serveur.	
Étape_2	Cliquer sur **Settings** dans le menu de gauche puis cliquer sur **User Management**.	
Étape_3	Sélectionner l'ID de l'utilisateur à activer. **NOTE :** Le premier et le deuxième utilisateur sont des champs réservés, ils ne peuvent par conséquent pas être modifiés.	
Étape_4	Configurer l'utilisateur en fonction des exigences de l'application. **NOTE :** Voir Configurer le niveau de privilège pour les utilisateurs du BMC en utilisant l'interface utilisateur Web pour plus d'instructions sur le niveau de privilège.	
Étape_5	Activer l'utilisateur sur le ou les canaux souhaités.	
Étape_6	Cliquer sur **Save** pour quitter.	

10.2.1.2.2. Ajouter un utilisateur du BMC en utilisant IPMI sur LAN (IOL)

Noter que le champ du mot de passe est obligatoire, qu'il doit comporter un minimum de 8 caractères et qu'il ne doit pas contenir de mots du dictionnaire. Il est recommandé, mais pas obligatoire, de saisir un mot de passe fort composé d'au moins une lettre majuscule, d'un caractère alphanumérique et d'un caractère spécial. Ne pas utiliser les symboles du code ASCII étendu, car ils ne sont pas gérés par l'outil IPMI.

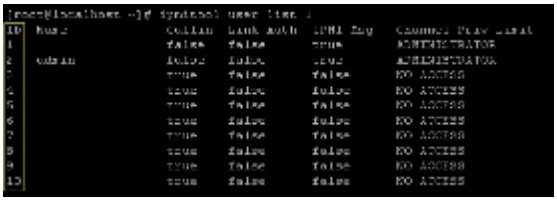
Voir Accéder au BMC en utilisant IPMI sur LAN (IOL) pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, afficher la liste des utilisateurs et sélectionner l'ID de l'utilisateur à ajouter. InviteSE_ServeurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] user list**	
Étape_2	Créer un nom d'utilisateur. InviteSE_ServeurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] user set name [ID_UTILISATEUR_IPMI] [NOUVEAU_NOM_UTILISATEUR_IPMI]** **NOTE :** Le premier et le deuxième noms d'utilisateur de la liste des utilisateurs sont des champs réservés et ne peuvent donc pas être modifiés.	
Étape_3	Créer le mot de passe. InviteSE_ServeurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] user set password [ID_UTILISATEUR_IPMI] [NOUVEAU_MOT_DE_PASSE_IPMI]**	
Étape_4	Activer l'accès au canal et configurer le niveau de privilège. InviteSE_ServeurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] channel setaccess [CANAL_LAN] [ID_UTILISATEUR] privilege=[NIVEAU_DE_PRIVILÈGE]**	
Étape_5	Activer l'utilisateur. InviteSE_ServeurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] user enable [ID_UTILISATEUR]**	

10.2.1.2.3. Ajouter un utilisateur du BMC en utilisant IPMI via KCS

Noter que le champ du mot de passe est obligatoire, qu'il **doit comporter un minimum de 8 caractères et qu'il ne doit pas contenir de mots du dictionnaire**. Il est recommandé, mais pas obligatoire, de saisir un mot de passe fort composé d'au moins une lettre majuscule, d'un caractère alphanumérique et d'un caractère spécial. **Ne pas utiliser les symboles du code ASCII étendu, car ils ne sont pas gérés par l'outil IPMI.**

Voir Accéder au BMC en utilisant IPMI via KCS pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, afficher la liste des utilisateurs et sélectionner l'ID de l'utilisateur à ajouter. InviteSE_ServeurLocal:~# **ipmitool user list [CANAL_LAN]**	
Étape_2	Créer un nom d'utilisateur. InviteSE_ServeurLocal:~# **ipmitool user set name [ID_UTILISATEUR_IPMI] [NOUVEAU_NOM_UTILISATEUR_IPMI]** **NOTE :** Le premier et le deuxième noms d'utilisateur de la liste des utilisateurs sont des champs réservés et ne peuvent donc pas être modifiés.	
Étape_3	Créer le mot de passe. InviteSE_ServeurLocal:~# **ipmitool user set password [ID_UTILISATEUR_IPMI] [NOUVEAU_MOT_DE_PASSE_IPMI]**	
Étape_4	Activer l'accès au canal et configurer le niveau de privilège. InviteSE_ServeurLocal:~# **ipmitool channel setaccess [CANAL_LAN] [ID_UTILISATEUR] privilege=[NIVEAU_DE_PRIVILÈGE]**	
Étape_5	Activer l'utilisateur. InviteSE_ServeurLocal:~# **ipmitool user enable [ID_UTILISATEUR]**	

10.2.1.3. Supprimer ou désactiver un utilisateur du BMC

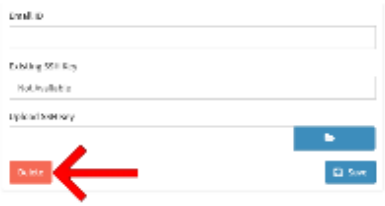
Les utilisateurs du BMC peuvent être :

- Supprimés en utilisant l'interface utilisateur Web
- Désactivés en utilisant IPMI sur LAN (IOL)
- Désactivés en utilisant IPMI via KCS

10.2.1.3.1. Supprimer un utilisateur du BMC en utilisant l'interface utilisateur Web

Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

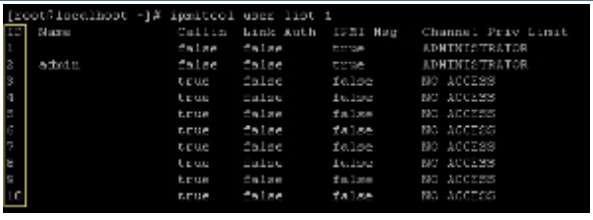
Étape_1	Accéder à l'interface utilisateur Web du BMC du serveur.	
Étape_2	Cliquer sur **Settings** dans le menu de gauche puis cliquer sur **User Management.**	

Étape_3	Sélectionner l'ID de l'utilisateur à supprimer. **NOTE :** Le premier et le deuxième utilisateur sont des champs réservés, ils ne peuvent par conséquent pas être supprimés.	
Étape_4	Appuyer sur **Delete** pour supprimer l'utilisateur.	

10.2.1.3.2. Désactiver un utilisateur du BMC en utilisant IPMI sur LAN (IOL)

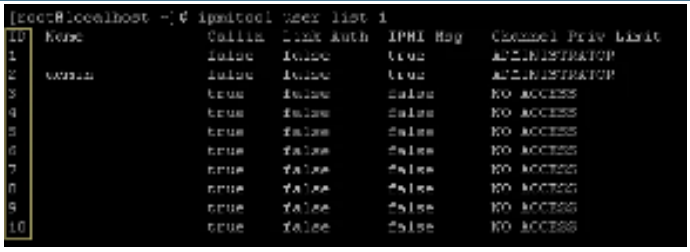
Les utilisateurs ne peuvent pas être supprimés avec ipmitool. Cependant, ils peuvent être désactivés.

Voir Accéder au BMC en utilisant IPMI sur LAN (IOL) pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, afficher la liste des utilisateurs et sélectionner l'ID de l'utilisateur à désactiver. InviteSE_ServeurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] user list**	
Étape_2	Désactiver l'utilisateur sélectionné. InviteSE_ServeurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] user disable [ID_UTILISATEUR]** **NOTE :** Le premier et le deuxième noms d'utilisateur de la liste des utilisateurs sont des champs réservés et ne peuvent donc pas être désactivés.	

10.2.1.3.3. Désactiver un utilisateur du BMC en utilisant IPMI via KCS

Les utilisateurs ne peuvent pas être supprimés avec ipmitool. Cependant, ils peuvent être désactivés. Voir Accéder au BMC en utilisant IPMI via KCS pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, afficher la liste des utilisateurs et sélectionner l'ID de l'utilisateur à désactiver. InviteSE_ServeurLocal:~# **ipmitool user list [CANAL_LAN]**	

Étape_2	Désactiver l'utilisateur sélectionné. InviteSE_ServeurLocal:~# **ipmitool user disable [ID_UTILISATEUR]** **NOTE :** Le premier et le deuxième noms d'utilisateur de la liste des utilisateurs sont des champs réservés et ne peuvent donc pas être désactivés.

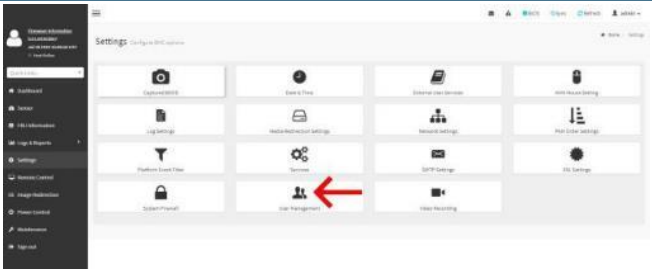
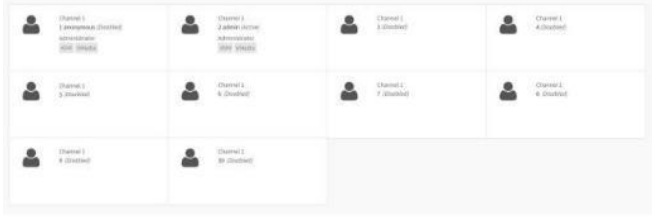
10.2.1.4. Configurer le niveau de privilège pour les utilisateurs du BMC

Le niveau de privilège des utilisateurs du BMC peut être configuré :

- En utilisant l'interface utilisateur Web
- En utilisant IPMI sur LAN (IOL)
- En utilisant IPMI via KCS

10.2.1.4.1. Configurer le niveau de privilège pour les utilisateurs du BMC en utilisant l'interface utilisateur Web

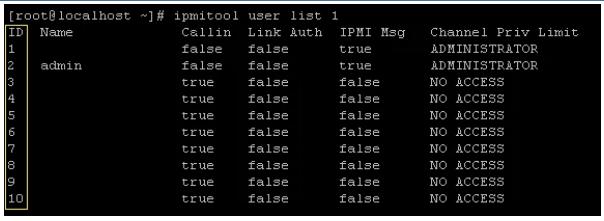
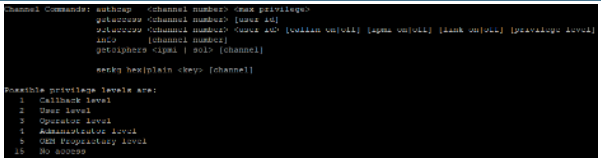
Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

Étape_1	Accéder à l'interface utilisateur Web du BMC du serveur.	
Étape_2	Cliquer sur **Settings** dans le menu de gauche puis cliquer sur **User Management.**	
Étape_3	Sélectionner l'ID de l'utilisateur à gérer. **NOTE :** Le premier et le deuxième utilisateur sont des champs réservés, ils ne peuvent par conséquent pas être écrasés.	
Étape_4	Configurer le niveau de privilège pour chaque canal en fonction des exigences de l'application.	

Étape_5	Cliquer sur **Save** pour quitter.	

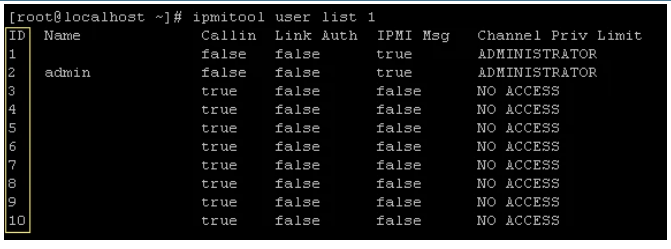
10.2.1.4.2. Configurer le niveau de privilège pour les utilisateurs du BMC en utilisant IPMI sur LAN (IOL)

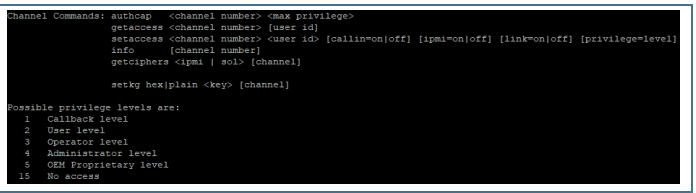
Voir Accéder au BMC en utilisant IPMI sur LAN (IOL) pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, afficher la liste des utilisateurs et sélectionner l'ID de l'utilisateur à gérer. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] user list**	
Étape_2	Lister les niveaux de privilèges disponibles. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] channel help**	
Étape_3	Définir le niveau de privilège pour chaque canal. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI_ADMINISTRATEUR] -P [MOT_DE_PASSE_IPMI_ADMINISTRATEUR] channel setaccess [CANAL_LAN] [ID_UTILISATEUR] privilege=[NIVEAU_DE_PRIVILÈGE]** **NOTE :** Le premier et le deuxième noms d'utilisateur de la liste des utilisateurs sont des champs réservés et ne peuvent donc pas être modifiés.	

10.2.1.4.3. Configurer le niveau de privilège pour les utilisateurs du BMC en utilisant IPMI via KCS

Voir Accéder au BMC en utilisant IPMI via KCS pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, afficher la liste des utilisateurs et sélectionner l'ID de l'utilisateur à gérer. InviteSE_ServeurLocal:~# **ipmitool user list [CANAL_LAN]**	

Étape_2	Lister les niveaux de privilèges disponibles. InviteSE_ServeurLocal:~# **ipmitool channel help**	
Étape_3	Définir le niveau de privilège pour chaque canal. InviteSE_ServeurLocal:~# **ipmitool channel setaccess [CANAL_LAN] [ID_UTILISATEUR] privilege=[NIVEAU_DE_PRIVILÈGE]** **NOTE :** Le premier et le deuxième noms d'utilisateur de la liste des utilisateurs sont des champs réservés et ne peuvent donc pas être modifiés.	

10.2.1.5. Configurer les utilisateurs SNMP

Sections pertinentes :

Accéder au BMC en utilisant BMC SNMP

Accéder au BMC en utilisant l'agent SNMP de Kontron pour Linux

10.2.1.5.1. Configurer les utilisateurs SNMP en utilisant BMC SNMP

Les utilisateurs BMC SNMP sont partagés avec les utilisateurs du BMC.

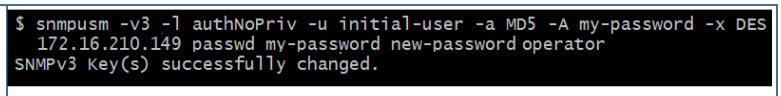
- Pour configurer un utilisateur, voir Configurer les utilisateurs du BMC.
- Pour activer ou désactiver l'accès SNMP, voir Configurer BMC SNMP.

10.2.1.5.2. Configurer les utilisateurs SNMP en utilisant l'agent SNMP de Kontron pour Linux

NOTE : La version actuelle prend en charge la version 3 du protocole SNMP. Pour que les commandes fonctionnent, la version 5.8 ou supérieure de snmpwalk doit être installée.

10.2.1.5.3. Configurer les mots de passe SNMP

Voir Accéder au BMC en utilisant l'agent SNMP de Kontron pour Linux pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, modifier le mot de passe. InviteSE_OrdinateurDistant:~# **snmpusm -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] -x [PROTOCOLE_PROTECTION] [IP_SERVEUR] passwd [ANCIEN_MOT_DE_PASSE] [NOUVEAU_MOT_DE_PASSE] [UTILISATEUR]**	

10.2.1.5.4. Ajouter un utilisateur SNMP

Voir Accéder au BMC en utilisant l'agent SNMP de Kontron pour Linux pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, créer un utilisateur SNMP. InviteSE_OrdinateurDistant:~# **snmpusm -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] [IP_SERVEUR] create [NOUVEL_UTILISATEUR]**	`$ snmpusm -v3 -l authNoPriv -u initial-user -a MD5 -A my-password 172.16.210.149 create operator` `User successfully created.`
Étape_2	Pour initialiser l'utilisateur créé, cloner ses configurations à partir d'un autre utilisateur existant. InviteSE_OrdinateurDistant:~# **snmpusm -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] [IP_SERVEUR] cloneFrom [NOUVEL_UTILISATEUR] [UTILISATEUR_CLONE]**	`$ snmpusm -v3 -l authNoPriv -u initial-user -a MD5 -A my-password 172.16.210.149 cloneFrom operator initial-user` `User successfully cloned.`

10.2.1.5.5. Supprimer un utilisateur SNMP

Voir Accéder au BMC en utilisant l'agent SNMP de Kontron pour Linux pour les instructions d'accès.

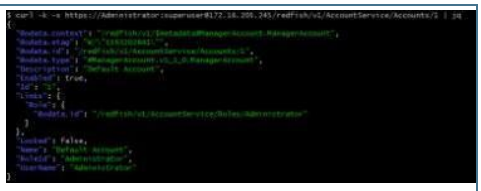
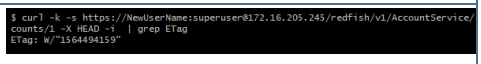
Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, supprimer un utilisateur SNMP. InviteSE_OrdinateurDistant:~# **snmpusm -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] [IP_SERVEUR] delete [UTILISATEUR]**	`$ snmpusm -v3 -l authNoPriv -u initial-user -a MD5 -A new-password 172.16.210.149 delete operator` `User successfully deleted.`

10.2.2. Gestion des utilisateurs Redfish

10.2.2.1. Configurer les noms d'utilisateur et mots de passe Redfish

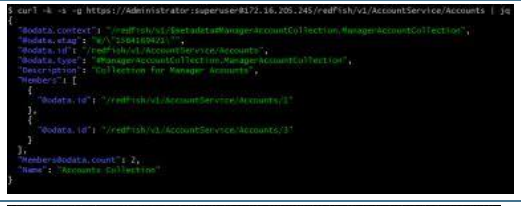
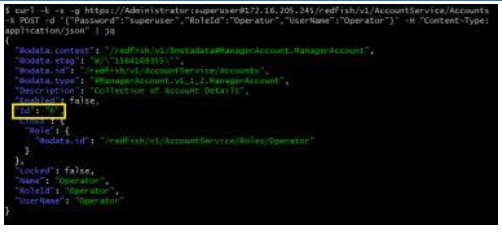
Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

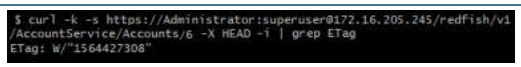
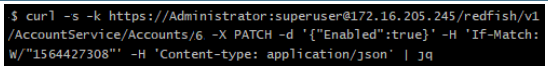
Étape_1	Afficher la liste des utilisateurs et sélectionner l'ID de l'utilisateur à modifier. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/AccountService/Accounts | jq**	

Étape_2	Ajouter à l'URL précédent l'ID sélectionné pour afficher les informations de l'utilisateur. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/AccountService/Accounts/[ID_UTILISATEUR] | jq**	
Étape_3	Afficher l'ETag de l'URL du compte souhaité. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/AccountService/Accounts/[ID_UTILISATEUR] -X HEAD -i | grep ETag**	
Étape_4	Modifier le nom d'utilisateur si requis. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/AccountService/Accounts/[ID_UTILISATEUR] -X PATCH -d '{"UserName":" [NOUVEAU_NOM_UTILISATEUR]"}' -H 'I f-Match: [VALEUR_ETAG]' -H 'Content-type: application/json' | jq** **NOTE :** Une fois le nom d'utilisateur modifié, il doit être mis à jour dans l'URL racine.	
Étape_5	Afficher l'ETag de l'URL du compte souhaité. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/AccountService/Accounts/[ID_UTILISATEUR] -X HEAD -i | grep ETag**	
Étape_6	Modifier le mot de passe si requis. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/AccountService/Accounts/[ID_UTILISATEUR] -X PATCH -d '{"Password":" [NOUVEAU_MOT_DE_PASSE]"}' -H 'I f-Match: [VALEUR_ETAG]' -H 'Content-type: application/json' | jq** **NOTE :** Une fois le mot de passe modifié, il doit être mis à jour dans l'URL racine.	
Étape_7	Vérifier que les données d'accès ont été correctement mises à jour en ouvrant une nouvelle session dans l'API Redfish.	

10.2.2.2. Ajouter un utilisateur Redfish

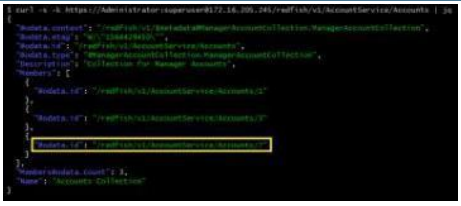
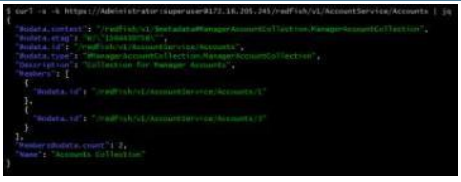
Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Ajouter à l'URL racine le suffixe AccountService/Accounts. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/AccountService/Accounts | jq**	
Étape_2	Créer l'utilisateur et obtenir son ID dans le message de réponse. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/AccountService/Accounts -X POST -d '{"Password":" [MOT_DE_PASSE] ","RoleId":" [ID_ROLE] ","UserName":" [NOM_UTILISATEUR] "}' -H "Content-Type: application/json" | jq** **NOTE :** L'ID de l'utilisateur sera automatiquement créé.	

Étape_3	Afficher l'ETag de l'URL du compte créé. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/AccountService/Accounts/[ID_UTILISATEUR] -X HEAD -i | grep ETag**	
Étape_4	Activer l'utilisateur. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/AccountService/Accounts/[ID_UTILISATEUR] -X PATCH -d '{"Enabled":true}' -H 'I f-Match: [VALEUR_ETAG]' -H 'Content-type: application/json' | jq**	
Étape_5	Vérifier que l'utilisateur a été créé correctement en établissant une connexion à Redfish à l'aide des données d'accès de cet utilisateur.	

10.2.2.3. Supprimer un utilisateur Redfish

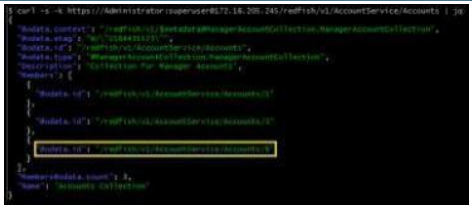
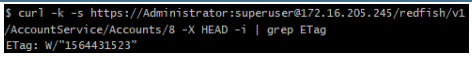
Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

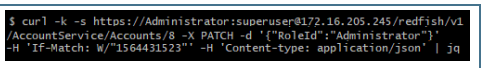
Étape_1	Ajouter à l'URL racine le suffixe AccountService/Accounts et sélectionner l'utilisateur à supprimer. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/AccountService/Accounts | jq**	
Étape_2	Supprimer l'utilisateur. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/AccountService/Accounts/[ID_UTILISATEUR] -X DELETE | jq**	
Étape_3	Vérifier que l'utilisateur a été correctement supprimé. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/AccountService/Accounts | jq**	

NOTE : Les comptes 2 et 3 (HostAutoFW et HostAutoOS) sont réservés à un usage interne et ne peuvent pas être supprimés. Ils ne peuvent pas être utilisés à des fins de gestion.

10.2.2.4. Configurer le niveau de privilège Redfish

Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Ajouter à l'URL racine le suffixe AccountService/Accounts et sélectionner l'utilisateur à configurer. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/AccountService/Accounts | jq**	
Étape_2	Afficher l'ETag de l'URL du compte souhaité. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/AccountService/Accounts/[ID_UTILISATEUR] -X HEAD -i | grep ETag**	

Étape_3	Définir le niveau de privilège. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/AccountService/Accounts/[ID_UTILISATEUR] -X PATCH -d '{"RoleId":" [ID_ROLE]"}' -H 'If-Match: [VALEUR_ETAG]' -H 'Content-type: application/json' | jq**	
Étape_4	Vérifier que le paramètre RoleID a été correctement mis à jour. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/AccountService/Accounts/[ID_UTILISATEUR] | jq**	

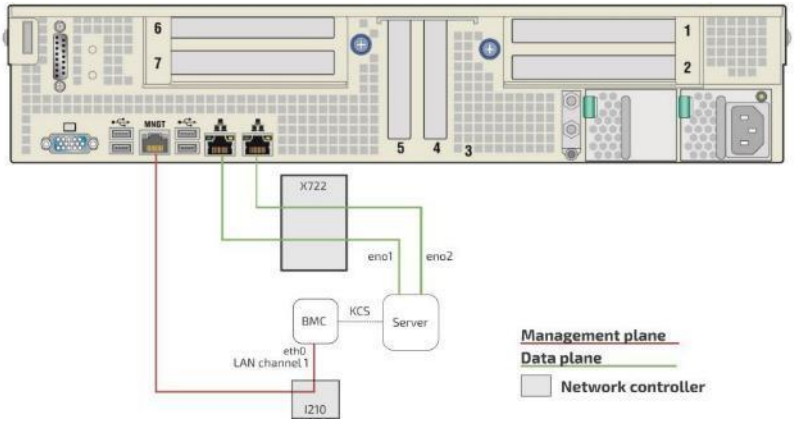
10.2.3. Configurer les utilisateurs du système d'exploitation

Voir Accéder au système d'exploitation d'un serveur pour les instructions d'accès.

Étape_1	Accéder au système d'exploitation en utilisant la méthode privilégiée.
Étape_2	Configurer les utilisateurs comme recommandé dans la documentation du système d'exploitation. **NOTE :** La procédure permettant de modifier les données d'accès pour le système d'exploitation est particulière à l'application et n'est donc pas documentée.

10.3. Contrôleur de gestion de carte mère – BMC

10.3.1. Architecture du BMC



- Une adresse IP de gestion peut être configurée pour la plateforme CG2400 (canal LAN 1).
- Par défaut, les adresses IP des interfaces réseau du BMC sont obtenues via le protocole DHCP.

Voir Architecture du produit pour plus d'information sur la connectivité de réseau.

10.3.2. Choisir une méthode d'accès

Le BMC peut être configuré en utilisant différentes méthodes d'accès en fonction de paramètres déterminés.

- Si l'adresse IP du BMC est inconnue et qu'aucun système d'exploitation n'est installé :

    - Utiliser le menu de configuration du BIOS
- Si l'adresse IP du BMC est inconnue et qu'un système d'exploitation est installé :
    - Utiliser IPMI via KCS
    - Utiliser le menu de configuration du BIOS
- Si l'adresse IP du BMC est connue et qu'un système d'exploitation est installé :
    - Utiliser IPMI (KCS ou IOL)
    - Utiliser le menu de configuration du BIOS

10.3.3. Découvrir l'adresse IP de gestion de la plateforme

Cette adresse IP est le minimum requis pour accéder à l'interface de gestion Web de la plateforme. Elle est également utilisée pour accéder à l'interface de surveillance et au KVM/VM (écran-clavier-souris/support virtuel) pour installer un système d'exploitation.

L'adresse IP de gestion peut être découverte :

- En utilisant la mise à jour DNS dynamique par DHCP
- En utilisant le BIOS via le port d'affichage VGA ou une console série (connexion physique) – plateforme sans système d'exploitation installé et sans adresse IP connue
- En utilisant les journaux du serveur DHCP

10.3.3.1. Découvrir l'adresse IP de gestion de la plateforme en utilisant la mise à jour DNS dynamique par DHCP

10.3.3.1.1. Préalables

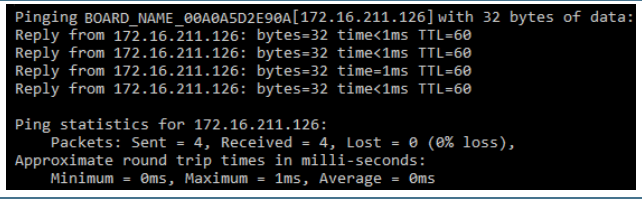
1	Un serveur DHCP avec une fonction active de mise à jour DNS dynamique est disponible.
2	Un ordinateur distant configuré avec la même information DNS est disponible.
3	L'adresse MAC du BMC (canal LAN 1) est connue.

10.3.3.1.2. Procédure

Lorsqu'un bail DHCP est demandé, le BMC de la plateforme fournit au serveur DHCP de l'information pour mettre à jour le système DNS. Si le serveur DHCP est configuré pour la mise à jour DNS dynamique, une entrée sera ajoutée pour un nom d'hôte composé d'un préfixe (modèle de la carte mère de plateforme) et de l'adresse MAC du BMC.

Par exemple, si l'adresse MAC découverte pour le port MGMT du CG2400 est utilisée (c.-à-d. **00:a0:a5:d2:e9:0a**, voir la section Adresses MAC), le nom d'hôte serait : **KMB-I XS100_00A0A5D2E90A**.

L'exemple suivant illustre la méthode qui utilise l'enregistrement DNS automatique avec un ordinateur distant qui a accès au réseau du serveur DHCP.

Étape_1	Sonder le nom de l'hôte par PING. InviteSE_OrdinateurDistant:~$ **ping [NOM_CARTE]_00A0A5D2E90A**	

10.3.3.2. Découvrir de l'adresse IP de gestion de la plateforme en utilisant le BIOS

L'adresse IP de gestion de la plateforme peut être découverte dans le BIOS :

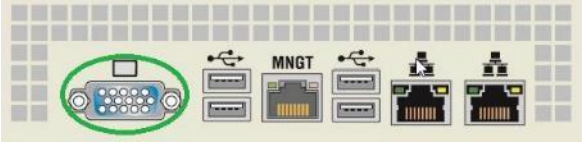
- En utilisant le port d'affichage VGA (connexion physique)
- En utilisant une console série (connexion physique)

10.3.3.2.1. Découvrir l'adresse IP de gestion dans le BIOS via le port d'affichage VGA

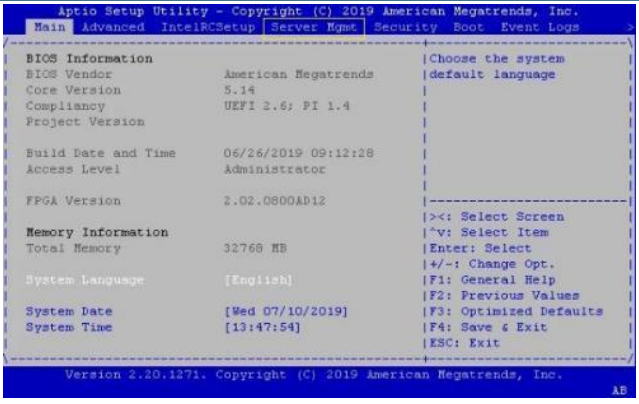
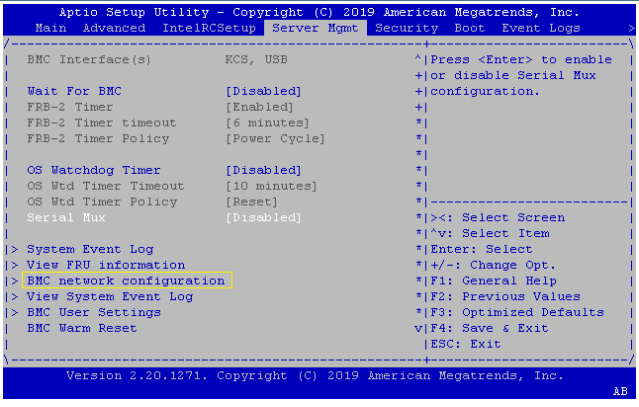
10.3.3.2.1.1. Préalables

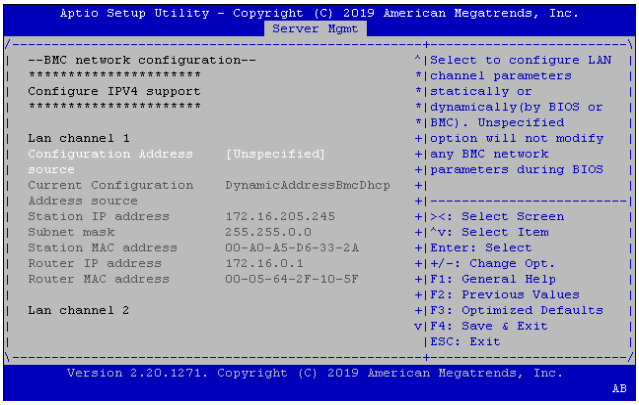
1	Une connexion physique au port d'affichage VGA de l'appareil est requise.
2	Une souris et/ou un clavier sont connectés.

Figure 30. Emplacement du port



10.3.3.2.1.2. Accéder au menu BMC network configuration

Étape_1	À partir du menu UEFI/BIOS, naviguer jusqu'à l'onglet **Server Mgmt**.	
Étape_2	Sélectionner **BMC network configuration**.	

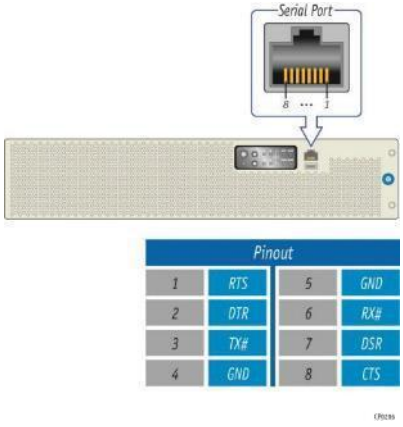
Étape_3	Le menu **BMC network configuration** s'affiche. **NOTE :** Lorsque la plateforme est démarrée après avoir été éteinte, l'UEFI/BIOS peut se charger avant que le BMC n'ait reçu son adresse IP. Dans ce cas, les informations du menu UEFI/BIOS devront être actualisées en redémarrant le serveur et en entrant à nouveau dans le menu UEFI/BIOS.	

10.3.3.2.2. Découvrir l'adresse IP de gestion dans le BIOS via une console série (connexion physique)

10.3.3.2.2.1. Préalables

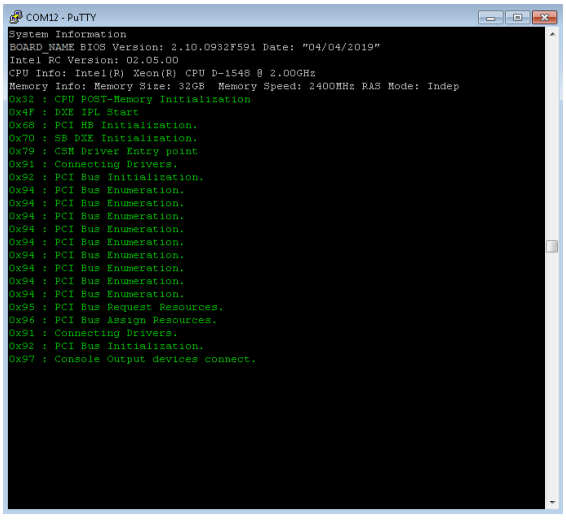
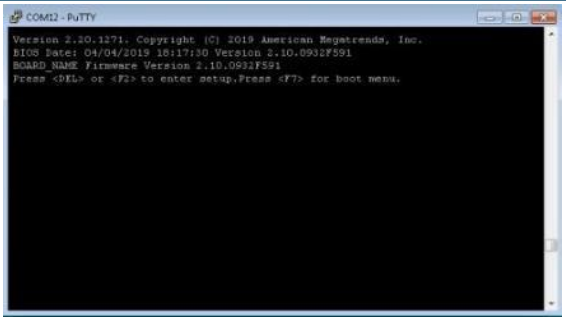
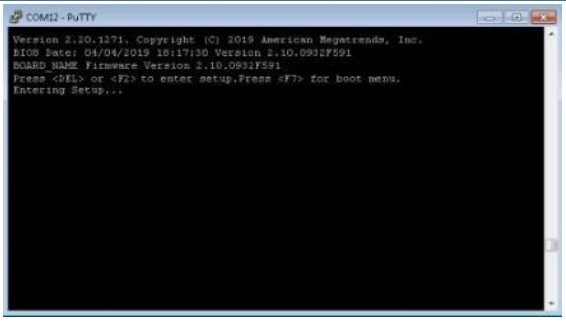
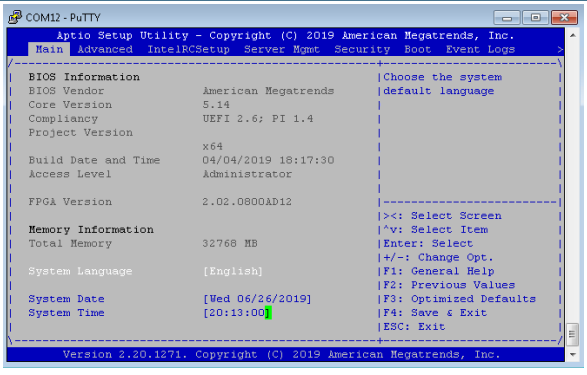
1	Une connexion physique à l'appareil est requise. **NOTE :** Le port de console série est compatible avec le câble 72-3383-01 de Cisco.
2	Un outil de console série est installé sur l'ordinateur distant. Vitesse (baud) : 115200 • Bits d'information : 8 • Bits d'arrêt : 1 • Parité : Aucune • Contrôle de flux : Aucun • Mode émulation recommandé : VT100+ **NOTE :** PuTTY est recommandé.

Figure 31. Emplacement du port série

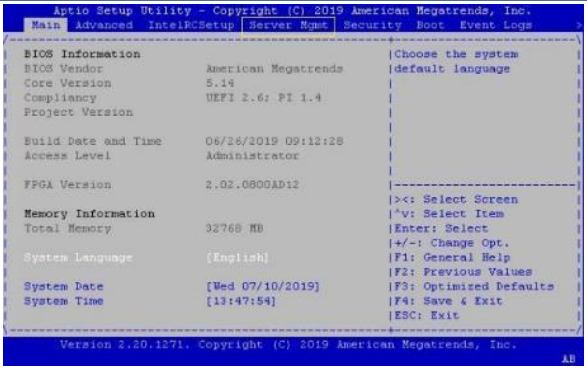
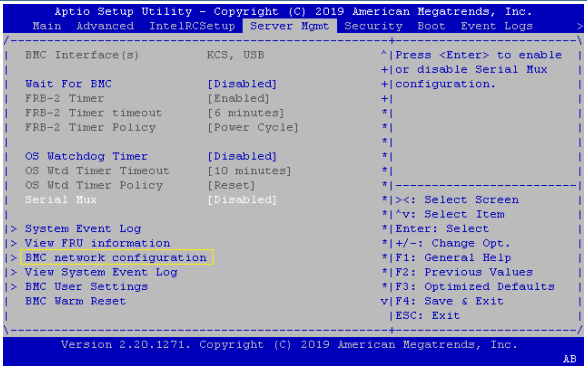
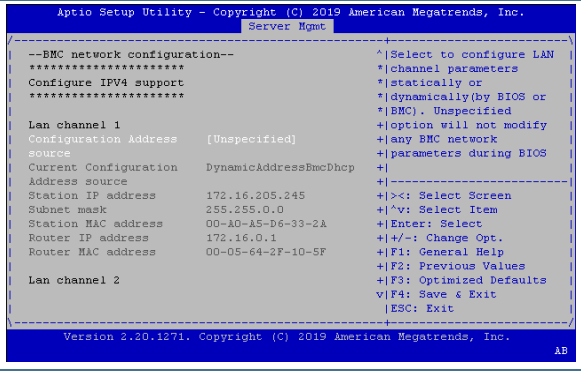


10.3.3.2.2.2. Procédure d'accès

Étape_1	À partir d'un ordinateur disposant d'une connexion physique au port série, ouvrir un outil de console série et démarrer la communication entre la console et le port auquel le système est connecté.

Étape_2	Réinitialiser le serveur (raccourci-clavier **Ctrl-Pause** [Ctrl-Break]). **NOTE :** Si un système d'exploitation est installé, le raccourci-clavier pourrait ne pas fonctionner correctement. Si c'est le cas, réinitialiser le serveur en suivant les recommandations propres au système d'exploitation. **NOTE :** Lorsqu'une commande de réinitialisation du serveur est lancée, quelques secondes peuvent s'écouler avant que l'écran d'accueil du BIOS ne s'affiche.	
Étape_3	Lorsque l'écran d'accueil du BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration du BIOS. **NOTE :** Il peut s'écouler quelques secondes avant que l'écran d'accueil du BIOS n'affiche le message de confirmation "Entering Setup...".	
Étape_4	L'écran d'accueil du BIOS affiche "Entering Setup...". **NOTE :** L'affichage et l'entrée dans le menu de configuration du BIOS prendront quelques secondes.	
Étape_5	Le menu de configuration du BIOS s'affiche.	

10.3.3.2.2.3. Accéder au menu BMC network configuration

Étape_1	À partir du menu UEFI/BIOS, naviguer jusqu'à l'onglet **Server Mgmt**.	
Étape_2	Sélectionner **BMC network configuration**.	
Étape_3	Le menu **BMC network configuration** s'affiche. **NOTE :** Lorsque la plateforme est démarrée après avoir été éteinte, l'UEFI/BIOS peut se charger avant que le BMC n'ait reçu son adresse IP. Dans ce cas, les informations du menu UEFI/BIOS devront être actualisées en redémarrant le serveur et en entrant à nouveau dans le menu UEFI/BIOS.	

10.3.3.2.3. Découvrir de l'adresse IP de gestion de la plateforme en utilisant les journaux du serveur DHCP

10.3.3.2.4. Préalables

1	L'accès aux journaux du serveur DHCP est nécessaire.
2	L'adresse MAC du BMC (canal LAN 1) est connue.

Section pertinente :

Adresses MAC

10.3.3.2.5. Procédure

L'attribution de l'adresse IP par DHCP est propre à l'infrastructure réseau à laquelle la plateforme est intégrée. L'assistance de l'administrateur du réseau pourrait donc être nécessaire pour obtenir l'adresse IP du composant (ex. BMC, système d'exploitation de réseau [NOS], système d'exploitation du serveur).

Si l'adresse MAC du composant est connue, il est possible de consulter les journaux du serveur DHCP pour déterminer l'adresse IP attribuée à un composant en particulier. Voir la section Adresses MAC pour déterminer celles qui sont propres à une plateforme.

Divers services de serveurs DHCP pourraient offrir d'autres capacités de recherche. Consulter l'administrateur du réseau ou la documentation du serveur DHCP. L'exemple suivant illustre une méthode avec une invite de commande à utiliser avec un serveur DHCP Linux. Il pourrait être nécessaire de l'ajuster pour refléter une infrastructure DHCP particulière (cette action peut généralement être effectuée via l'interface Web d'un serveur DHCP).

```
DHCP_Server:~$ cat /var/log/messages * | grep -i 00:a0:a5:d2:e9:0a
Mar  1 13:44:15 DHCP_Server dhcpd: DHCPDISCOVER from 00:a0:a5:d2:e9:0a via ens192
Mar  1 13:44:16 DHCP_Server dhcpd: DHCPOFFER on 172.16.211.126 to 00:a0:a5:d2:e9:0a via ens192
Mar  1 13:44:16 DHCP_Server dhcpd: DHCPREQUEST for 172.16.211.126 (172.16.0.10) from 00:a0:a5:d2:e9:0a via ens192
Mar  1 13:44:16 DHCP_Server dhcpd: DHCPACK on 172.16.211.126 to 00:a0:a5:d2:e9:0a via ens192
```

Variable	Description
00:a0:a5:d2:e9:0a	Adresse MAC découverte pour le composant (voir Adresses MAC)
ens192	Nom de l'interface réseau du serveur DHCP Linux
172.16.211.126	Adresse IP attribuée au composant par le serveur DHCP
172.16.0.10	Adresse IP du serveur DHCP Linux

10.3.4. Configurer une adresse IP statique

Les procédures décrites ci-dessous doivent être effectuées pour une interface à la fois. Si l'application nécessite plusieurs interfaces, les configurer séparément.

Une adresse IP statique peut être configurée :

- En utilisant le menu de configuration du BIOS
- En utilisant IPMI

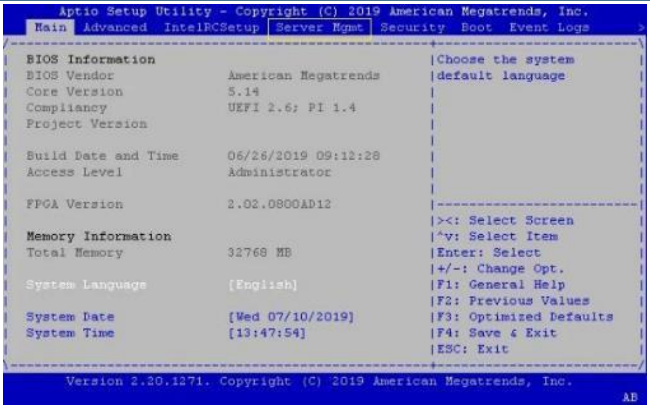
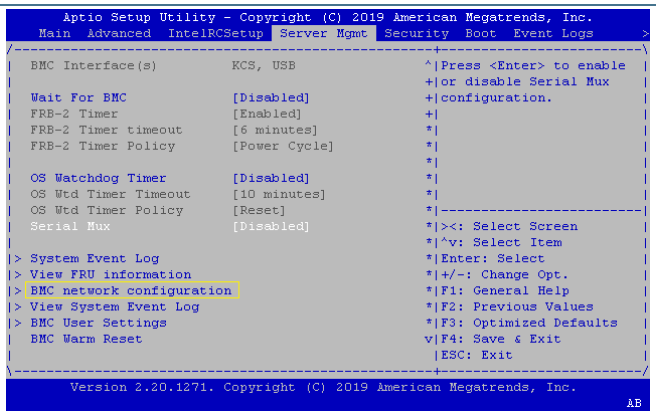
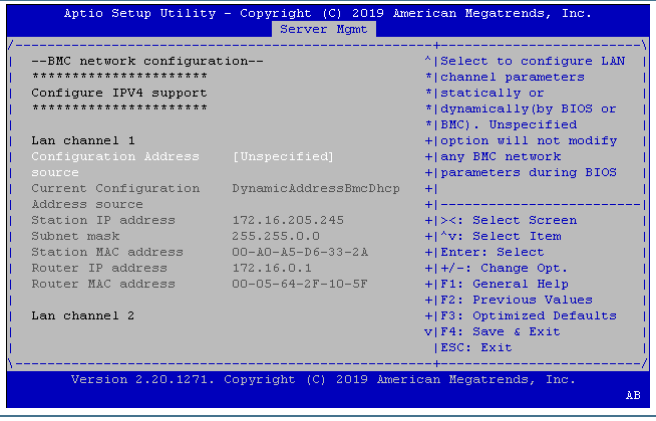
10.3.4.1. Configurer une adresse IP statique en utilisant le menu de configuration du BIOS

10.3.4.1.1. Accéder au menu de configuration du BIOS

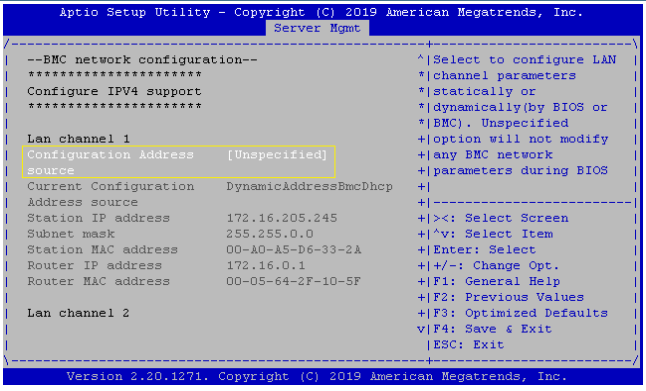
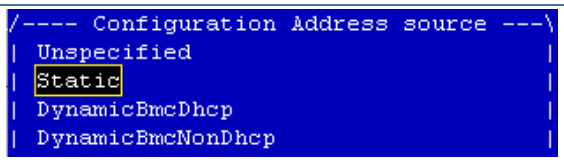
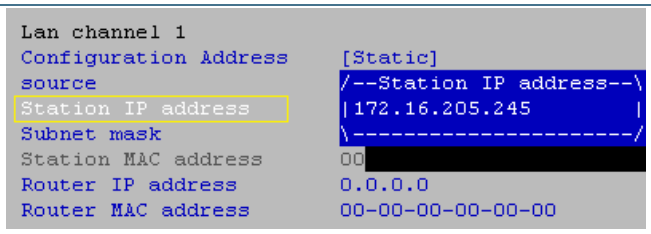
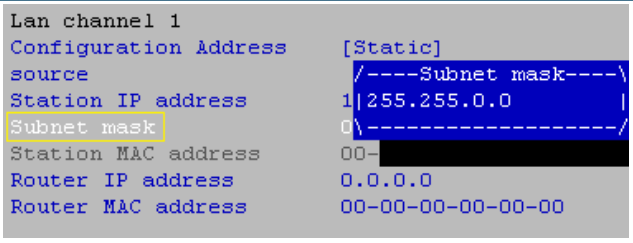
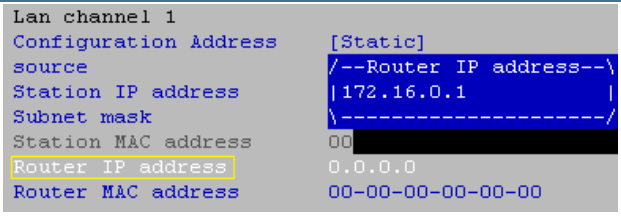
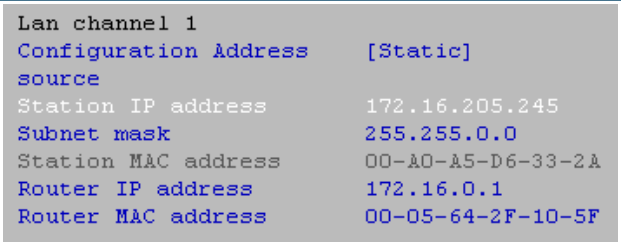
Le menu de configuration du BIOS est accessible par différentes méthodes :

- Si aucun système d'exploitation n'est installé et qu'aucune adresse IP n'est connue, il est obligatoire d'utiliser une console série. Voir Accéder au BIOS à l'aide d'une console série (connexion physique).
- Si l'adresse IP du BMC est connue, toutes les méthodes d'accès au BIOS fonctionneront. Voir Accéder au BIOS pour choisir une méthode d'accès.

10.3.4.1.2. Accéder au menu BMC network configuration

Étape_1	À partir du menu UEFI/BIOS, naviguer jusqu'à l'onglet **Server Mgmt**.	
Étape_2	Sélectionner **BMC network configuration**.	
Étape_3	Le menu **BMC network configuration** s'affiche. **NOTE :** Lorsque la plateforme est démarrée après avoir été éteinte, l'UEFI/BIOS peut se charger avant que le BMC n'ait reçu son adresse IP. Dans ce cas, les informations du menu UEFI/BIOS devront être actualisées en redémarrant le serveur et en entrant à nouveau dans le menu UEFI/BIOS.	

10.3.4.1.3. Configurer une adresse IP statique

Étape_1	À partir du menu **BMC network configuration**, sélectionner l'option **Configuration Address source** pour l'interface LAN à configurer (canal LAN 1 dans cet exemple).	
Étape_2	Sélectionner **Static**.	
Étape_3	Modifier le paramètre **Station IP address**. **NOTE :** Il s'agit de l'adresse IP de gestion (**IP_GESTION_BMC**).	
Étape_4	Modifier le paramètre **Subnet mask**.	
Étape_5	(Optionnel) Modifier le paramètre **Router IP address**.	
Étape_6	Confirmer que la configuration a été modifiée et quitter le menu **BMC network configuration** en utilisant la touche **Échap** [ESC].	

10.3.4.2. Configurer une adresse IP statique en utilisant IPMI

10.3.4.2.1. Accéder au BMC

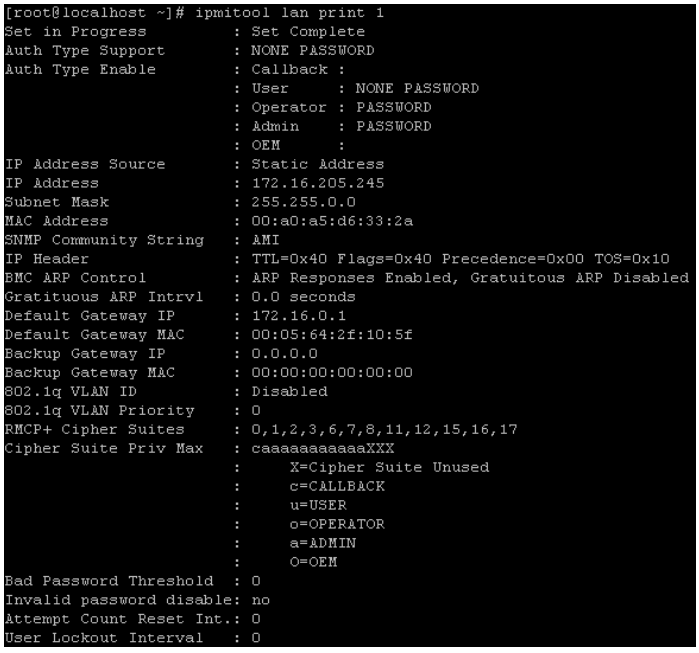
Le BMC est accessible par deux méthodes IPMI.

- Si un système d'exploitation est installé (adresse IP du BMC connue ou non), IPMI via KCS peut être utilisé. Voir Accéder au BMC en utilisant IPMI via KCS.
- Si l'adresse IP du BMC est connue (système d'exploitation installé ou non), IPMI sur LAN peut être utilisé. Voir **Erreur! Source du renvoi introuvable.**.

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL. Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

10.3.4.2.2. Configurer une adresse IP statique

Étape_1	Définir la source IP sur statique. InviteSE_ServeurLocal:~# **ipmitool lan set [CANAL_LAN] ipsrc static**	
Étape_2	Définir l'adresse IP à utiliser. InviteSE_ServeurLocal:~# **ipmitool lan set [CANAL_LAN] ipaddr [NOUVEL_IP]** **NOTE :** Il s'agit de l'adresse IP du BMC (**IP_GESTION_BMC**). **NOTE :** La définition d'une adresse IP peut prendre plusieurs secondes.	`[root@localhost ~]# ipmitool lan set 1 ipaddr 172.16.205.245` `Setting LAN IP Address to 172.16.205.245`
Étape_3	Définir le masque de sous-réseau. InviteSE_ServeurLocal:~# **ipmitool lan set [CANAL_LAN] netmask [NOUVEAU_MASQUE]** **NOTE :** La définition d'un masque de sous-réseau peut prendre plusieurs secondes.	`[root@localhost ~]# ipmitool lan set 1 netmask 255.255.0.0` `Setting LAN Subnet Mask to 255.255.0.0`
Étape_4	Définir l'adresse IP de la passerelle par défaut. InviteSE_ServeurLocal:~# **ipmitool lan set [CANAL_LAN] defgw ipaddr [IP_ROUTEUR]** **NOTE** : La définition de l'adresse IP de la passerelle par défaut peut prendre plusieurs secondes.	`[root@localhost ~]# ipmitool lan set 1 defgw ipaddr 172.16.0.1` `Setting LAN Default Gateway IP to 172.16.0.1`
Étape_5	Définir l'adresse MAC de la passerelle par défaut. InviteSE_ServeurLocal:~# **ipmitool lan set [CANAL_LAN] defgw macaddress [MAC_ROUTEUR]**	`[root@localhost ~]# ipmitool lan set 1 defgw macaddress 00:05:64:2f:10:5f` `Setting LAN Default Gateway MAC to 00:05:64:2f:10:5f`

Étape_6	Vérifier que la configuration a été modifiée. InviteSE_ServeurLocal:~# **ipmitool lan print [CANAL_LAN]**	

10.3.5. Configurer une adresse IP dynamique en utilisant DHCP

Les procédures décrites ci-dessous doivent être effectuées pour une interface à la fois. Si l'application nécessite plusieurs interfaces, les configurer séparément.

Une adresse IP dynamique peut être configurée :

- En utilisant le menu de configuration du BIOS
- En utilisant IPMI

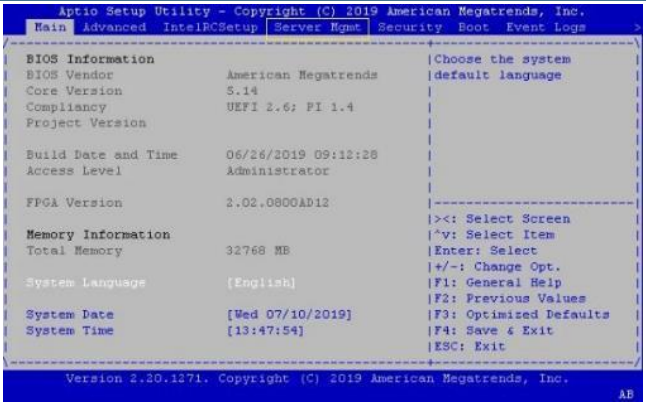
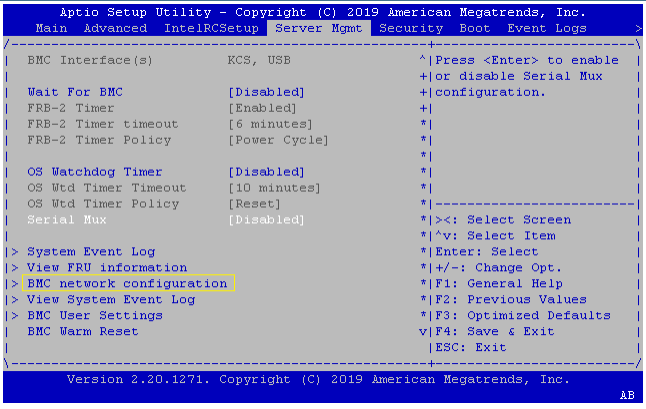
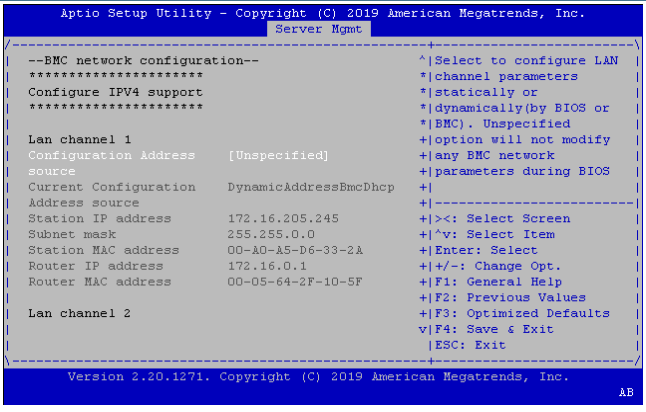
10.3.5.1. Configurer une adresse IP dynamique en utilisant le menu de configuration du BIOS

10.3.5.1.1. Accéder au menu de configuration du BIOS

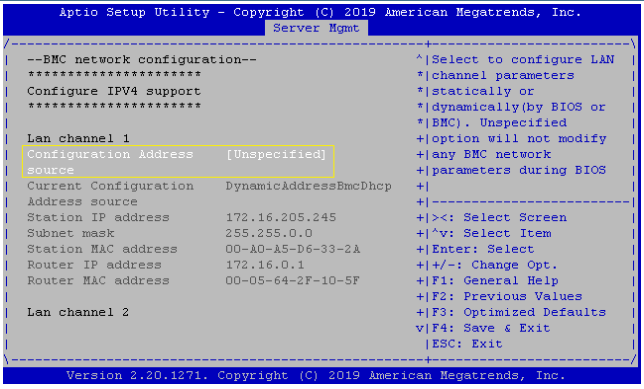
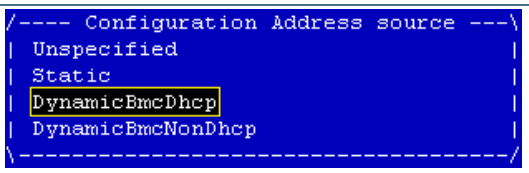
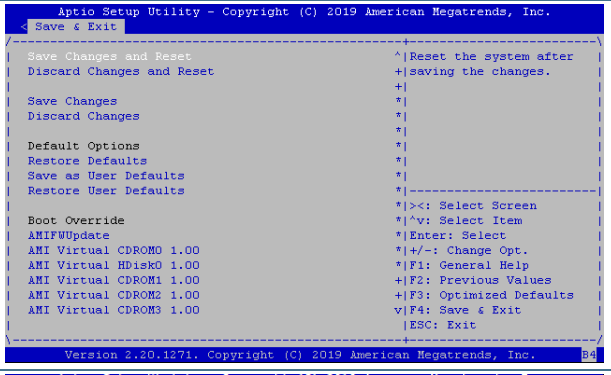
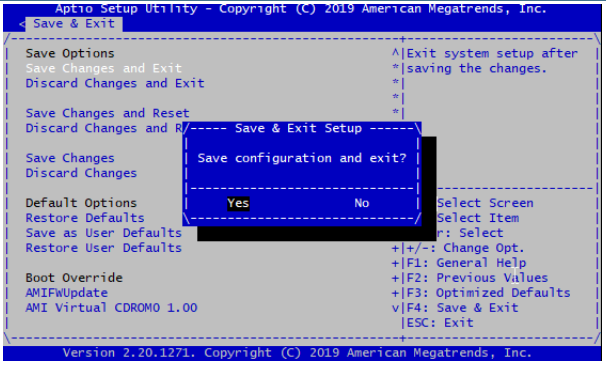
Le menu de configuration du BIOS est accessible par différentes méthodes :

- Si aucun système d'exploitation n'est installé et qu'aucune adresse IP n'est connue, il est obligatoire d'utiliser une console série. Voir Accéder au BIOS à l'aide d'une console série (connexion physique).
- Si l'adresse IP du BMC est connue, toutes les méthodes d'accès au BIOS fonctionneront. Voir Accéder au BIOS pour choisir une méthode d'accès.

10.3.5.1.2. Accéder au menu BMC network configuration

Étape_1	À partir du menu UEFI/BIOS, naviguer jusqu'à l'onglet **Server Mgmt**.	
Étape_2	Sélectionner **BMC network configuration**.	
Étape_3	Le menu **BMC network configuration** s'affiche. **NOTE** : Lorsque la plateforme est démarrée après avoir été éteinte, l'UEFI/BIOS peut se charger avant que le BMC n'ait reçu son adresse IP. Dans ce cas, les informations du menu UEFI/BIOS devront être actualisées en redémarrant le serveur et en entrant à nouveau dans le menu UEFI/BIOS.	

10.3.5.1.3. Configurer une adresse IP dynamique en utilisant DHCP

Étape_1	À partir du menu **BMC network configuration**, sélectionner l'option **Configuration Address source** pour l'interface LAN à configurer (canal LAN 1 dans cet exemple).	
Étape_2	Sélectionner **DynamicBmcDhcp**.	
Étape_3	Naviguer vers l'onglet **Save & Exit**.	
Étape_4	Sélectionner **Save Changes and Exit**, ce qui entraîne une réinitialisation du serveur.	
Étape_5	Lorsque l'écran d'accueil du BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration du BIOS. Ensuite, accéder au menu **Server Mgmt** et sélectionner **BMC network configuration**. L'adresse affichée est l'adresse IP de gestion (IP_GESTION_BMC).	

10.3.5.2. Configurer une adresse IP dynamique en utilisant IPMI

10.3.5.2.1. Accéder au BMC

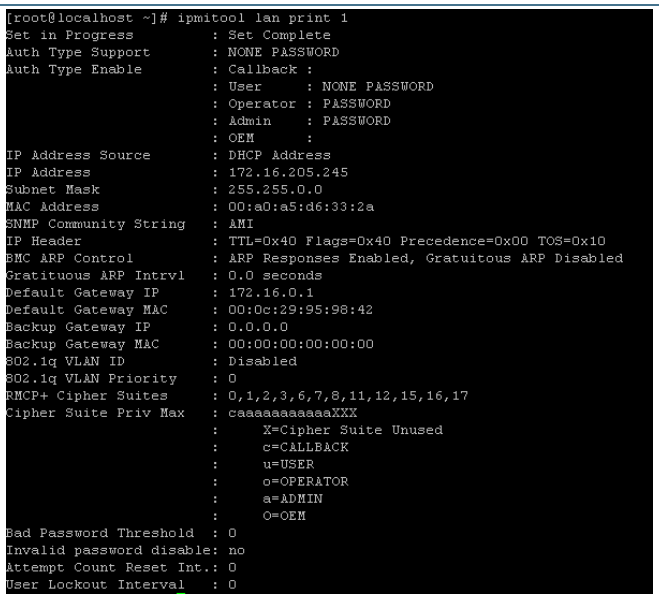
Le BMC est accessible par deux méthodes IPMI.

- Si un système d'exploitation est installé (adresse IP du BMC connue ou non), IPMI via KCS peut être utilisé. Voir Accéder au BMC en utilisant IPMI via KCS.

- Si l'adresse IP du BMC est connue (système d'exploitation installé ou non), IPMI sur LAN peut être utilisé. Voir **Erreur! Source du renvoi introuvable.**.

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL. Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

10.3.5.2.2. Configurer une adresse IP dynamique

Étape_1	Définir la source IP sur DHCP. InviteSE_ServeurLocal:~# **ipmitool lan set [CANAL_LAN] ipsrc dhcp** **NOTE** : En fonction de l'infrastructure existante, plusieurs secondes peuvent s'écouler avant d'obtenir une adresse IP du serveur DHCP.	
Étape_2	Vérifier que la configuration a été modifiée. InviteSE_ServeurLocal:~# **ipmitool lan print [CANAL_LAN]** **NOTE** : Il s'agit de l'adresse IP du BMC (**IP_GESTION_BMC**).	

10.4. Configuration du protocole de diffusion du temps en réseau

Le protocole de diffusion du temps en réseau (NTP) peut être configuré :

- En utilisant l'interface utilisateur Web
- En utilisant IPMI (IOL ou KCS)

NOTE : L'heure du système n'est pas réglée après le démarrage de l'unité. Il suffit de réinitialiser le serveur pour définir l'heure automatiquement une fois que le serveur NTP du BMC est configuré.

10.4.1. Configurer le NTP en utilisant l'interface utilisateur Web

10.4.1.1. Préalables

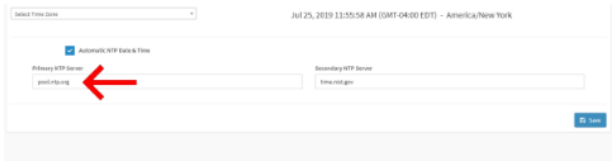
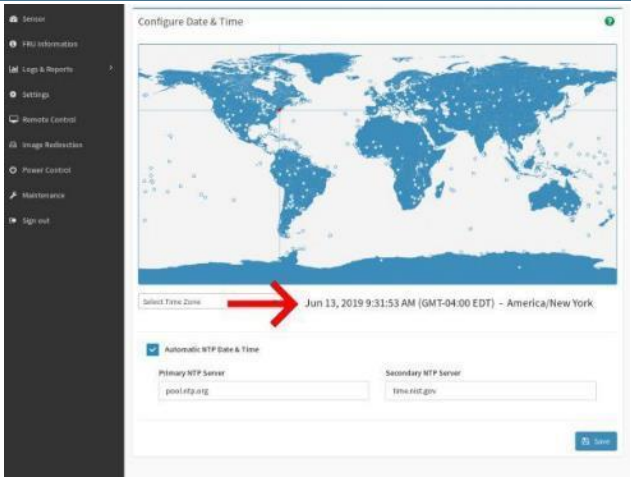
1	L'adresse IP du BMC est connue (voir la section Configuration > Contrôleur de gestion de carte mère – BMC pour obtenir le paramètre IP_GESTION_BMC).
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.

Sections pertinentes :

Contrôleur de gestion de carte mère – BMC

Accéder au BMC

10.4.1.2. Procédure

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, accéder à l'interface utilisateur Web du BMC avec l'adresse IP du BMC.	
Étape_2	Cliquer sur **Settings** dans le menu de gauche. Cliquer ensuite sur **Date & Time**.	
Étape_3	Dans le champ **Primary NTP Server**, saisir l'adresse du serveur NTP souhaité.	
Étape_4	Vérifier que l'heure et la date affichées correspondent à l'heure et à la date locales. **NOTE** : Il peut s'écouler plusieurs secondes ou minutes avant que le BMC ne synchronise l'heure avec le serveur NTP.	

10.4.2. Configurer le NTP en utilisant IPMI (IOL ou KCS)

10.4.2.1. Préalables (IOL)

1	L'adresse IP du BMC est connue.
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.
3	Une version de la communauté d'ipmitool est installée sur un ordinateur distant pour permettre la surveillance à distance – il est recommandé d'utiliser la version 1.8.18 d'ipmitool.

Sections pertinentes :

Contrôleur de gestion de carte mère – BMC

Accéder au système d'exploitation d'un serveur

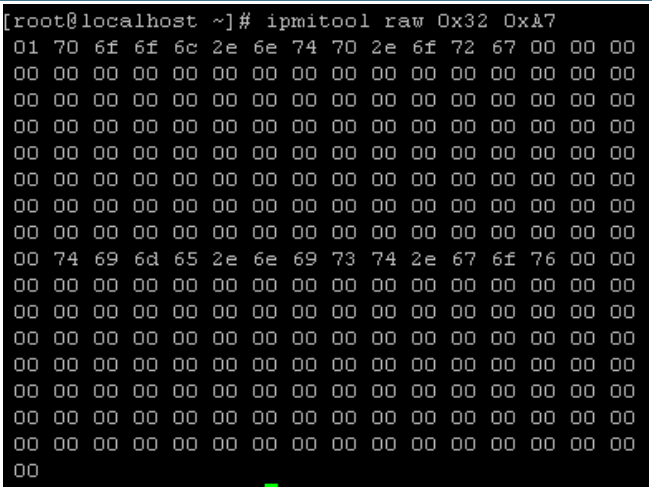
10.4.2.2. Préalables (KCS)

1	Un système d'exploitation est installé.
2	L'ordinateur distant a accès au système d'exploitation du serveur (SSH/RDP/port série de la plateforme).
3	Une version de la communauté d'ipmitool est installée sur le serveur local pour permettre la surveillance locale – il est recommandé d'utiliser la version 1.8.18 d'ipmitool.

10.4.2.3. Définir l'heure et la date du BMC

Section pertinente :

Décodage des données de configuration brute NTP

Étape_1	Activer le service NTP. InviteSE_ServeurLocal:~# **ipmitool raw 0x32 0xA8 3 1**	
Étape_2	Obtenir les données de configuration NTP pour récupérer l'adresse du serveur NTP actuel. InviteSE_ServeurLocal:~# **ipmitool raw 0x32 0xA7**	
Étape_3	Décoder le tableau des données brutes. Voir Décodage des données de configuration brute NTP.	Données décodées pour cet exemple : Statut NTP : 0x01 Enabled NTP primaire : 70 6f 6f 6c 2e 6e 74 70 2e 6f 72 67 "pool.ntp.org" NTP secondaire : 74 69 6d 65 2e 6e 69 73 74 2e 67 6f 76 "time.nist.gov"

Étape_4	Définir les deux adresses NTP avec les paramètres suivants : • Le paramètre **ADRESSE_NTP** peut prendre les valeurs suivantes : 0x01 (pour le primaire) ou 0x02 (pour le secondaire). • Le paramètre **DATA** doit être converti de chaîne (string) à brute (raw). • Le paramètre **DATA** doit avoir une longueur de 128 octets et doit être complété par des 0 jusqu'à ce que la longueur de l'adresse soit de 128 octets. • Le format du paramètre **DATA** peut être décimal ou hexadécimal. Si l'hexadécimal est utilisé, chaque nombre doit être précédé du préfixe 0x. InviteSE_ServeurLocal:~# **ipmitool raw 0x32 0xA8 [ADRESSE_NTP] [DONNÉES]**	ipmitool raw 0x32 0xA8 0x01 49 48 46 49 46 50 48 46 49 48 0
Étape_5	Redémarrer le service NTP afin de sauvegarder la configuration NTP. InviteSE_ServeurLocal:~# **ipmitool -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR] -P [MOT_DE_PASSE] -I lanplus raw 0x32 0xA8 4**	

10.4.2.4. Confirmer la configuration

Étape_1	Obtenir l'heure et la date du BMC. InviteSE_ServeurLocal:~# **ipmitool sel time get**	[root@localhost ~]# ipmitool sel time get 07/16/2019 23:14:24
Étape_2	Vérifier que l'heure et la date du BMC affichées correspondent à l'heure et à la date locales. **NOTE :** Il peut s'écouler plusieurs secondes ou minutes avant que le BMC ne synchronise l'heure avec le serveur NTP.	

10.4.2.5. Décodage des données de configuration brute NTP

Octets	Description	Valeurs possibles
0	Statut du NTP	• 0x00 : Désactivé • 0x01 : Activé • 0x02 : État d'échec
1:128	IP du serveur primaire, chiffre de poids fort (MSB) en premier	Valeurs hexadécimales (0:255)
139:256	IP du serveur secondaire, chiffre de poids fort (MSB) en premier	Valeurs hexadécimales (0:255)

Ce script peut être utilisé pour convertir des données de chaîne (string) en données brutes (raw) et pour compléter les données brutes avec le nombre requis de 0.

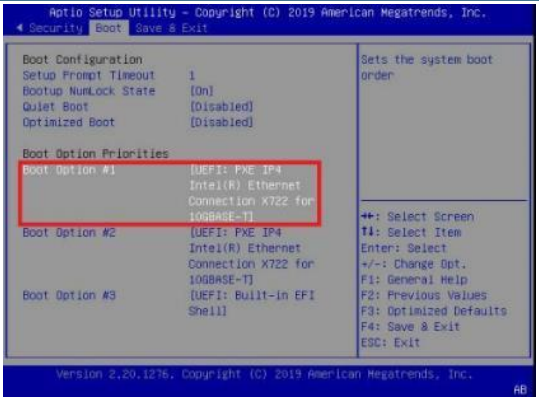
Conversion d'adresse
string="$(printf "10.1.20.10" \| od -t d1 \| head -n1 \| sed 's/0000000 //g' \| sed 's/ //g')" length=$(echo $string \| wc -w) string_padded="$string" for i in $(seq 0 $((127 - length))); do   string_padded="$string_padded 0" done echo $string_padded

Pour convertir des données ASCII et hexadécimales, vous pouvez utiliser cet outil en ligne https://www.rapidtables.com/convert/number/ascii-to-hex.html et compléter jusqu'à 128 octets avec 0.

10.5. Configuration de base des options du BIOS

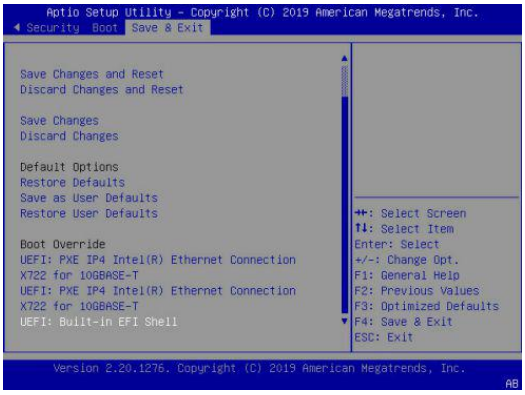
10.5.1. Modifier l'ordre de démarrage (boot order)

Voir Accéder au BIOS pour les instructions d'accès.

Étape_1	Dans le menu de configuration du BIOS, utiliser les flèches du clavier pour sélectionner le menu **Boot**. Configurez l'ordre de démarrage comme souhaité.	
Étape_2	À l'aide des flèches du clavier, sélectionner le menu **Save & Exit**, aller à **Save Changes and Exit** et appuyer sur **Entrée** pour confirmer et enregistrer le nouvel ordre de démarrage.	

10.5.2. Modifier l'ordre de démarrage pour un démarrage unique

Voir Accéder au BIOS pour les instructions d'accès.

Étape_1	Dans le menu de configuration du BIOS, utiliser les flèches du clavier pour sélectionner le menu **Save & Exit**. Dans la section **Boot Override**, sélectionner l'option souhaitée et appuyer sur **Entrée**. Le serveur démarrera à partir d'un périphérique particulier. **NOTE** : Cette sélection n'affecte que le démarrage à venir.	

10.5.3. Modifier l'ordre de démarrage pour un démarrage unique en utilisant IPMI

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL. Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

Étape_1	Afficher la liste des périphériques de démarrage et sélectionner l'option souhaitée. InviteSE_ServeurLocal:~# **ipmitool chassis bootdev help** **NOTE** : Tous les périphériques ne sont pas pris en charge par ipmitool.	`$ ipmitool chassis bootdev help` `bootdev <device> [clear-cmos=yes|no]` `bootdev <device> [options=help,...]` `none : Do not change boot device order` `pxe : Force PXE boot` `disk : Force boot from default Hard-drive` `safe : Force boot from default Hard-drive, request Safe Mode` `diag : Force boot from Diagnostic Partition` `cdrom : Force boot from CD/DVD` `bios : Force boot into BIOS Setup` `floppy: Force boot from Floppy/primary removable media`
Étape_2	Outrepasser l'ordre de démarrage InviteSE_ServeurLocal:~# **ipmitool chassis bootdev [APPAREIL]**	`$ ipmitool chassis bootdev pxe` `Set Boot Device to pxe`

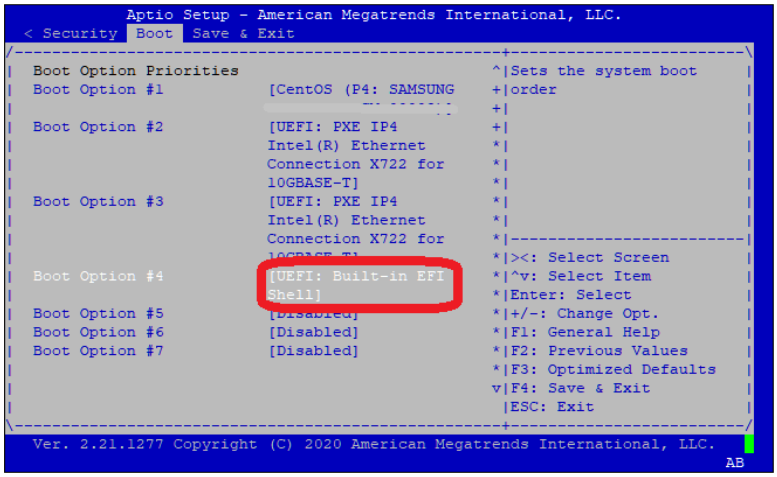
10.5.4. Entrer dans le menu BIOS au prochain démarrage en utilisant IPMI

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL. Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

Étape_1	Exécuter la commande suivante pour entrer automatiquement dans le menu BIOS au prochain démarrage. InviteSE_ServeurLocal:~# **ipmitool chassis bootdev bios**	`$ ipmitool chassis bootdev bios` `Set Boot Device to bios`

10.5.5. Activer l'option pour réessayer indéfiniment la séquence de démarrage lorsque le module de support de compatibilité (CSM) est désactivé

Voir Accéder au BIOS pour les instructions d'accès.

Étape_1	Pour pouvoir réessayer indéfiniment la séquence de démarrage, le shell EFI doit être désactivé dans la liste des options de démarrage.	

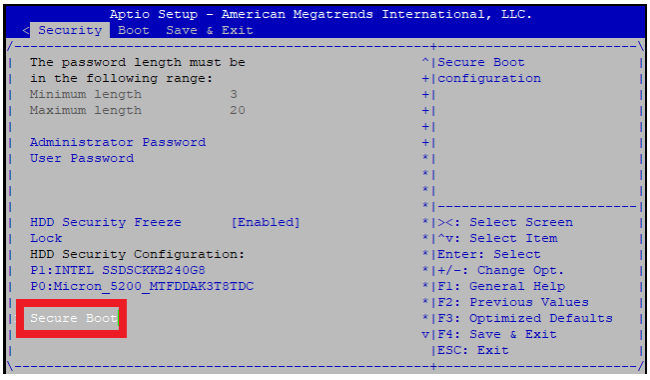
10.5.6. Configurer l'effacement sécurisé

Voir Accéder au BIOS pour les instructions d'accès.

Étape_1	Dans le menu de configuration du BIOS, sélectionner le menu **Security** et désactiver l'option **HDD Security Freeze Lock**.	
Étape_2	À l'aide des flèches du clavier, sélectionner le menu **Save & Exit**, aller à **Save Changes and Exit** et appuyer sur **Entrée** pour confirmer et enregistrer la nouvelle configuration.	
Étape_3	Utiliser la note d'application suivante pour procéder à l'effacement sécurisé du disque concerné. Effacement sécurisé (Secure Erase)	

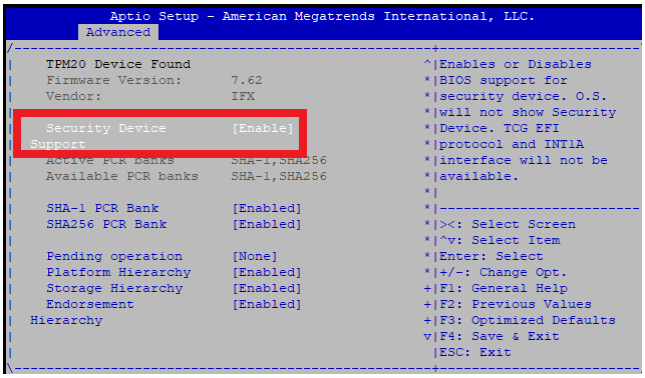
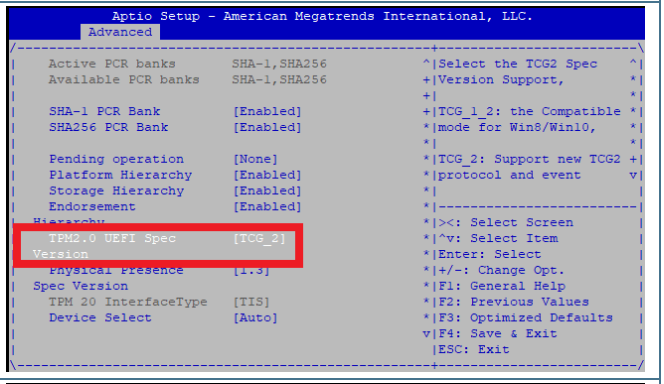
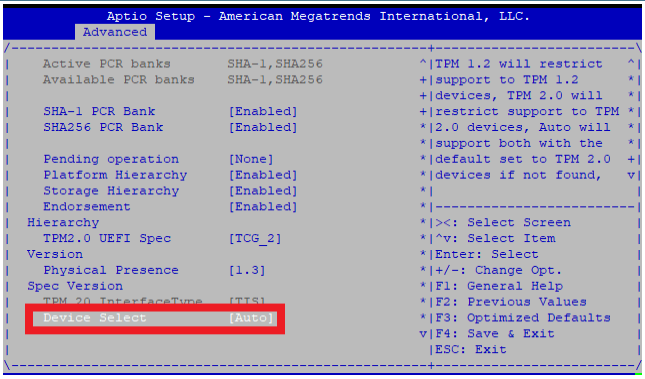
10.5.7. Activer le démarrage sécurisé

Voir Accéder au BIOS pour les instructions d'accès.

Étape_1	Accéder au sous-menu **Secure Boot** dans l'onglet **Security**.	
Étape_2	Sélectionner l'option **Secure Boot** et la mettre à **Enabled**.	
Étape_3	Utiliser les notes d'application suivantes pour générer et configurer des clés de démarrage sécurisées.	Générer des clés de démarrage sécurisé personnalisées Installer des clés de démarrage sécurisé personnalisées
Étape_4	À l'aide des flèches du clavier, sélectionner le menu **Save & Exit**, aller à **Save Changes and Exit** et appuyer sur **Entrée** pour confirmer.	

10.5.8. Configurer le TPM

Voir Accéder au BIOS pour les instructions d'accès.

Étape_1	Sélectionner le menu **Advanced**, aller à **Trusted Computing** et sélectionner **Security Device Support**. Vérifier qu'il est réglé sur **Enable**. Valeurs possibles : [**Enable** / Disable] **NOTE** : Le TPM doit être inséré pour voir le menu.	
Étape_2	Sélectionner le menu **Advanced**, aller à **Trusted Computing** et sélectionner **TPM2.0 UEFI Spec Version**. Sélectionner la spécification applicable. Valeurs possibles : [TCG_1_2 / **TCG_2**] **NOTE** : Le TPM doit être inséré pour voir le menu.	
Étape_3	Sélectionner le menu **Advanced**, aller à **Trusted Computing** et sélectionner **Device Select**. Sélectionner le périphérique applicable. Valeurs possibles : [TPM 1.2 / TPM 2.0 / **Auto**] **NOTE** : Le TPM doit être inséré pour voir le menu.	
Étape_4	À l'aide des flèches du clavier, sélectionner le menu **Save & Exit**, aller à **Save Changes and Exit** et appuyer sur **Entrée** pour confirmer.	

10.6. Personnalisation des données de la plateforme

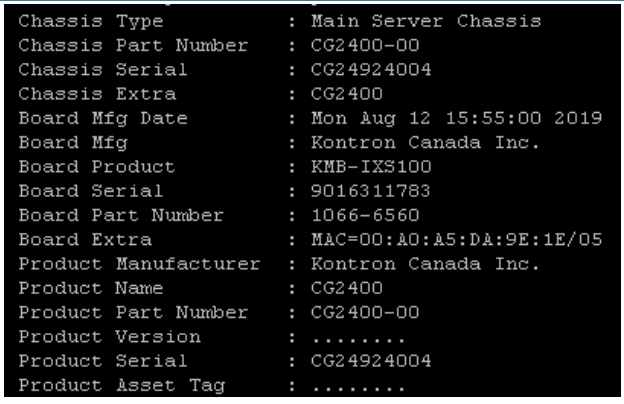
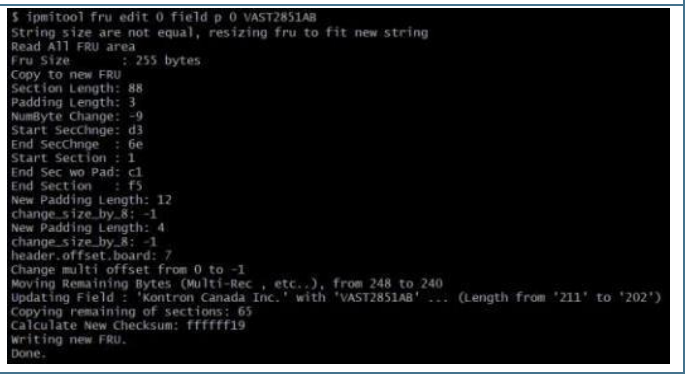
10.6.1. Personnaliser les données FRU de la plateforme en utilisant IPMI

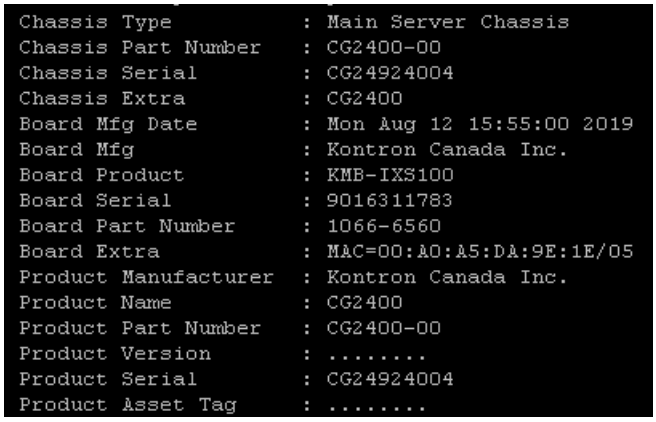
Le BMC est accessible par deux méthodes IPMI.

- Si un système d'exploitation est installé (adresse IP du BMC connue ou non), IPMI via KCS peut être utilisé. Voir Accéder au BMC en utilisant IPMI via KCS.
- Si l'adresse IP du BMC est connue (système d'exploitation installé ou non), IPMI sur LAN peut être utilisé. Voir **Erreur! Source du renvoi introuvable.**.

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL. Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

Pour les commandes servant à personnaliser les données FRU, la version d'ipmitool requise est la 1.8.13. La plus récente version d'ipmitool recommandée (1.8.18) ne donnera pas les résultats escomptés.

Étape_1	Afficher les données FRU actuelles. InviteSE_ServeurLocal:~# **ipmitool fru print**	
Étape_2	Utiliser la commande IPMI suivante pour personnaliser les données FRU. InviteSE_ServeurLocal:~# **ipmitool fru edit [ID_FRU] field [COMMANDE_FRU] [VALEUR]** **NOTE** : Voir Commandes de personnalisation des données FRU pour les commandes disponibles.	

Étape_3	Confirmer que les changements ont été correctement appliqués. InviteSE_ServeurLocal:~# **ipmitool fru print**	

10.6.2. Commandes de personnalisation des données FRU

Pour les commandes servant à personnaliser les données FRU, la version d'ipmitool requise est la 1.8.13. La plus récente version d'ipmitool recommandée (1.8.18) ne donnera pas les résultats escomptés.

10.6.2.1. Personnaliser les données relatives au produit

Commande	Donnée FRU	Exemple
p 0	Product Manufacturer	InviteSE_ServeurLocal:~# **ipmitool fru edit 0 field p 0 [VALEUR]**
p 1	Product Name	
p 2	Product Part Number	
p 3	Product Version	
p 4	Product Serial Number	
p 5	Product Asset Tag	

10.6.2.2. Personnaliser les données relatives au châssis

Commande	Donnée FRU	Exemple
c 0	Chassis Part Number	InviteSE_ServeurLocal:~# **ipmitool fru edit 0 field c 0 [VALEUR]**
c 1	Chassis Serial Number	

10.6.3. Personnaliser les logos

Il est possible de personnaliser les micrologiciels avec le logo de votre entreprise, sous certaines conditions. Communiquer avec le soutien technique ou votre représentant commercial pour de plus amples renseignements.

10.7. Intégration dans l'infrastructure réseau

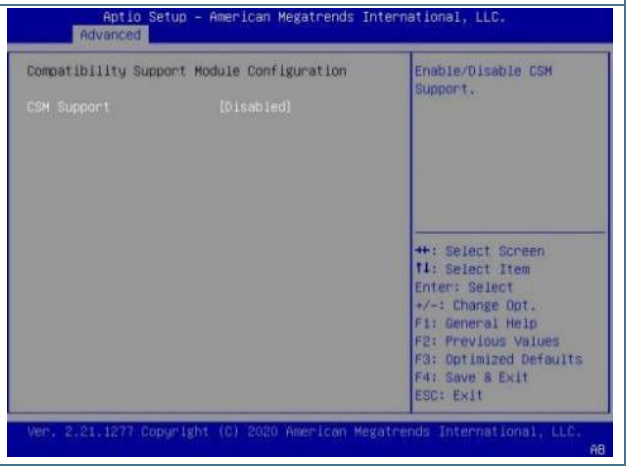
10.7.1. Configurer des VLAN

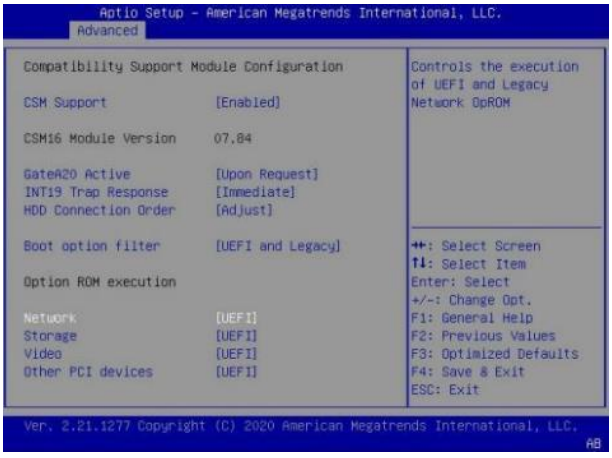
Le menu de configuration du BIOS propose des menus pour créer/configurer/supprimer des réseaux locaux virtuels (VLAN) sur chacun des deux ports 10GbE natifs. Toutefois, les menus de configuration du BIOS permettant de configurer les VLAN ne sont disponibles que lorsque les services réseau UEFI sont activés (ils ne sont pas disponibles lorsque le CSM [module de support de compatibilité] hérité est activé).

Si les services réseau UEFI ne sont pas activés, ils doivent l'être avant que les VLAN puissent être configurés.

10.7.1.1. Activer l'option Network Stack de l'UEFI et configurer le CSM

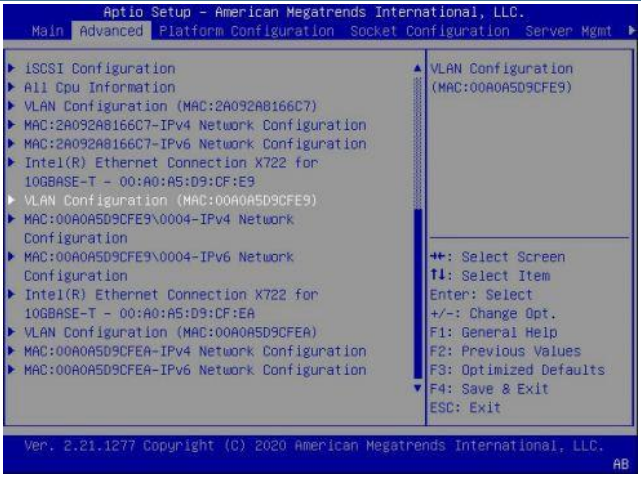
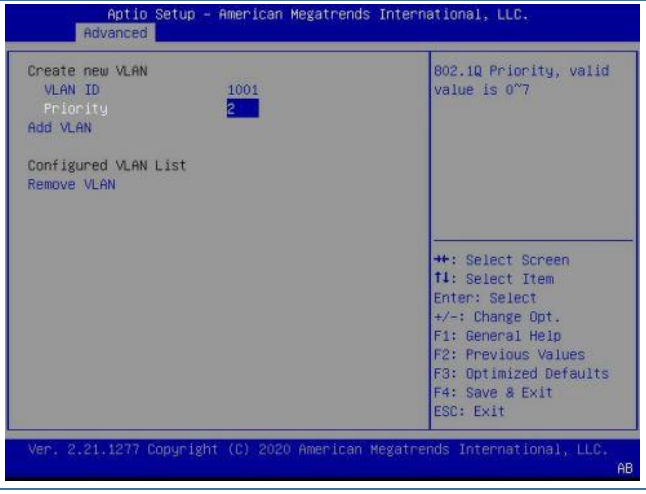
Voir Accéder au BIOS pour les instructions d'accès.

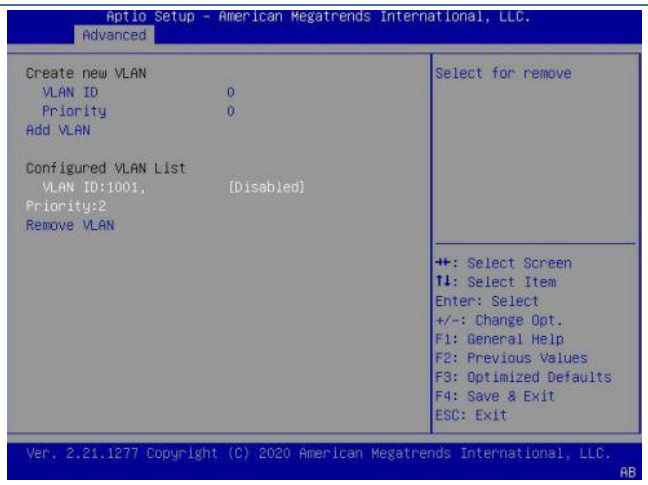
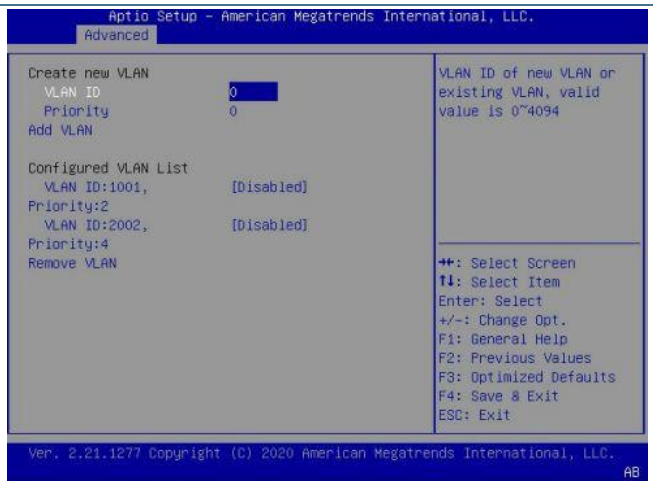
Étape_1	Dans le menu de configuration du BIOS, sélectionner le menu **Advanced** et naviguer à la section **Network Stack Configuration**. Mettre **Network Stack** à **Enabled**.	
Étape_2	Dans le menu **Advanced**, aller à la section **Compatibility Support Module Configuration**. Si l'option **CSM Support** est à **Disabled**, passer à l'étape 4. Si l'option **CSM Support** est à **Enabled**, passer à l'étape 3.	

Étape_3	Sous **Option ROM execution**, mettre **Network** à UEFI, si ce n'est pas déjà fait. **NOTE** : Les autres paramètres sous **Option ROM execution** (**Storage**, **Video**, **Other PCI devices**) doivent également être mis à UEFI (mélanger des options associées à la mémoire morte UEFI et héritées pourrait entraîner des problèmes de démarrage du système d'exploitation).	
Étape_4	Appuyer sur **F4** pour enregistrer et quitter.	

10.7.1.2. Créer des VLAN

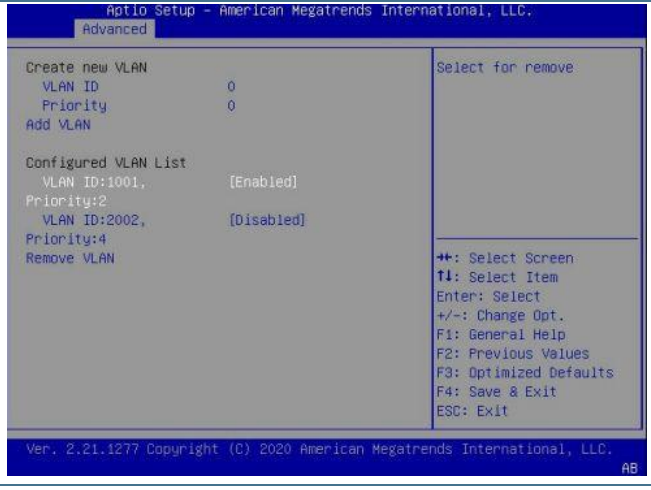
Voir Accéder au BIOS pour les instructions d'accès.

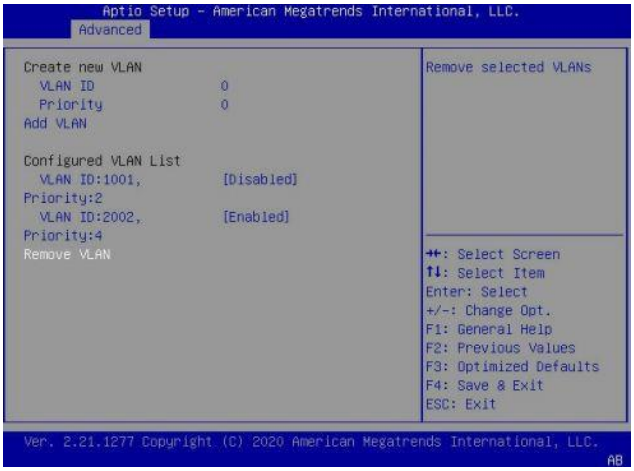
Étape_1	Dans le menu de configuration du BIOS, sélectionner le menu **Advanced** et naviguer à la section **VLAN Configuration (MAC:xxxxxxxxxxxx)**. Sélectionner **Enter Configuration Menu**. **NOTE** : L'adresse MAC sera celle du port X722 10GbE pour lequel des VLAN doivent être configurés.	
Étape_2	Créer un nouveau VLAN comme requis en définissant son identifiant et sa priorité : • **VLAN ID** : valeur comprise entre 0 et 4094 • **Priority** : valeur comprise entre 0 et 7 Dans l'exemple de la figure, VLAN ID = 1001 et Priority = 2 (802.1Q).	

Étape_3	Sélectionner **Add VLAN** pour créer un VLAN. **NOTE** : Il est aussi possible de mettre à jour l'ID d'un VLAN existant en suivant les étapes 2 et 3.	
Étape_4	Ajouter d'autres VLAN si nécessaire, en suivant les étapes 2 et 3. Exemple : VLAN ID 2002, avec une priorité 802.1Q de 4. NOTES : Les VLAN de la liste Configured VLAN List sont actifs, peu importe s'ils ont Enabled ou Disabled comme configuration. Dans cet exemple, les VLAN 1001 et 2002 sont actifs (même s'ils sont désactivés). Les paramètres (Enabled ou Disabled) des VLAN de la liste ne sont utilisés que lorsqu'un VLAN est supprimé.	
Étape_5	Répéter les étapes 1 à 4 pour définir des VLAN dans l'autre port X722 10GbE, si nécessaire.	
Étape_6	Appuyer sur F4 pour enregistrer et quitter.	

10.7.1.3. Supprimer des VLAN

Voir Accéder au BIOS pour les instructions d'accès.

Étape_1	Dans le menu de configuration du BIOS, sélectionner le menu **Advanced** et naviguer à la section **VLAN Configuration (MAC:xxxxxxxxxxxx)**. Sélectionner **Enter Configuration Menu**. **NOTE** : L'adresse MAC sera celle du port X722 10GbE pour lequel des VLAN doivent être supprimés.	

Étape_2	Mettre le statut du ou des VLAN à supprimer à **Enabled**. Une fois que tous les VLAN à supprimer sont sélectionnés, sélectionner **Remove VLAN**. Dans l'exemple de la figure, le VLAN 2002 sera supprimé et le VLAN 1001 sera maintenu.	
Étape_3	Répéter les étapes 1 à 2 pour supprimer des VLAN dans l'autre port X722 10GbE, si nécessaire.	
Étape_4	Appuyer sur **F4** pour enregistrer et quitter.	

10.8. Configuration du BMC en cas de configuration non redondante du bloc d'alimentation

La configuration par défaut de la plateforme CG2400 comprend deux blocs d'alimentation redondants. Si la configuration finale du système n'utilise qu'un seul bloc d'alimentation, le BMC doit être reconfiguré.

NOTICE

La plateforme ne sera pas totalement saine si le BMC n'est pas reconfiguré en fonction du nombre réel de blocs d'alimentation utilisés. La plateforme enverra des messages d'état défaillant en raison d'un composant manquant (bloc d'alimentation) prévu dans la configuration par défaut. Ces messages pourraient inclure :

- Les ventilateurs du système qui fonctionnent à leur vitesse maximale en tout temps
- Les DEL du panneau avant qui indiquent des états d'alarme (DEL d'état du système)
- États défaillants dans le Journal des événements système

Sections pertinentes :

Installation et assemblage des composants

Guide de démarrage – installation de l'application et évaluation des performances

Le BMC est accessible par deux méthodes IPMI.

- Si un système d'exploitation est installé (adresse IP du BMC connue ou non), IPMI via KCS peut être utilisé. Voir Accéder au BMC en utilisant IPMI via KCS.
- Si l'adresse IP du BMC est connue (système d'exploitation installé ou non), IPMI sur LAN peut être utilisé. Voir **Erreur! Source du renvoi introuvable.**.

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL. Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

Étape_1	Inscrire le nombre de redondances. Si un seul bloc d'alimentation est utilisé, la valeur est de 1. InviteSE_ServeurLocal:~# **ipmitool -H 192.168.1.10 -I lanplus -U admin -P admin raw 0x3c 0x02 0x00 0x01 0x00 0x01**
Étape_2	Lire le nombre de redondances pour confirmer la modification. La réponse devrait être 1. InviteSE_ServeurLocal:~# **ipmitool -H 192.168.1.10 -I lanplus -U admin -P admin raw 0x3c 0x02 0x00 0x00 0x00**

11/ Accès aux composants de la plateforme

11.1. Accéder au système d'exploitation d'un serveur

Un système d'exploitation est accessible par différentes méthodes :

- En utilisant le KVM (écran-clavier-souris)
- En utilisant le port d'affichage (VGA) – il s'agit de la méthode recommandée pour la configuration initiale d'un système sorti de son emballage
- En utilisant les protocoles SSH, RDP et des applications clients
- En utilisant série sur LAN (SOL)
- En utilisant une console série (connexion physique)

Voir Description des méthodes d'accès au système pour plus d'informations sur les différentes méthodes d'accès.

11.1.1. Accéder à un système d'exploitation en utilisant le KVM

11.1.1.1. Préalables

1	Un système d'exploitation est installé.
2	L'adresse IP du BMC est connue (voir la section Configuration > Contrôleur de gestion de carte mère – BMC pour obtenir le paramètre IP_GESTION_BMC).
3	L'ordinateur distant a accès au sous-réseau du réseau de gestion.

Section pertinente :

Contrôleur de gestion de carte mère – BMC

11.1.1.2. Considérations relatives au navigateur

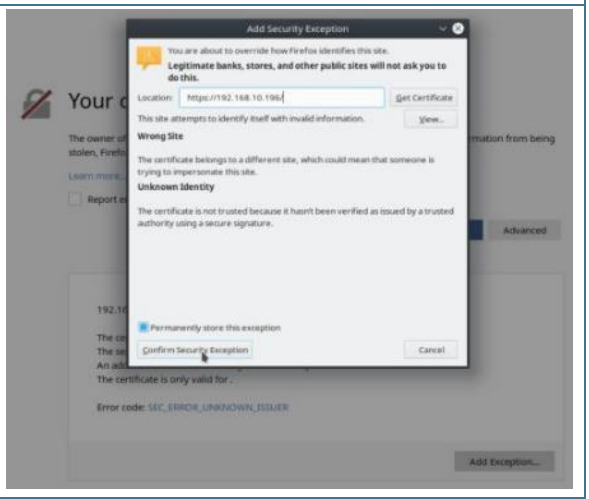
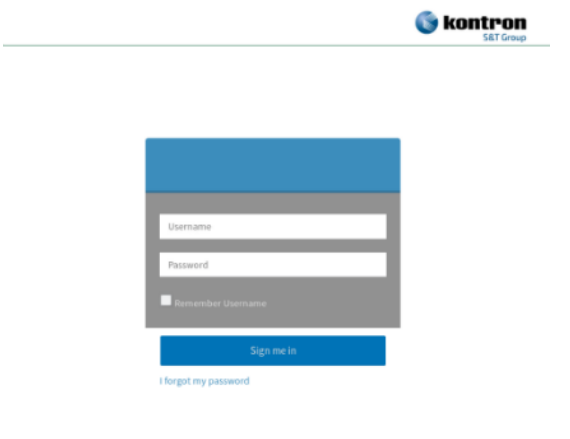
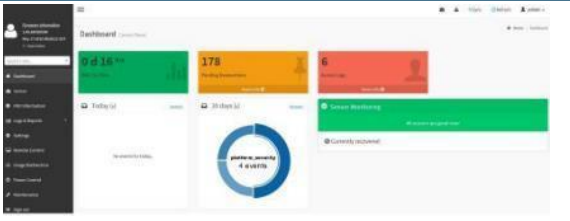
HTML5	Pour établir une communication avec l'interface utilisateur Web, un navigateur Web prenant en charge HTML5 est nécessaire.
Certificat auto-signé HTTPS	Lors de l'établissement d'une connexion à l'interface Web, il est obligatoire d'accepter le certificat auto-signé HTTPS. Pour plus d'information sur l'acceptation des certificats auto-signés HTTPS, se reporter à la documentation du navigateur Web.
Autorisation de téléchargement de fichiers	Le téléchargement de fichiers à partir du site doit être autorisé. Pour plus d'information sur les autorisations de téléchargement de fichiers, se reporter à la documentation du navigateur Web.
Témoins	Les témoins doivent être activés pour pouvoir accéder au site Web. Pour plus d'information sur l'activation des témoins, se reporter à la documentation du navigateur Web.

NOTE : La procédure peut varier selon le navigateur utilisé. Les exemples fournis utilisent Firefox.

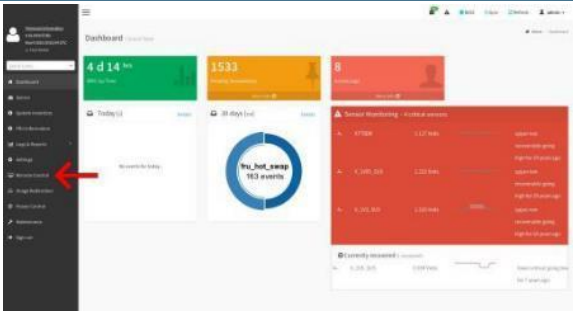
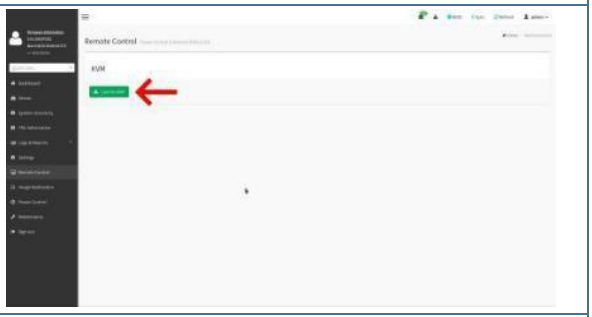
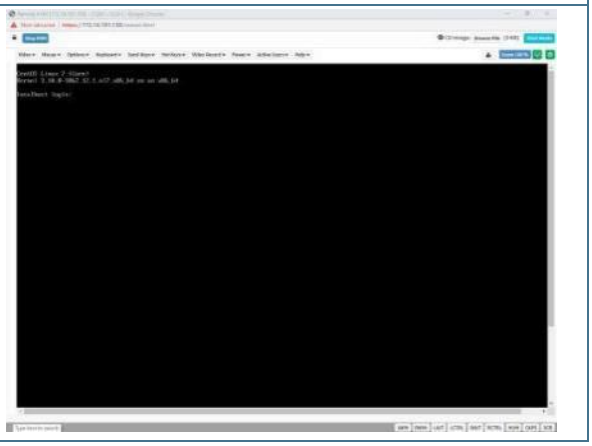
11.1.1.3. Procédure d'accès

11.1.1.3.1. Accéder au BMC du serveur pour lequel vous souhaitez accéder au système d'exploitation

Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut.

Étape_1	À partir d'un ordinateur distant ayant accès au réseau de gestion, ouvrir une fenêtre de navigateur et entrer l'adresse IP découverte pour le BMC. **NOTE : Le préfixe HTTPS est obligatoire.** *https://[IP_GESTION_BMC]*	
Étape_2	Cliquer sur **Advanced** pour lancer le processus d'acceptation du certificat auto-signé HTTPS. De l'information sur le message d'erreur s'affichera.	
Étape_3	Cliquer sur **Add Exception...** La fenêtre contextuelle Add Security Exception s'affichera. Cliquer sur **Confirm Security Exception** pour autoriser le navigateur à accéder à l'interface utilisateur Web de gestion de cette interface.	
Étape_4	Ouvrir une session dans l'interface utilisateur Web du BMC à l'aide des données d'accès appropriées. **NOTE** : Le nom d'utilisateur et le mot de passe par défaut de l'interface utilisateur Web sont admin/admin.	
Étape_5	Vous avez maintenant accès à l'interface utilisateur Web de gestion du BMC. Vous pouvez utiliser l'interface.	

11.1.1.3.2. Lancer le KVM

Étape_1	Dans le menu de gauche, cliquer sur **Remote Control**.	
Étape_2	Dans le menu **Remote Control**, cliquer sur le bouton **Launch KVM**.	
Étape_3	Une nouvelle fenêtre de navigateur s'ouvre et affiche l'écran du serveur. **NOTE** : Si un système d'exploitation est installé, l'image affichée pourrait être celle du système d'exploitation.	

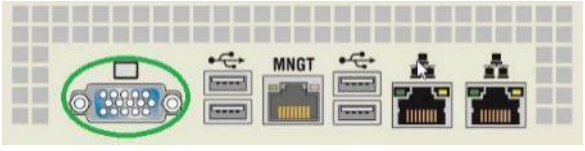
Si le système d'exploitation n'est pas affiché, effectuer une réinitialisation du serveur comme décrit dans la section Envoyer une commande d'alimentation en utilisant l'interface utilisateur Web. Relancer ensuite le KVM.

11.1.2. Accéder à un système d'exploitation en utilisant le port d'affichage (VGA)

11.1.2.1. Préalables

1	Un système d'exploitation est installé.
2	Une connexion physique au port d'affichage VGA de l'appareil est requise.
3	Une souris et/ou un clavier sont connectés.

Figure 32. Emplacement du port VGA



11.1.2.2. Procédure d'accès

Étape_1	Connecter le câble VGA au moniteur et à la plateforme.
Étape_2	L'écran du système d'exploitation devrait s'afficher sur le moniteur.

11.1.3. Accéder à un système d'exploitation en utilisant le protocole SSH, RDP ou des applications clients

11.1.3.1. Préalables

1	Un système d'exploitation est installé.
2	L'adresse IP du système d'exploitation est connue.
3	L'ordinateur distant a accès au sous-réseau du système d'exploitation.

11.1.3.2. Procédure d'accès

Étape_1	En utilisant l'adresse IP du système d'exploitation, utiliser la méthode d'accès à distance de votre choix.

11.1.4. Accéder à un système d'exploitation en utilisant série sur LAN (SOL)

11.1.4.1. Préalables

1	Un système d'exploitation est installé.
2	L'adresse IP du BMC est connue (voir la section Configuration > Contrôleur de gestion de carte mère – BMC pour obtenir le paramètre IP_GESTION_BMC).
3	L'ordinateur distant a accès au sous-réseau du réseau de gestion.
4	Une version de la communauté d'ipmitool est installée sur un ordinateur distant pour permettre la surveillance à distance – il est recommandé d'utiliser la version 1.8.18 d'ipmitool.

Sections pertinentes :

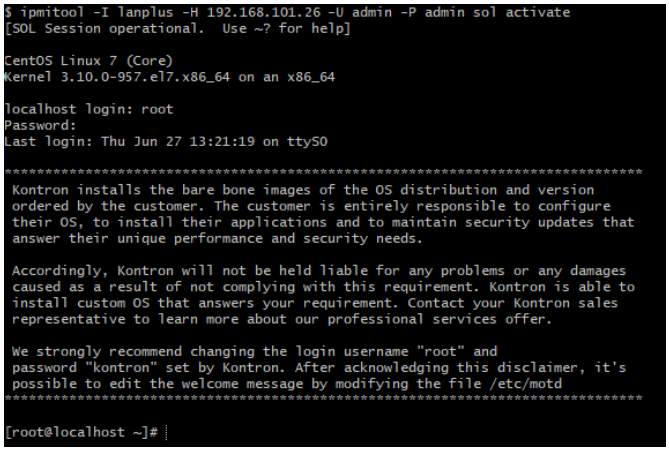
Contrôleur de gestion de carte mère – BMC

Installation des logiciels courants

11.1.4.2. Procédure d'accès

Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, ouvrir l'invite de commande et désactiver toutes les sessions SOL précédentes. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] sol deactivate**	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin sol deactivate`

Étape_2	Activer une session SOL. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] sol activate**	
Étape_3	L'écran de démarrage du système d'exploitation s'affiche.	

NOTE : Si le système d'exploitation n'est pas affiché, réinitialisez le serveur. Voir Gestion de l'alimentation de la plateforme.

11.1.5. Accéder au système d’exploitation à l'aide d’une console série (connexion physique)

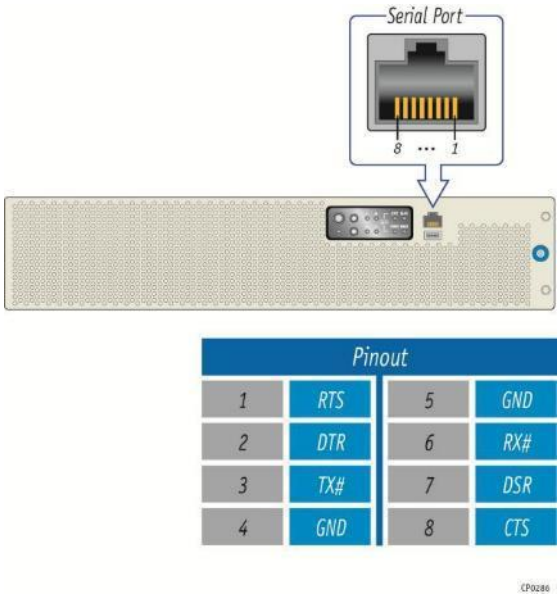
11.1.5.1. Préalables

1	Un système d'exploitation est installé.
2	Une connexion physique à l'appareil est requise. NOTE : Le port de console série est compatible avec le câble 72-3383-01 de Cisco.
3	Un outil de console série est installé sur l'ordinateur distant. Vitesse (baud) : 115200 • Bits d'information : 8 • Bits d'arrêt : 1 • Parité : Aucune • Contrôle de flux : Aucun • Mode émulation recommandé : VT100+ **NOTE** : PuTTY est recommandé.
4	La redirection vers le port série est configurée dans le système d'exploitation. **NOTE** : Si le système d’exploitation a été installé par Kontron, la redirection de la console est activée par défaut.

Section pertinente :

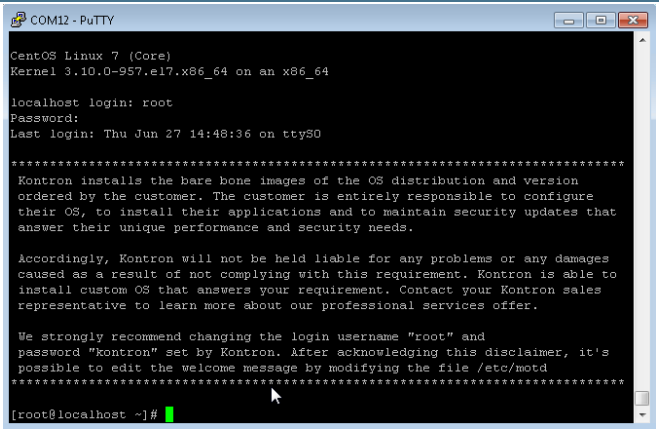
Contrôleur de gestion de carte mère – BMC

Figure 33. Emplacement du port série



11.1.5.2. Procédure d'accès

Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut.

Étape_1	À partir d'un ordinateur disposant d'une connexion physique au port série, ouvrir un outil de console série et démarrer la communication entre la console et le port auquel le système est connecté.	
Étape_2	L'écran de démarrage du système d'exploitation s'affiche.	

NOTE : Si le système d'exploitation n'est pas affiché, réinitialisez le serveur. Voir Gestion de l'alimentation de la plateforme.

11.2. Accéder au BIOS

Le BIOS est accessible par différentes méthodes :

- En utilisant le KVM (écran-clavier-souris)
- En utilisant le port d'affichage (VGA) – il s'agit de la méthode recommandée pour la configuration initiale d'un système sorti de son emballage
- En utilisant série sur LAN (SOL)
- En utilisant une console série (connexion physique)

Voir Description des méthodes d'accès au système pour plus d'informations sur les différentes méthodes d'accès.

11.2.1. Accéder au BIOS en utilisant le KVM

11.2.1.1. Préalables

1	L'adresse IP du BMC est connue (voir la section Configuration > Contrôleur de gestion de carte mère – BMC pour obtenir le paramètre IP_GESTION_BMC).
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.

Section pertinente :

Contrôleur de gestion de carte mère – BMC

11.2.1.2. Considérations relatives au navigateur

HTML5	Pour établir une communication avec l'interface utilisateur Web, un navigateur Web prenant en charge HTML5 est nécessaire.
Certificat auto-signé HTTPS	Lors de l'établissement d'une connexion à l'interface Web, il est obligatoire d'accepter le certificat auto-signé HTTPS. Pour plus d'information sur l'acceptation des certificats auto-signés HTTPS, se reporter à la documentation du navigateur Web.
Autorisation de téléchargement de fichiers	Le téléchargement de fichiers à partir du site doit être autorisé. Pour plus d'information sur les autorisations de téléchargement de fichiers, se reporter à la documentation du navigateur Web.
Témoins	Les témoins doivent être activés pour pouvoir accéder au site Web. Pour plus d'information sur l'activation des témoins, se reporter à la documentation du navigateur Web.

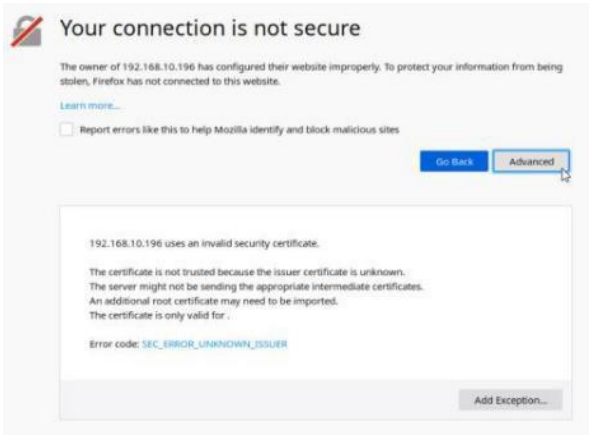
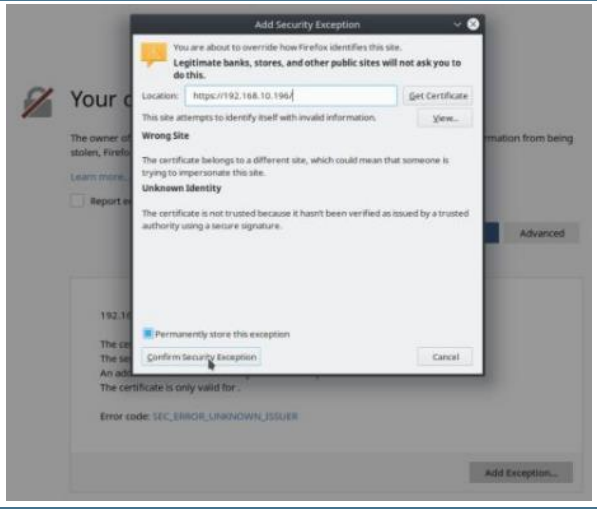
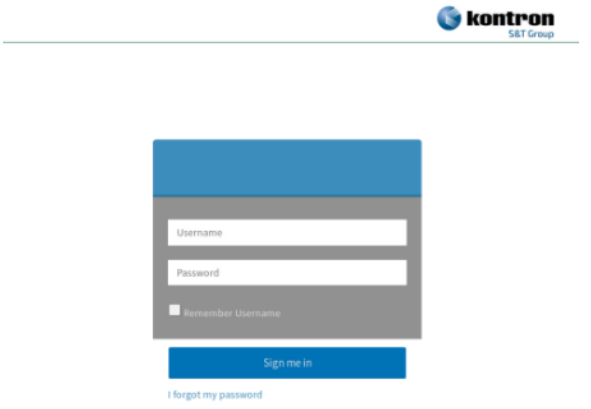
NOTE : La procédure peut varier selon le navigateur utilisé. Les exemples fournis utilisent Firefox.

11.2.1.3. Procédure d'accès

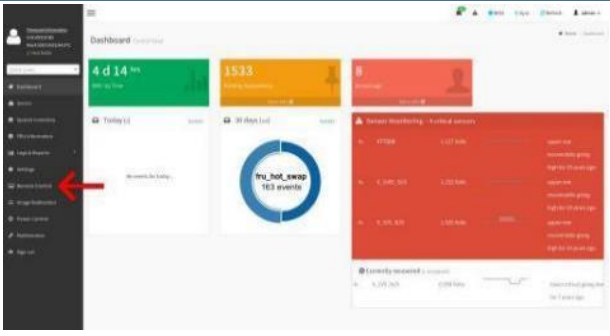
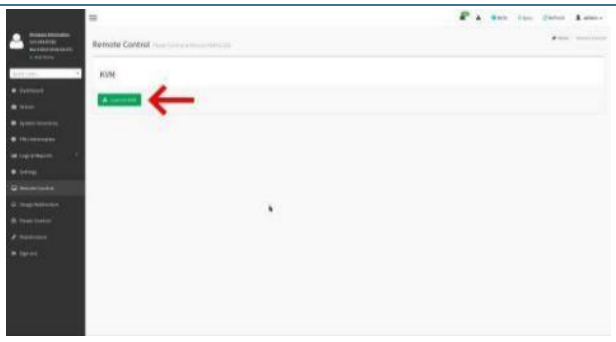
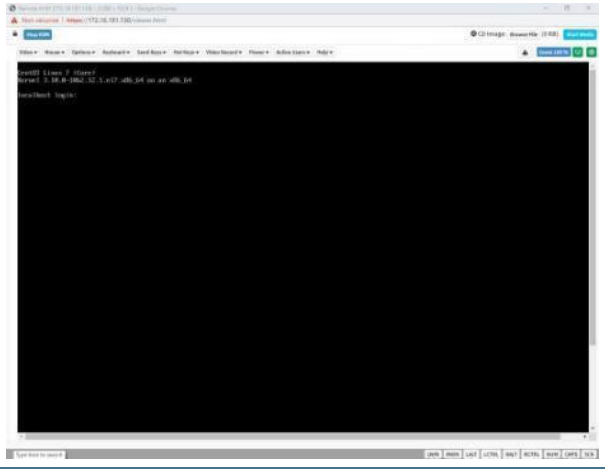
11.2.1.3.1. Accéder au BMC du serveur pour lequel vous souhaitez accéder au BIOS

Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut.

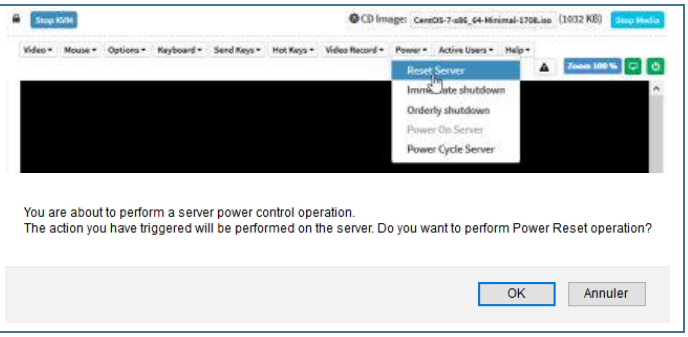
Étape_1	À partir d'un ordinateur distant ayant accès au réseau de gestion, ouvrir une fenêtre de navigateur et entrer l'adresse IP découverte pour le BMC. **NOTE : Le préfixe HTTPS est obligatoire.** *https://[IP_GESTION_BMC]*

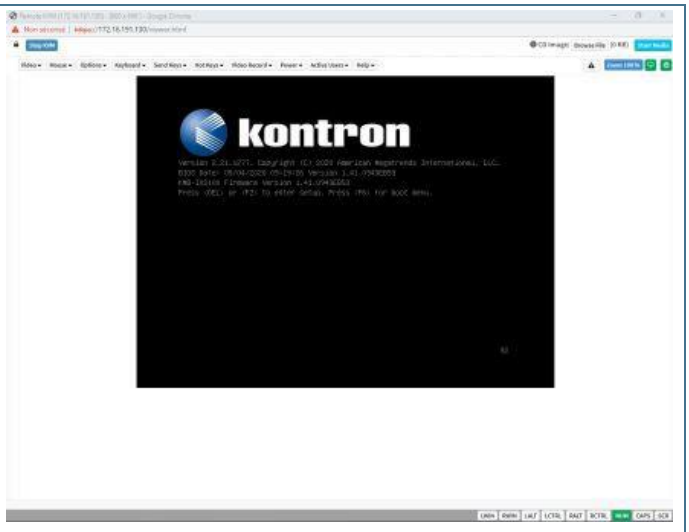
Étape_2	Cliquer sur **Advanced** pour lancer le processus d'acceptation du certificat auto-signé HTTPS. De l'information sur le message d'erreur s'affichera.	
Étape_3	Cliquer sur **Add Exception...** La fenêtre contextuelle Add Security Exception s'affichera. Cliquer sur **Confirm Security Exception** pour autoriser le navigateur à accéder à l'interface utilisateur Web de gestion de cette interface.	
Étape_4	Ouvrir une session dans l'interface utilisateur Web du BMC à l'aide des données d'accès appropriées. **NOTE** : Le nom d'utilisateur et le mot de passe par défaut de l'interface utilisateur Web sont admin/admin.	
Étape_5	Vous avez maintenant accès à l'interface utilisateur Web de gestion du BMC. Vous pouvez utiliser l'interface.	

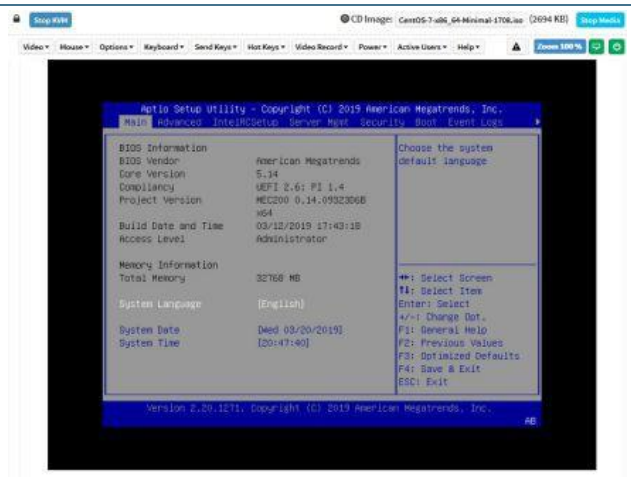
11.2.1.3.2. Lancer le KVM

Étape_1	Dans le menu de gauche, cliquer sur **Remote Control**.	
Étape_2	Dans le menu **Remote Control**, cliquer sur le bouton **Launch KVM**.	
Étape_3	Une nouvelle fenêtre de navigateur s'ouvre et affiche l'écran du serveur. **NOTE** : Si un système d'exploitation est installé, l'image affichée pourrait être celle du système d'exploitation.	

11.2.1.3.3. Accéder au menu de configuration du BIOS

Étape_1	Dans le menu déroulant **Power**, sélectionner **Reset Server** pour accéder au menu BIOS. Cliquer sur **OK** pour confirmer l'opération. **NOTE** : Lorsqu'une commande de réinitialisation du serveur est lancée, quelques secondes peuvent s'écouler avant que l'écran d'accueil du BIOS ne s'affiche.	

Étape_2	Lorsque l'écran d'accueil du BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration du BIOS. **NOTE** : Il peut s'écouler quelques secondes avant que l'écran d'accueil du BIOS n'affiche le message de confirmation "Entering Setup…". **Conseil :** Certains utilisateurs appuient plusieurs fois et très rapidement sur Échap/F2 (DEL/F2) pour s'assurer que le serveur attrape la touche et entre dans le menu de configuration du BIOS. Cela peut entraîner l'affichage du message suivant sur l'écran du KVM : **HID Queue is about to get full. Kindly hold on a second(s)...** Kontron suggère de modifier le paramètre **Setup Prompt Timeout** pour donner aux utilisateurs plus de temps pour réagir. Maintenir l'attention (monotâche) sur la fenêtre KVM est également une bonne pratique pour entrer dans le menu de configuration du BIOS chaque fois que c'est nécessaire. Le paramètre **Setup Prompt Timeout** se trouve dans l'onglet Boot du menu de configuration du BIOS. La valeur par défaut est de 1 seconde. La changer pour une valeur comprise entre 3 et 10 secondes constitue une bonne cible.	
Étape_3	L'écran d'accueil du BIOS affiche "Entering Setup...". **NOTE** : L'affichage et l'entrée dans le menu de configuration du BIOS prendront quelques secondes.	

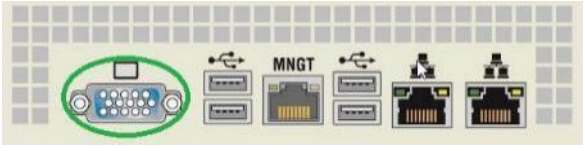
Étape_4	Le menu de configuration du BIOS s'affiche.	

11.2.2. Accéder au BIOS en utilisant le port d'affichage (VGA)

11.2.2.1. Préalables

1	Une connexion physique au port d'affichage VGA de l'appareil est requise.
2	Une souris et/ou un clavier sont connectés.

Figure 34. Emplacement du port VGA



11.2.2.2. Procédure d'accès

Étape_1	Connecter le câble VGA au moniteur et à la plateforme.
Étape_2	Réinitialiser la plateforme.
Étape_3	L'écran du BIOS devrait s'afficher sur le moniteur.

11.2.3. Accéder au BIOS en utilisant série sur LAN (SOL)

11.2.3.1. Préalables

1	L'adresse IP du BMC est connue (voir la section Configuration > Contrôleur de gestion de carte mère – BMC pour obtenir le paramètre IP_GESTION_BMC).
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.
3	Une version de la communauté d'ipmitool est installée sur un ordinateur distant pour permettre la surveillance à distance – il est recommandé d'utiliser la version 1.8.18 d'ipmitool.

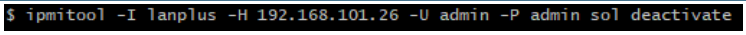
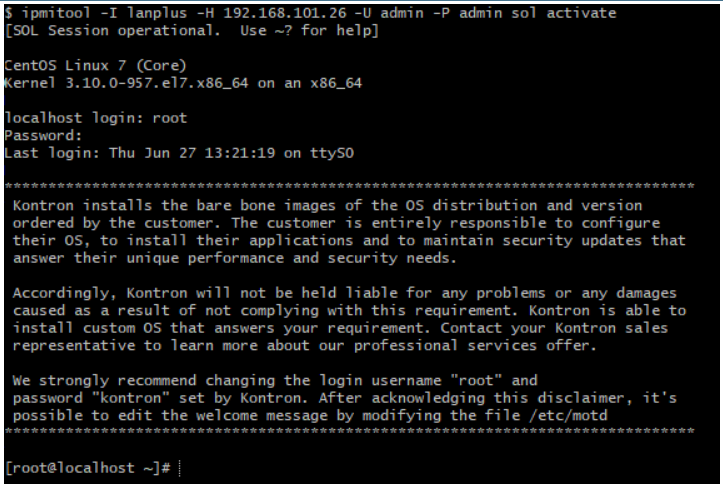
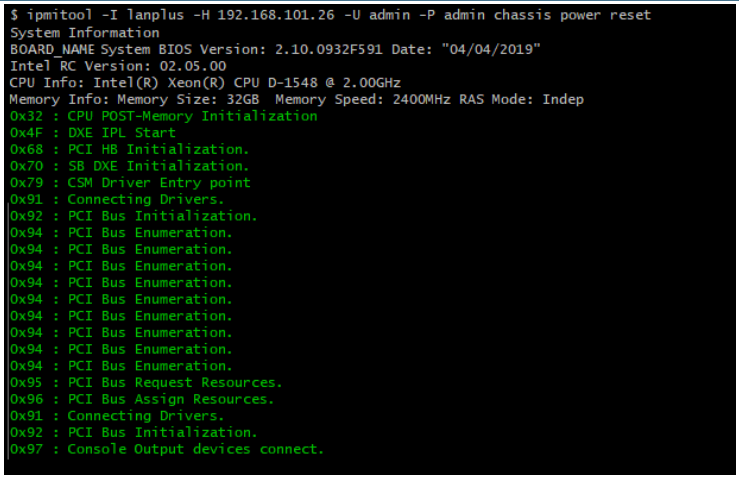
Sections pertinentes :

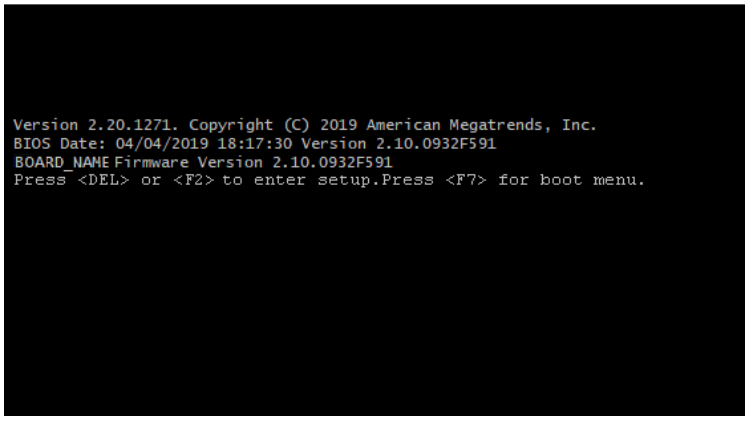
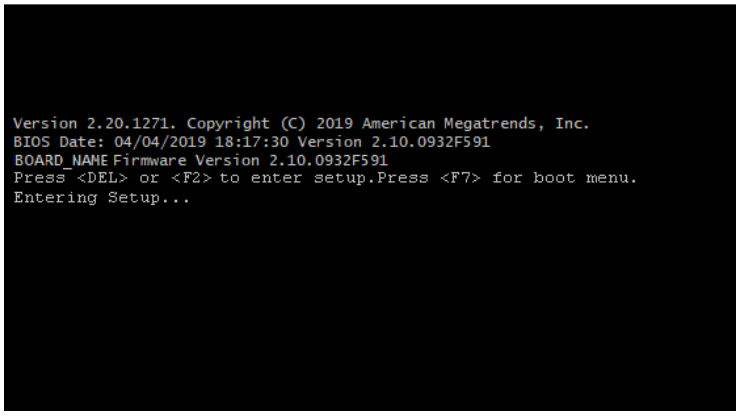
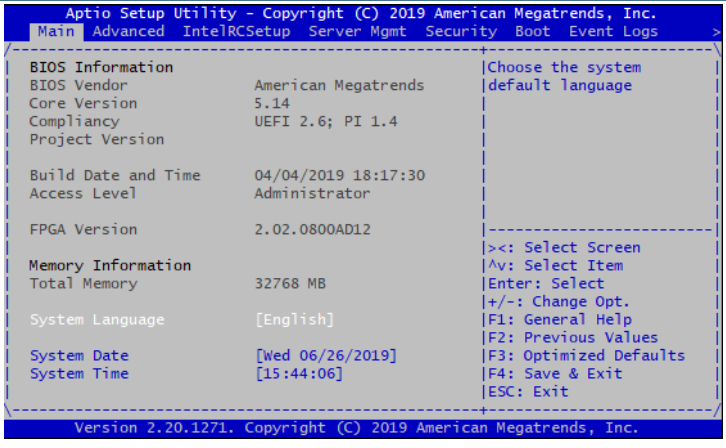
Contrôleur de gestion de carte mère – BMC

Installation des logiciels courants

11.2.3.2. Procédure d'accès

Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, ouvrir l'invite de commande du système d'exploitation et désactiver toutes les sessions SOL précédentes. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] sol deactivate**	
Étape_2	Activer une session SOL. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] sol activate** **NOTE** : Il pourrait être nécessaire d'appuyer sur la touche **Entrée** pour que l'écran du système d'exploitation s'affiche.	
Étape_3	Réinitialiser le serveur. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] chassis power reset** **NOTE** : Lorsqu'une commande de réinitialisation du serveur est lancée, quelques secondes peuvent s'écouler avant que l'écran d'accueil du BIOS ne s'affiche.	

Étape_4	Lorsque l'écran d'accueil du BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration du BIOS. **NOTE** : Il peut s'écouler quelques secondes avant que l'écran d'accueil du BIOS n'affiche le message de confirmation "Entering Setup...".	
Étape_5	L'écran d'accueil du BIOS affiche "Entering Setup...". **NOTE** : L'affichage et l'entrée dans le menu de configuration du BIOS prendront quelques secondes.	
Étape_6	Le menu de configuration du BIOS s'affiche.	

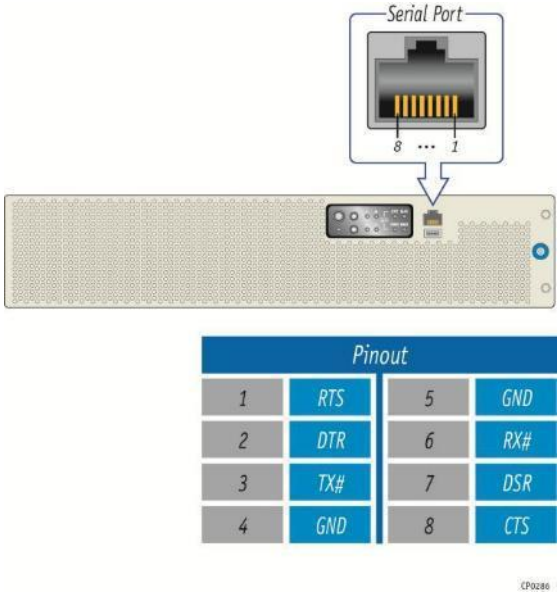
11.2.4. Accéder au BIOS à l'aide d'une console série (connexion physique)

11.2.4.1. Préalables

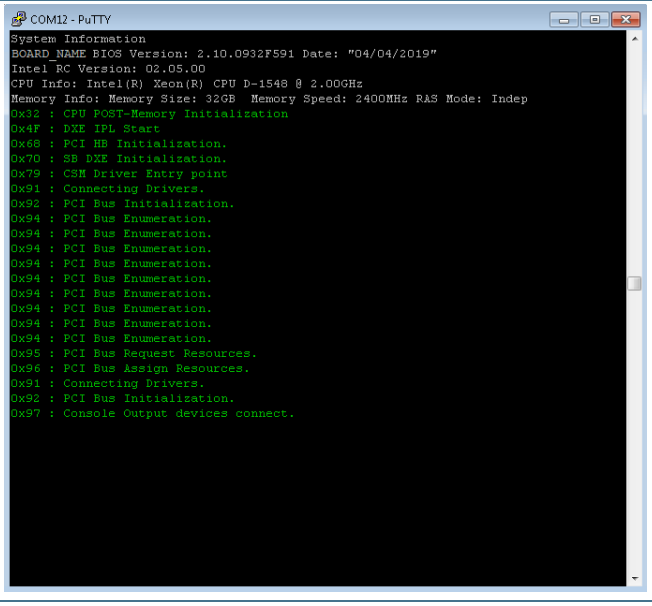
1	Une connexion physique à l'appareil est requise. **NOTE** : Le port de console série est compatible avec le câble 72-3383-01 de Cisco.

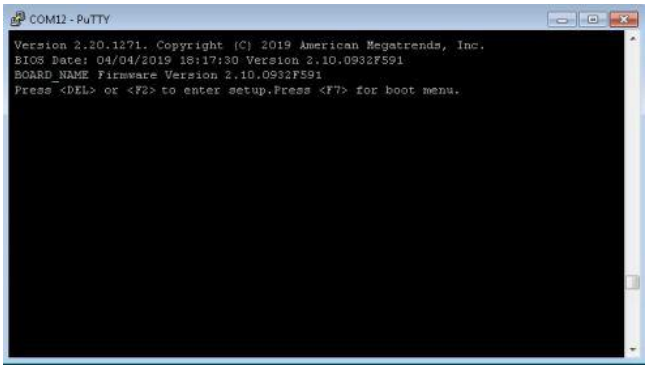
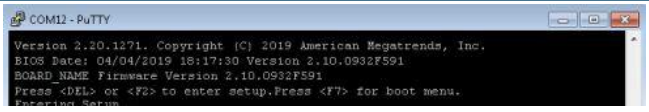
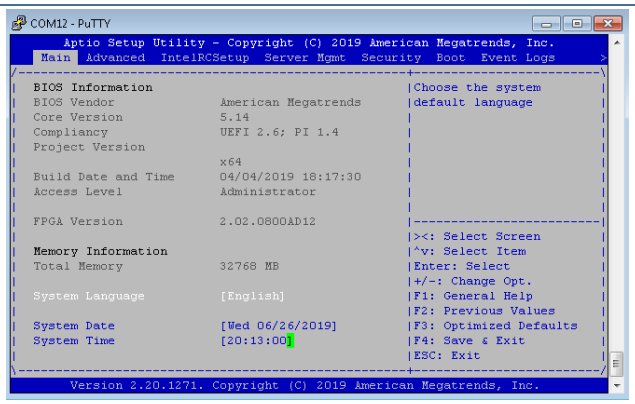
2	Un outil de console série est installé sur l'ordinateur distant. Vitesse (baud) : 115200 • Bits d'information : 8 • Bits d'arrêt : 1 • Parité : Aucune • Contrôle de flux : Aucun • Mode émulation recommandé : VT100+ **NOTE** : PuTTY est recommandé.

Figure 35. Emplacement du port série



11.2.4.2. Procédure d'accès

Étape_1	À partir d'un ordinateur disposant d'une connexion physique au port série, ouvrir un outil de console série et démarrer la communication entre la console et le port auquel le système est connecté.	
Étape_2	Réinitialiser le serveur (raccourci-clavier **Ctrl-Pause** [Ctrl-Break]). **NOTE** : Si un système d'exploitation est installé, le raccourci-clavier pourrait ne pas fonctionner correctement. Si c'est le cas, réinitialiser le serveur en suivant les recommandations propres au système d'exploitation. **NOTE** : Lorsqu'une commande de réinitialisation du serveur est lancée, quelques secondes peuvent s'écouler avant que l'écran d'accueil du BIOS ne s'affiche.	

Étape_3	Lorsque l'écran d'accueil du BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration du BIOS. **NOTE** : Il peut s'écouler quelques secondes avant que l'écran d'accueil du BIOS n'affiche le message de confirmation "Entering Setup...".	
Étape_4	L'écran d'accueil du BIOS affiche "Entering Setup...". **NOTE** : L'affichage et l'entrée dans le menu de configuration du BIOS prendront quelques secondes.	
Étape_5	Le menu de configuration du BIOS s'affiche.	

11.3. Accéder au BMC

Un BMC est accessible par différentes méthodes :

- En utilisant l'interface utilisateur Web – il s'agit de la méthode recommandée pour la configuration initiale d'un système sorti de son emballage
- En utilisant IPMI sur LAN (IOL)
- En utilisant IPMI via KCS
- En utilisant SNMP
- En utilisant Redfish

Voir Description des méthodes d'accès au système pour plus d'informations sur les différentes méthodes d'accès.

11.3.1. Accéder au BMC en utilisant l'interface utilisateur Web

11.3.1.1. Préalables

1	L'adresse IP du BMC est connue (voir la section Configuration > Contrôleur de gestion de carte mère – BMC pour obtenir le paramètre IP_GESTION_BMC).
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.

Section pertinente :

Contrôleur de gestion de carte mère – BMC

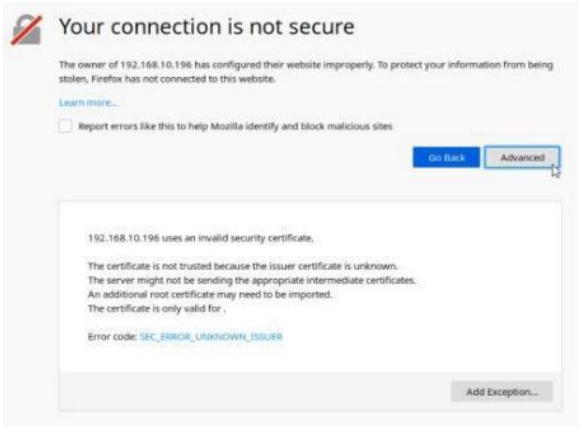
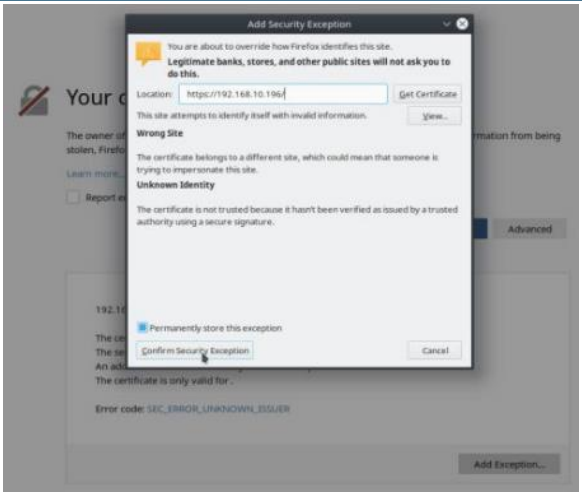
11.3.1.2. Considérations relatives au navigateur

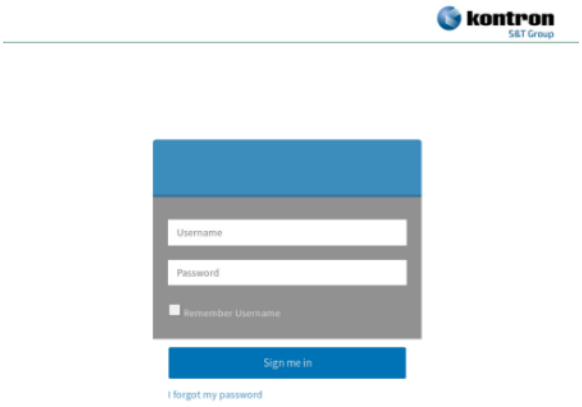
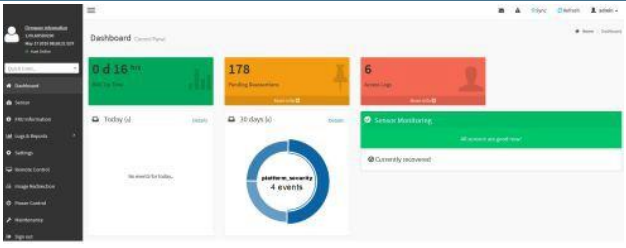
HTML5	Pour établir une communication avec l'interface utilisateur Web, un navigateur Web prenant en charge HTML5 est nécessaire.
Certificat auto-signé HTTPS	Lors de l'établissement d'une connexion à l'interface Web, il est obligatoire d'accepter le certificat auto-signé HTTPS. Pour plus d'information sur l'acceptation des certificats auto-signés HTTPS, se reporter à la documentation du navigateur Web.
Autorisation de téléchargement de fichiers	Le téléchargement de fichiers à partir du site doit être autorisé. Pour plus d'information sur les autorisations de téléchargement de fichiers, se reporter à la documentation du navigateur Web.
Témoins	Les témoins doivent être activés pour pouvoir accéder au site Web. Pour plus d'information sur l'activation des témoins, se reporter à la documentation du navigateur Web.

NOTE : La procédure peut varier selon le navigateur utilisé. Les exemples fournis utilisent Firefox.

11.3.1.3. Procédure d'accès

Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut.

Étape_1	À partir d'un ordinateur distant ayant accès au réseau de gestion, ouvrir une fenêtre de navigateur et entrer l'adresse IP découverte pour le BMC. **NOTE : Le préfixe HTTPS est obligatoire.** *https://[IP_GESTION_BMC]*	
Étape_2	Cliquer sur **Advanced** pour lancer le processus d'acceptation du certificat auto-signé HTTPS. De l'information sur le message d'erreur s'affichera.	
Étape_3	Cliquer sur **Add Exception...** La fenêtre contextuelle Add Security Exception s'affichera. Cliquer sur **Confirm Security Exception** pour autoriser le navigateur à accéder à l'interface utilisateur Web de gestion de cette interface.	

Étape_4	Ouvrir une session dans l'interface utilisateur Web du BMC à l'aide des données d'accès appropriées. **NOTE** : Le nom d'utilisateur et le mot de passe par défaut de l'interface utilisateur Web sont admin/admin.	
Étape_5	Vous avez maintenant accès à l'interface utilisateur Web de gestion du BMC. Vous pouvez utiliser l'interface.	

11.3.2. Accéder au BMC en utilisant IPMI sur LAN (IOL)

11.3.2.1. Préalables

1	L'adresse IP du BMC est connue.
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.
3	Une version de la communauté d'ipmitool est installée sur un ordinateur distant pour permettre la surveillance à distance – il est recommandé d'utiliser la version 1.8.18 d'ipmitool.

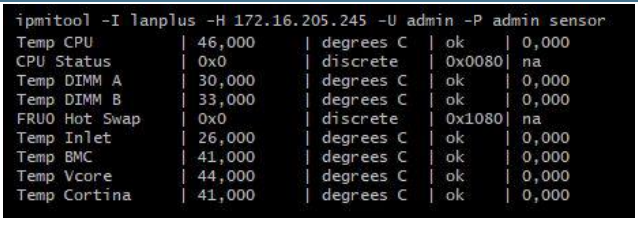
Sections pertinentes :

Contrôleur de gestion de carte mère – BMC

Installation des logiciels courants

11.3.2.2. Procédure d'accès

Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, saisir la commande souhaitée. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] [COMMANDE_IPMI]**	

Pour une liste des Commandes IPMI prises en charge, voir Commandes IPMI prises en charge.

Pour une liste de tous les capteurs, voir Liste des capteurs.

11.3.3. Accéder au BMC en utilisant IPMI via KCS

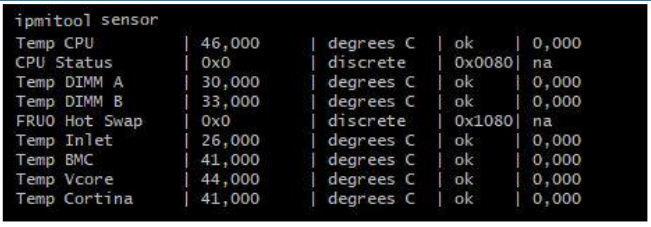
11.3.3.1. Préalables

1	Un système d'exploitation est installé.
2	L'ordinateur distant a accès au système d'exploitation du serveur (SSH/RDP/port série de la plateforme).
3	Une version de la communauté d'ipmitool est installée sur le serveur local pour permettre la surveillance locale – il est recommandé d'utiliser la version 1.8.18 d'ipmitool.

Section pertinente :

Installation des logiciels courants

11.3.3.2. Procédure d'accès

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, saisir la commande. InviteSE_ServeurLocal:~# **ipmitool [COMMANDE_IPMI]**	

Pour une liste des Commandes IPMI prises en charge, voir Commandes IPMI prises en charge.

Pour une liste de tous les capteurs, voir Liste des capteurs.

11.3.4. Accéder au BMC en utilisant SNMP

Le BMC est accessible :

- En utilisant BMC SNMP
- En utilisant l'agent SNMP de Kontron pour Linux

11.3.4.1. Accéder au BMC en utilisant BMC SNMP

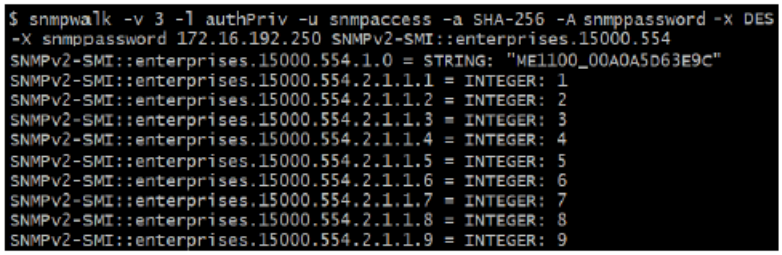
11.3.4.1.1. Préalables

1	L'adresse IP du BMC est connue (voir la section Configuration > Contrôleur de gestion de carte mère – BMC pour obtenir le paramètre IP_GESTION_BMC).
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.
3	Un client snmp est installé sur l'ordinateur distant.

Section pertinente :

Configuration des méthodes d'accès au système

11.3.4.1.2. Procédure d'accès

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, saisir la commande souhaitée. InviteSE_OrdinateurDistant:~# **snmpwalk -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] [IP_GESTION_BMC] [OID]**	

11.3.4.2. Accéder au BMC en utilisant l'agent SNMP de Kontron pour Linux

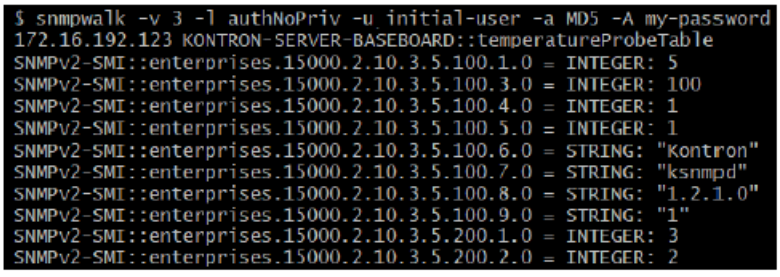
11.3.4.2.1. Préalables

1	Un système d'exploitation est installé.
2	L'adresse IP du système d'exploitation est connue.
3	L'ordinateur distant a accès au sous-réseau du système d'exploitation.
4	Le plus récent paquet RPM pour snmp-agent fourni par Kontron est installé sur le serveur.

Section pertinente :

Configuration des méthodes d'accès au système

11.3.4.2.2. Procédure d'accès

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau du serveur, saisir la commande souhaitée. InviteSE_OrdinateurDistant:~# **snmpwalk -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] [IP_SERVEUR] [OID]**	

11.3.5. Accéder au BMC en utilisant Redfish

11.3.5.1. Préalables

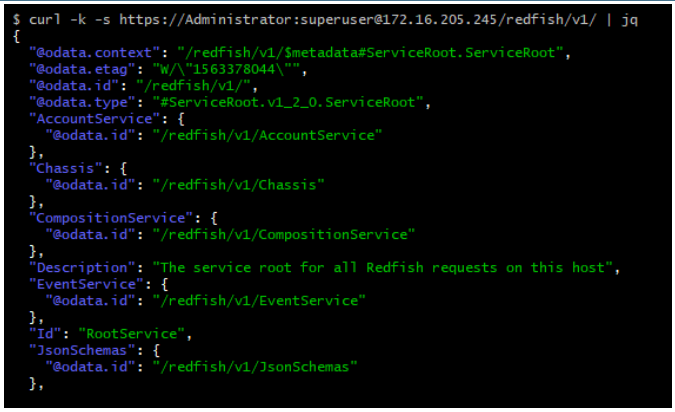
1	L'adresse IP du BMC est connue.
2	Un outil client HTTP est installé sur l'ordinateur distant.
3	Un outil de ligne de commande pour analyser le JSON, tel que jq, est installé.

Sections pertinentes :

Configuration des méthodes d'accès au système

Commandes Redfish prises en charge

11.3.5.2. Procédure d'accès

Étape_1	Accéder à l'API Redfish en utilisant l'URL racine. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE] | jq**	
Étape_2	Ajouter l'extension Managers/Self. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Managers/Self | jq**	

12/ Opération

12.1. Noms d'utilisateur et mots de passe par défaut

12.1.1. Système d'exploitation

Interface utilisateur	Nom d'utilisateur	Mot de passe
Système d'exploitation	Propre à l'application	Propre à l'application
Agent SNMP de Kontron pour Linux	Propre à l'application Voir Configuration des méthodes d'accès au système	Propre à l'application Voir Configuration des méthodes d'accès au système

12.1.2. BIOS

Aucun mot de passe n'est défini par défaut.

12.1.3. Interface de gestion (BMC)

Le BMC est accessible via SNMP. Cependant, avant de configurer SNMP, le nom d'utilisateur et le mot de passe par défaut doivent être modifiés, car un minimum de 8 caractères est requis pour chacun d'eux. Voir Configurer les noms d'utilisateur et mots de passe du BMC en utilisant l'interface utilisateur Web.

La plateforme CG2400 comprend un BMC.

Interface utilisateur	Nom d'utilisateur	Mot de passe
Interface utilisateur Web	admin	admin
IPMI	admin	admin
Redfish	Administrator	superuser
SNMP	Nouveau nom d'utilisateur à 8 caractères minimum configuré après la première connexion	Nouveau mot de passe à 8 caractères minimum configuré après la première connexion

NOTE : Pour des raisons de sécurité, il est important de modifier les noms d'utilisateur et les mots de passe par défaut dès que possible. Voir Configuration et gestion des utilisateurs.

12.2. Gestion de l'alimentation de la plateforme

12.2.1. Commandes d'alimentation disponibles

Les états d'alimentation de la plateforme peuvent être gérés avec diverses commandes envoyées via l'interface utilisateur Web de la plateforme ou un client IPMI (IOL ou KCS). Il est recommandé d'utiliser l'interface utilisateur Web, et l'automatisation des tâches de gestion de l'alimentation nécessite un accès IPMI.

Les commandes d'alimentation sont les suivantes :

- Éteindre : éteint la plateforme immédiatement. **AVERTISSEMENT** : Cette commande ne déclenche pas un arrêt propre du système d'exploitation avant d'éteindre le système.
- Démarrer : démarre la plateforme. **NOTE** : En raison de la configuration électrique du système, il y a un délai de 30 secondes avant que le système ne démarre.

- Réinitialiser (démarrage à chaud) : Redémarre la plateforme sans éteindre l'alimentation. **AVERTISSEMENT** : Cette commande ne déclenche pas un arrêt propre du système d'exploitation avant le redémarrage du système.
- Cycle d'alimentation (démarrage à froid) : éteint la plateforme avant de la redémarrer. **AVERTISSEMENT** : Cette commande ne déclenche pas un arrêt propre du système d'exploitation avant le redémarrage du système.
- Arrêt ACPI (arrêt propre) : Lance et termine l'arrêt du système d'exploitation avant d'éteindre la plateforme. **NOTE** : La norme ACPI doit être prise en charge par le système d'exploitation du serveur.

12.2.2. Éteindre

- En utilisant l'interface utilisateur Web
- En utilisant IPMI (IOL)
- En utilisant IPMI (KCS)
- En utilisant Redfish

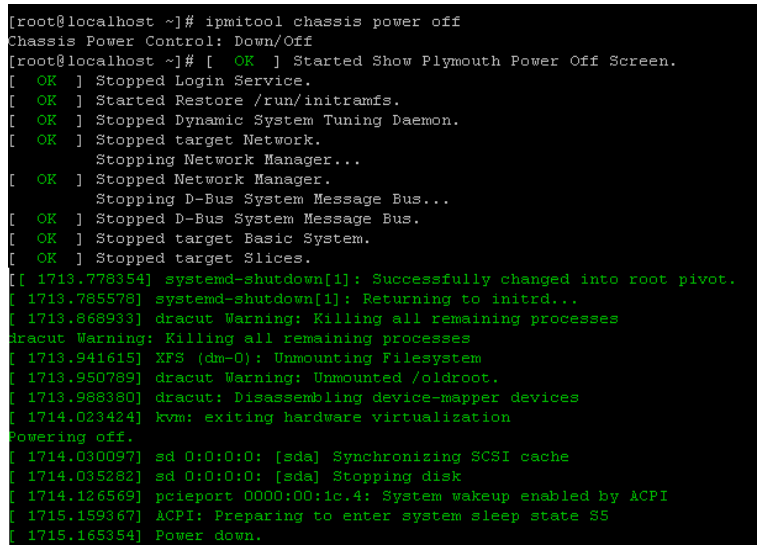
12.2.2.1. Éteindre en utilisant IPMI (IOL)

Voir pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, ouvrir l'invite de commande du système d'exploitation et éteindre la plateforme. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] chassis power off**	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power off` `Chassis Power Control: Down/Off`
Étape_2	Vérifier l'état de l'alimentation pour confirmer que la commande d'alimentation a bien été exécutée. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] chassis power status**	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status` `Chassis Power is off`

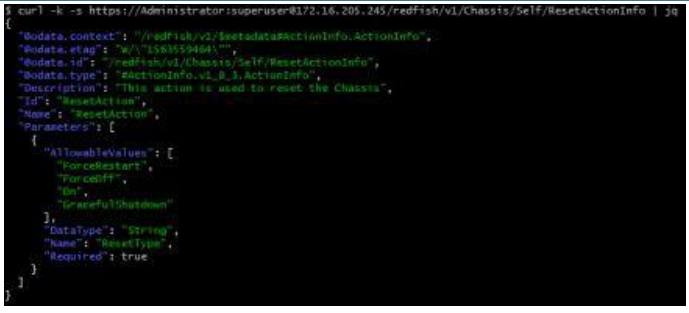
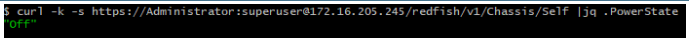
12.2.2.2. Éteindre en utilisant IPMI (KCS)

Voir Accéder au BMC en utilisant IPMI via KCS pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, éteindre la plateforme. InviteSE_ServeurLocal:~# **ipmitool chassis power off**	

12.2.2.3. Éteindre en utilisant Redfish

Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

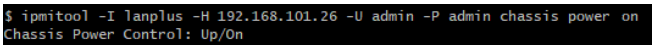
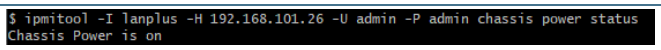
Étape_1	Afficher la liste des commandes d'alimentation disponibles. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Chassis/Self/ResetActionInfo | jq**	
Étape_2	Éteindre la plateforme. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"ForceOff"}' -H "Content- Type: application/json"**	
Étape_3	Vérifier l'état de l'alimentation. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Chassis/Self | jq .PowerState**	

12.2.3. Démarrer

- En utilisant l'interface utilisateur Web
- En utilisant IPMI (IOL)
- En utilisant Redfish

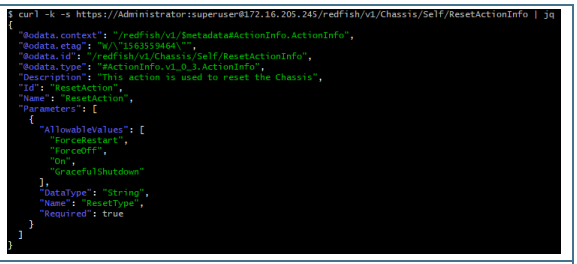
12.2.3.1. Démarrer en utilisant IPMI (IOL)

Voir Accéder au BMC en utilisant IPMI sur LAN (IOL) pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, ouvrir l'invite de commande du système d'exploitation et démarrer la plateforme. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] chassis power on**	
Étape_2	Vérifier l'état de l'alimentation pour confirmer que la commande d'alimentation a bien été exécutée. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] chassis power status**	

12.2.3.2. Démarrer en utilisant Redfish

Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Afficher la liste des commandes d'alimentation disponibles. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Chassis/Self/ResetActionInfo | jq**	
Étape_2	Démarrer la plateforme. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"On"}' -H "Content-Type: application/json"**	
Étape_3	Vérifier l'état de l'alimentation. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Chassis/Self | jq .PowerState**	

12.2.4. Réinitialiser (démarrage à chaud)

- En utilisant l'interface utilisateur Web
- En utilisant IPMI (IOL)
- En utilisant IPMI (KCS)
- En utilisant Redfish

12.2.4.1. Réinitialiser (démarrage à chaud) en utilisant IPMI (IOL)

Voir Accéder au BMC en utilisant IPMI sur LAN (IOL) pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, ouvrir l'invite de commande du système d'exploitation et réinitialiser la plateforme. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] chassis power reset**	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power reset` `Chassis Power Control: Reset`
Étape_2	Vérifier l'état de l'alimentation pour confirmer que la commande d'alimentation a bien été exécutée. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] chassis power status** **NOTE** : Le redémarrage du système d'exploitation peut prendre un certain temps.	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status` `Chassis Power is on`

12.2.4.2. Réinitialiser (démarrage à chaud) en utilisant IPMI (KCS)

Voir Accéder au BMC en utilisant IPMI via KCS pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, réinitialiser la plateforme. InviteSE_ServeurLocal:~# **ipmitool chassis power reset** **NOTE** : Le redémarrage du système d'exploitation peut prendre un certain temps.	`[root@localhost ~]# ipmitool chassis power reset` `Chassis Power Control: Reset`

12.2.4.3. Réinitialiser (démarrage à chaud) en utilisant Redfish

Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Afficher la liste des commandes d'alimentation disponibles. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Chassis/Self/ResetActionInfo | jq**	`$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Chassis/Self/ResetActionInfo | jq` `{` `"@odata.context": "/redfish/v1/$metadata#ActionInfo.ActionInfo",` `"@odata.etag": "W/\"1563559464\"",` `"@odata.id": "/redfish/v1/Chassis/Self/ResetActionInfo",` `"@odata.type": "#ActionInfo.v1_0_3.ActionInfo",` `"Description": "This action is used to reset the Chassis",` `"Id": "ResetAction",` `"Name": "ResetAction",` `"Parameters": [` `{` `"AllowableValues": [` `"ForceRestart",` `"ForceOff",` `"On",` `"GracefulShutdown"` `],` `"DataType": "String",` `"Name": "ResetType",` `"Required": true` `}` `]` `}`
Étape_2	Réinitialiser la plateforme. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"ForceRestart"}' -H "Content- Type: application/json"**	

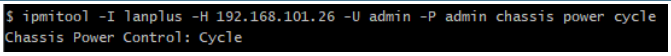
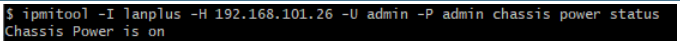
Étape_3	Vérifier l'état de l'alimentation. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Chassis/Self | jq .PowerState**	

12.2.5. Cycle d'alimentation (démarrage à froid)

- En utilisant l'interface utilisateur Web
- En utilisant IPMI (IOL)
- En utilisant IPMI (KCS)

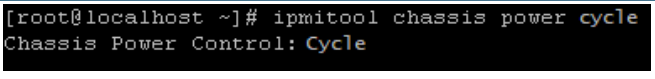
12.2.5.1. Cycle d'alimentation (démarrage à froid) en utilisant IPMI (IOL)

Voir Accéder au BMC en utilisant IPMI sur LAN (IOL) pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, ouvrir l'invite de commande du système d'exploitation et effectuer un cycle d'alimentation. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] chassis power cycle**	
Étape_2	Vérifier l'état de l'alimentation pour confirmer que la commande d'alimentation a bien été exécutée. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] chassis power status** **NOTE** : Le redémarrage du système d'exploitation peut prendre un certain temps.	

12.2.5.2. Cycle d'alimentation (démarrage à froid) en utilisant IPMI (KCS)

Voir Accéder au BMC en utilisant IPMI via KCS pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, effectuer un cycle d'alimentation. InviteSE_ServeurLocal:~# **ipmitool chassis power cycle** **NOTE** : Le redémarrage du système d'exploitation peut prendre un certain temps.	

12.2.6. Arrêt ACPI (arrêt propre)

- En utilisant l'interface utilisateur Web
- En utilisant IPMI (IOL)
- En utilisant IPMI (KCS)
- En utilisant Redfish

12.2.6.1. Arrêt ACPI en utilisant IPMI (IOL)

Voir Accéder au BMC en utilisant IPMI sur LAN (IOL) pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, ouvrir l'invite de commande du système d'exploitation et effectuer un arrêt ACPI. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] chassis power soft**	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power soft` `Chassis Power Control: Soft`
Étape_2	Vérifier l'état de l'alimentation pour confirmer que la commande d'alimentation a bien été exécutée. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] chassis power status**	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status` `Chassis Power is off`

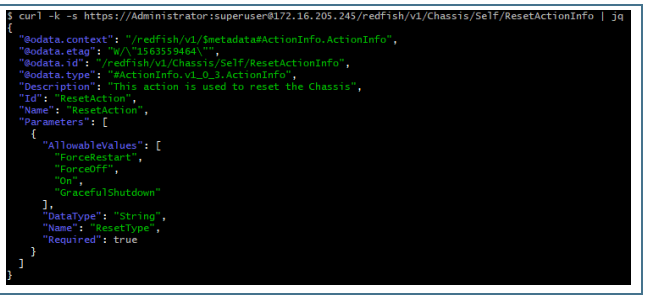
12.2.6.2. Arrêt ACPI en utilisant IPMI (KCS)

Voir Accéder au BMC en utilisant IPMI via KCS pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, effectuer un arrêt ACPI. InviteSE_ServeurLocal:~# **ipmitool chassis power soft**	`[root@localhost ~]# ipmitool chassis power soft` `Chassis Power Control: Soft` `[root@localhost ~]# [  OK  ] Started Show Plymouth Power Off Screen.` `[  OK  ] Stopped Network Manager.` `Stopping D-Bus System Message Bus...` `[  OK  ] Stopped D-Bus System Message Bus.` `[  OK  ] Stopped Login Service.` `[  OK  ] Stopped target Basic System.`

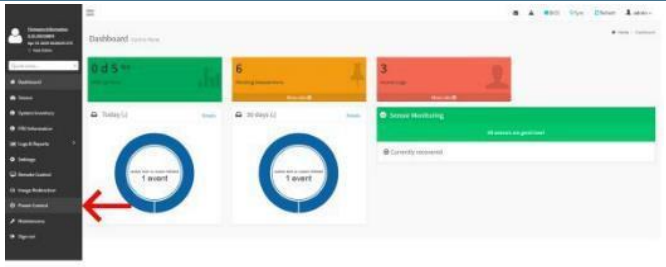
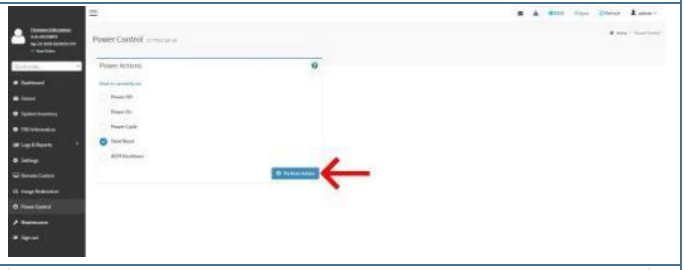
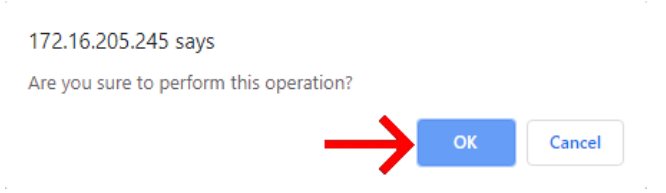
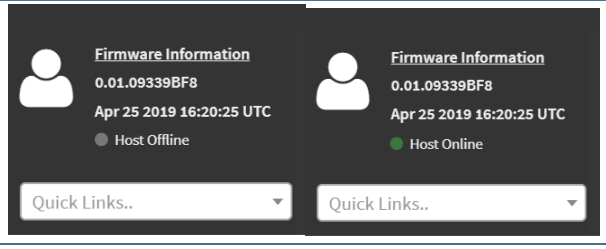
12.2.6.3. Arrêt ACPI en utilisant Redfish

Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Afficher la liste des commandes d'alimentation disponibles. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Chassis/Self/ResetActionInfo | jq**	
Étape_2	Envoyer la commande d'alimentation à la plateforme. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"GracefulShutdown"}' -H "Content-Type: application/json"**	
Étape_3	Vérifier l'état de l'alimentation. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Chassis/Self | jq .PowerState**	

12.2.7. Envoyer une commande d'alimentation en utilisant l'interface utilisateur Web

Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

Étape_1	Accéder à l'interface utilisateur Web du BMC d'un serveur.	
Étape_2	Une fois la session ouverte dans l'interface utilisateur Web, cliquer sur **Power Control** dans le menu de gauche.	
Étape_3	Sélectionner la commande d'alimentation souhaitée. Appuyer sur le bouton **Perform Action**.	
Étape_4	Une demande de confirmation s'affiche. Confirmer la commande en cliquant sur **OK**. Après confirmation, la commande sélectionnée sera exécutée et l'état de la plateforme sera mis à jour après quelques minutes.	
Étape_5	Vérifier l'état d'alimentation en regardant l'état d'alimentation dans le menu de gauche.	

12.2.8. Politique de contrôle de l'alimentation en cas de panne de courant

Il est possible de configurer le comportement d'un système sur le plan de la gestion de l'alimentation en cas de perte ou de panne de courant. Cette fonction était appelée **Resume on AC Power Loss** dans la précédente génération de systèmes CG de Kontron (CG2200, CG2300).

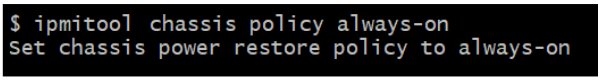
Ce paramètre peut être défini :

- En utilisant IPMI
- En utilisant le menu BIOS

Voici les valeurs possibles et la correspondance entre IPMI et le menu BIOS.

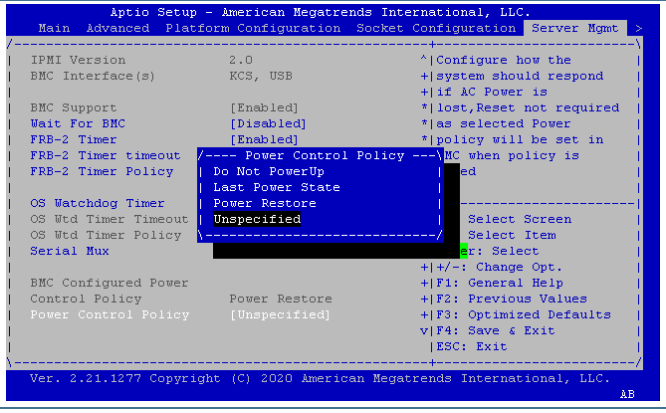
IPMI	Menu BIOS	Note
always-on	Power Restore	La plateforme démarre lorsque le courant est rétabli
previous	Last Power State	La plateforme revient à l'état précédent (avant la panne de courant) lorsque le courant est rétabli
always-off	Do Not Power Up	La plateforme ne démarre pas même si l'alimentation est rétablie

12.2.8.1. Configurer le comportement en utilisant IPMI

Étape_1	Définir la politique de contrôle de l'alimentation. InviteSE_ServeurLocal:~# **ipmitool chassis power policy [POLITIQUE]**	

12.2.8.2. Configurer le comportement en utilisant le menu BIOS

Voir Accéder au BIOS pour les instructions d'accès.

Étape_1	Dans le menu **Server Mgmt**, sélectionner la valeur de l'option **Power Control Policy**.	

12.2.9. Délai de rétablissement de l'alimentation en cas de panne de courant

Il est possible d'ajouter un certain temps avant que la plateforme démarre lorsque le courant est rétabli.

Ce paramètre peut être défini :

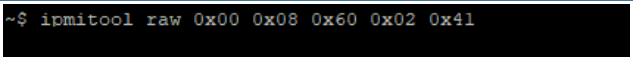
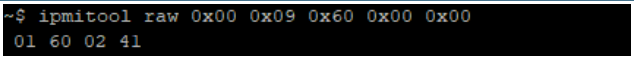
- En utilisant IPMI

- En utilisant le menu BIOS

Voici les valeurs possibles prises en charge par cette fonctionnalité :

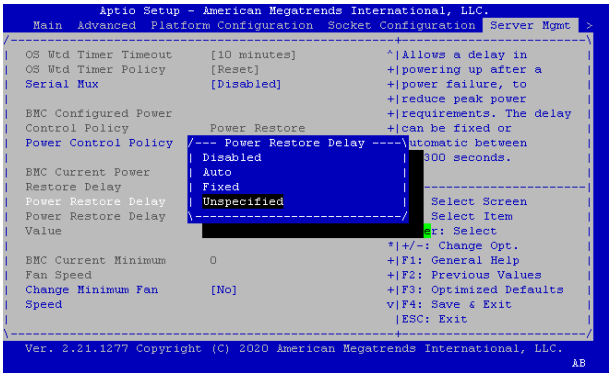
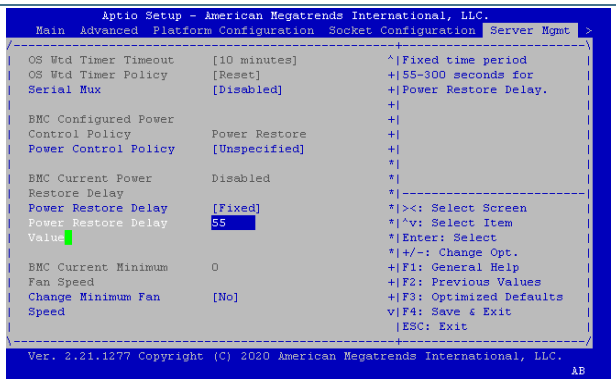
Valeur BIOS	Note
Disabled	Aucun délai de rétablissement de l'alimentation n'est défini, la plateforme démarre automatiquement après une panne de courant (valeur par défaut).
Auto	Une valeur aléatoire (entre 55 et 300 secondes) est définie, la plateforme démarre après cette temporisation.
Fixed	Une valeur choisie (entre 55 et 300 secondes) est définie, la plateforme démarre après cette temporisation.

12.2.9.1. Configurer le rétablissement en utilisant IPMI

Étape_1	La commande ipmitool raw OEM suivante permet de définir les paramètres du délai de rétablissement de l'alimentation. InviteSE_ServeurLocal:~# **ipmitool raw 0x00 0x08 0x60 [DONNÉE1] [DONNÉE2]** Où les valeurs possibles pour **DONNÉE1** sont : • 0x00 = Disabled • 0x01 = Auto (valeur aléatoire entre 55 et 300 secondes) • 0x02 = Fixed (valeur manuelle entre 55 et 300 secondes) Où **DONNÉE2** contient la valeur de la temporisation lorsque le paramètre Fixed est sélectionné : • La valeur minimale 0x00 représente 55 secondes La valeur maximale 0xF5 représente 300 secondes	
Étape_2	La commande **ipmitool raw OEM** suivante permet de vérifier les paramètres actuels. InviteSE_ServeurLocal:~# **ipmitool raw 0x00 0x09 0x60 0x00 0x00** **NOTE** : La réponse contient toujours 4 octets de données : **01 60 [DONNÉE1] [DONNÉE2]**	

12.2.9.2. Configurer le rétablissement en utilisant le menu BIOS

Voir Accéder au BIOS pour les instructions d'accès.

Étape_1	Dans le menu **Server Mgmt**, sélectionner la valeur de l'option **Power Restore Delay**. **NOTE** : Lors de l'accès au menu, la valeur par défaut est toujours **Unspecified**. Il est impératif de sélectionner la valeur souhaitée pour déclencher le changement.	
Étape_2	Si le paramètre **Fixed** est sélectionné, entrer une valeur comprise entre 55 et 300 secondes dans le champ **Power Restore Delay Value**.	

12.3. Surveillance

12.3.1. Surveillance des capteurs

La plateforme est équipée de nombreux capteurs, consulter la Liste des capteurs pour plus de détails et pour déterminer l'ID d'un capteur. Les capteurs de la plateforme peuvent être surveillés :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant IPMI
- En utilisant SNMP
- En utilisant Redfish

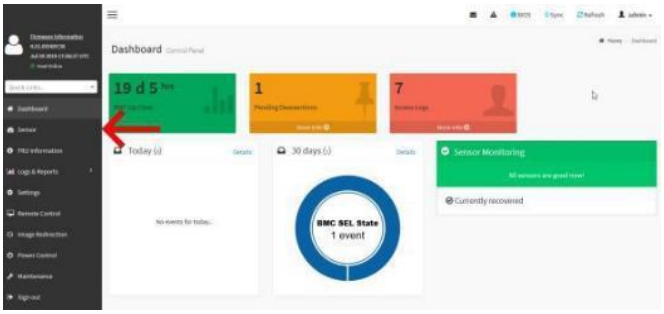
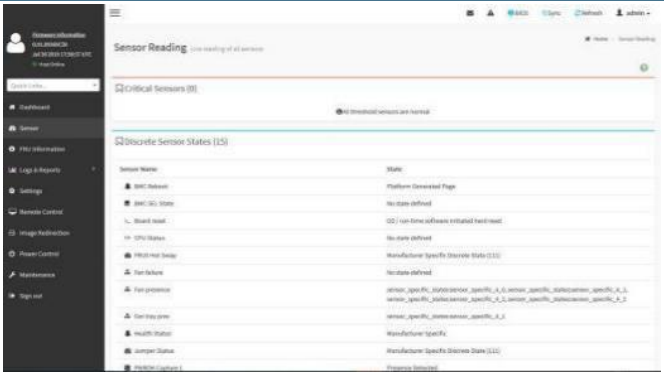
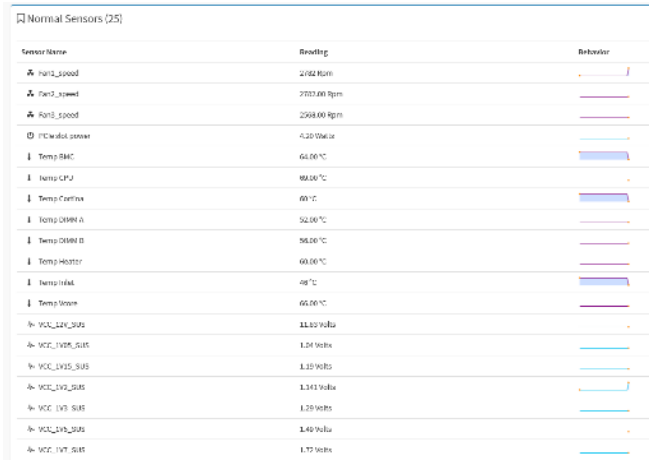
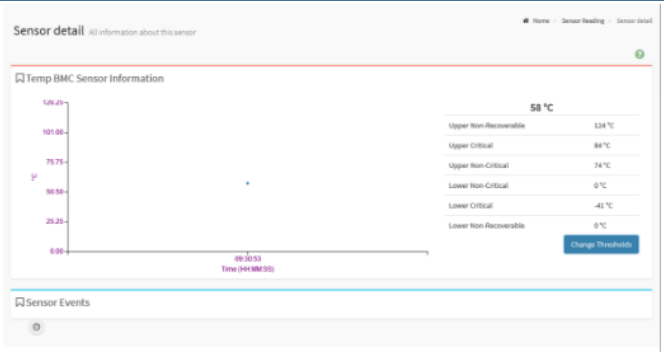
Pour les instructions d'Interprétation des données des capteurs, voir Interprétation des données des capteurs. Pour des instructions sur la façon d'accéder au BMC, voir Accéder au BMC.

12.3.1.1. Surveiller les capteurs en utilisant l'interface utilisateur Web du BMC

12.3.1.1.1. Accéder aux informations des capteurs

Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

Étape_1	Accéder à l'interface utilisateur Web du BMC.

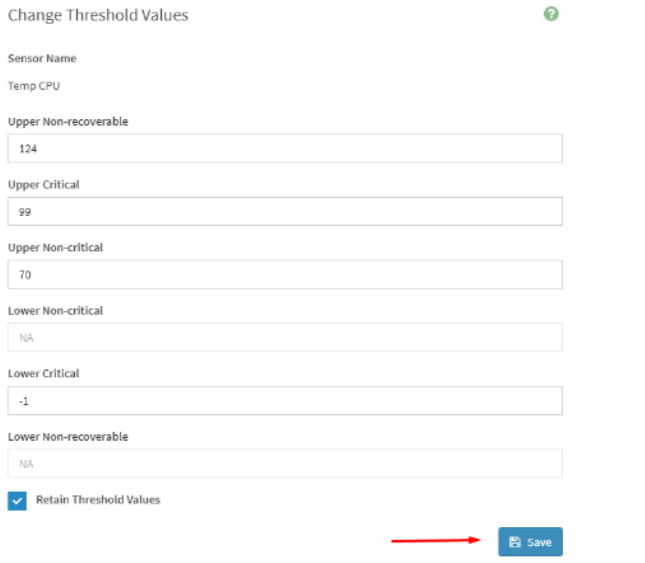
Étape_2	Dans le menu de gauche, cliquer sur **Sensor**.	
Étape_3	La liste des capteurs s'affiche.	
Étape_4	Faire défiler vers le bas pour voir la liste des capteurs.	
Étape_5	Cliquer sur un capteur pour afficher plus de détails.	

12.3.1.1.2. Configurer les capteurs

NOTE : Les seuils des capteurs sont réglés sur les configurations par défaut lorsque la plateforme est réinitialisée.

NOTICE

Les seuils par défaut des capteurs de plateforme ne devraient pas être modifiés. Ils ont été réglés pour assurer un bon fonctionnement de la plateforme. Si vous décidez de les modifier, faites preuve de prudence, car des réglages inappropriés pourraient causer des dommages matériels.

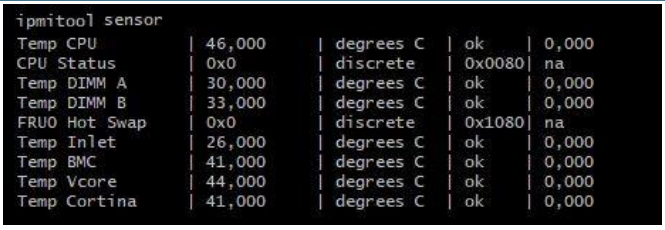
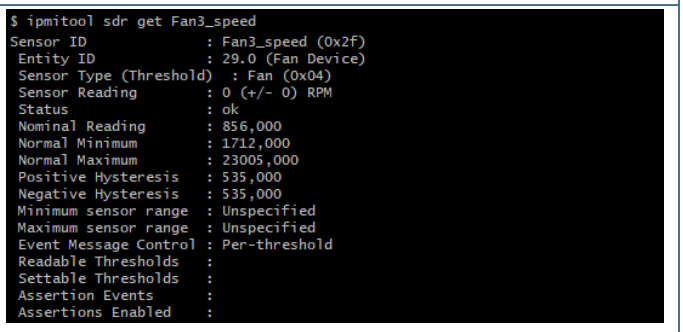
Étape_1	Dans la page Sensor detail, cliquer sur **Change Thresholds**.	
Étape_2	Régler les seuils comme désiré et cliquer sur **Save**. Optionnel : Cocher la case **Retain Thresholds** si vous souhaitez conserver les seuils définis après un redémarrage du BMC.	

12.3.1.2. Surveiller les capteurs en utilisant IPMI

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL (Accéder au BMC en utilisant IPMI sur LAN (IOL)).

Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

12.3.1.2.1. Voir les informations des capteurs

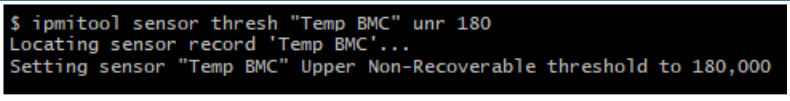
Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, saisir la commande. InviteSE_ServeurLocal:~# **ipmitool sensor**	
Étape_2	Utiliser la commande sdr pour obtenir plus de détails sur un capteur particulier. InviteSE_ServeurLocal:~# **ipmitool sdr get [ID_CAPTEUR]**	

12.3.1.2.2. Configurer les capteurs

NOTE : Les seuils des capteurs sont réglés sur les configurations par défaut lorsque la plateforme est réinitialisée.

NOTICE

Les seuils par défaut des capteurs de plateforme ne devraient pas être modifiés. Ils ont été réglés pour assurer un bon fonctionnement de la plateforme. Si vous décidez de les modifier, faites preuve de prudence, car des réglages inappropriés pourraient causer des dommages matériels.

Étape_1	Modifier la valeur de seuil du capteur souhaité. InviteSE_ServeurLocal:~# **ipmitool sensor thresh [ID_CAPTEUR] [TYPE_SEUIL] [VALEUR]** **NOTE** : Pour une valeur de seuil négative, ajouter des doubles tirets (--) avant la commande sensor et taper la valeur négative. InviteSE_ServeurLocal:~# **ipmitool -- sensor thresh [ID_CAPTEUR] [TYPE_SEUIL] [VALEUR_NEG]**	

12.3.1.3. Surveiller les capteurs en utilisant SNMP

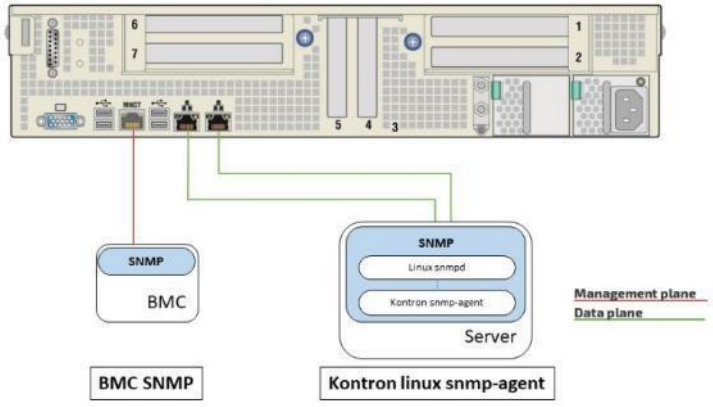
La plateforme peut être surveillée à distance avec le protocole SNMP :

- En utilisant BMC SNMP
- En utilisant l'agent SNMP de Kontron pour Linux

Chaque méthode est indépendante.

Lors de la surveillance de la plateforme, de nombreux facteurs doivent être pris en compte pour chaque méthode.

- Chaque méthode donne accès à des informations différentes. Par exemple, les valeurs de seuil ne peuvent être lues qu'en utilisant l'agent SNMP de Kontron pour Linux.
- Chaque méthode a ses propres données d'accès. Voir Noms d'utilisateur et mots de passe par défaut pour les données d'accès par défaut.
- Certains OID pourraient être différents en fonction de la méthode d'accès.
- BMC SNMP est accessible à partir du port LAN dédié sur le plan de gestion.
- L'agent SNMP pour Linux est accessible depuis les deux ports LAN 10GbE du plan des données.



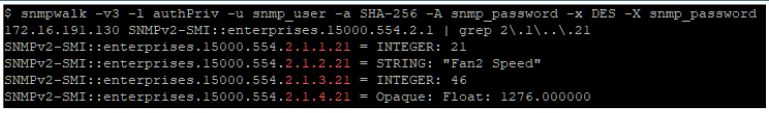
12.3.1.3.1. Surveiller les capteurs en utilisant BMC SNMP

NOTE : La version actuelle prend en charge la version 3 du protocole SNMP. Pour que les commandes fonctionnent, la version 5.8 ou supérieure de snmpwalk doit être installée. Voir Accéder au BMC en utilisant BMC SNMP pour les instructions d'accès.

12.3.1.3.1.1. Afficher la liste des capteurs

Étape_1	Pour accéder à tous les capteurs du BMC, utiliser la commande suivante. InviteSE_OrdinateurDistant:~# **snmpwalk -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] -x [PROTOCOLE_ENC] -X "[MOT_DE_PASSE]" [IP_GESTION] [OID]**	`$ snmpwalk -v3 -l authPriv -u snmp_user -a SHA-256 -A snmp_password -x DES -X snmp_password 172.16.191.130 SNMPv2-SMI::enterprises.15000.554.2.1.2` `SNMPv2-SMI::enterprises.15000.554.2.1.2.1 = STRING: "Pwr Unit Redund"` `SNMPv2-SMI::enterprises.15000.554.2.1.2.2 = STRING: "IPMI Watchdog"` `SNMPv2-SMI::enterprises.15000.554.2.1.2.3 = STRING: "FP NMI Diag Int"` `SNMPv2-SMI::enterprises.15000.554.2.1.2.4 = STRING: "System Event Log"` `SNMPv2-SMI::enterprises.15000.554.2.1.2.5 = STRING: "System Event"` `SNMPv2-SMI::enterprises.15000.554.2.1.2.6 = STRING: "BMC Watchdog"` `SNMPv2-SMI::enterprises.15000.554.2.1.2.7 = STRING: "VR Watchdog"` `SNMPv2-SMI::enterprises.15000.554.2.1.2.8 = STRING: "P2 TJMAX"` `SNMPv2-SMI::enterprises.15000.554.2.1.2.9 = STRING: "PS1 Input Power"` `SNMPv2-SMI::enterprises.15000.554.2.1.2.10 = STRING: "PS2 Input Power"` `SNMPv2-SMI::enterprises.15000.554.2.1.2.11 = STRING: "PS1 Temp"` `SNMPv2-SMI::enterprises.15000.554.2.1.2.12 = STRING: "PS2 Temp"`

12.3.1.3.1.2. Afficher les détails d'un capteur

Étape_ 1	Utiliser la commande suivante pour afficher les détails d'un capteur. InviteSE_OrdinateurDistant:~# **snmpwalk -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] -x [PROTOCOLE_ENC] -X "[MOT_DE_PASSE]" [IP_GESTION] [OID] | grep "\.[NUMERO_ENTREE_TABLEAU] "** **NOTE** : L'espace entre l'attribut [NUMERO_ENTREE_TABLEAU] et le guillemet est nécessaire au bon fonctionnement de la commande grep.	

12.3.1.3.2. Surveiller les capteurs en utilisant l'agent SNMP de Kontron pour Linux

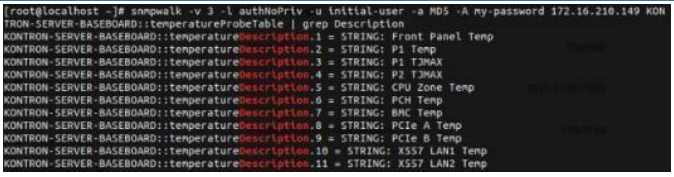
Voir Configurer l'agent SNMP (snmp-agent) de Kontron pour Linux sur la plateforme pour les instructions de configuration.

Voir aussi Configurer les utilisateurs SNMP en utilisant l'agent SNMP de Kontron pour Linux pour gérer les utilisateurs SNMP.

12.3.1.3.2.1. OID de l'agent SNMP de Kontron pour Linux

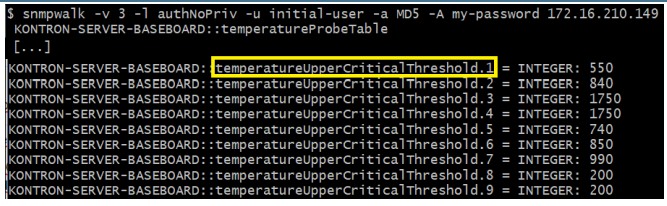
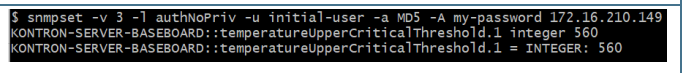
Groupe	Groupe OID	Sous-groupe	Sous-groupe OID | OID numérique
Power	powerGroup	Power unit	powerUnitTable | 1.3.6.1.4.1.15000.2.10.3.5.400.10
		Power supply	powerSupplyTable | 1.3.6.1.4.1.15000.2.10.3.5.400.20
		Voltages	voltageProbeTable | 1.3.6.1.4.1.15000.2.10.3.5.400.30
		Discrete voltage	discreteVoltageProbeTable | 1.3.6.1.4.1.15000.2.10.3.5.400.40
Thermal	thermalGroup	Cooling unit	coolingUnitTable | 1.3.6.1.4.1.15000.2.10.3.5.600.10
		Cooling device	coolingDeviceTable | 1.3.6.1.4.1.15000.2.10.3.5.600.20
		Discrete cooling device	discreteCoolingTable | 1.3.6.1.4.1.15000.2.10.3.5.600.30
		Temperature	temperatureProbeTable | 1.3.6.1.4.1.15000.2.10.3.5.600.40

12.3.1.3.2.2. Afficher les détails d'un capteur

Étape_1	Trouver le bon numéro d'entrée du capteur dans le tableau en fonction du NOM DU CAPTEUR IPMI (ex. BMC Temp est l'entrée 7 du tableau). InviteSE_OrdinateurDistant:~# **snmpwalk -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] [IP_SERVEUR] KONTRON-SERVER-BASEBOARD:: [OID_SUB_GROUP] | grep Description**	
Étape_2	Afficher les détails d'un capteur particulier. InviteSE_OrdinateurDistant:~# **snmpwalk -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] [IP_SERVEUR] KONTRON-SERVER-BASEBOARD:: | grep "\.[NUMERO_ENTREE_TABLEAU] "** **NOTE** : L'espace entre l'attribut [NUMERO_ENTREE_TABLEAU] et le guillemet est nécessaire au bon fonctionnement de la commande grep.	

12.3.1.3.2.3. Configurer les capteurs

NOTE : Les seuils des capteurs sont réglés sur les configurations par défaut lorsque la plateforme est réinitialisée.

Étape_1	Trouver l'OID de la valeur à modifier. InviteSE_OrdinateurDistant:~# **snmpwalk -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] [IP_SERVEUR] KONTRON-SERVER-BASEBOARD:: [OID_SUB_GROUP] | grep "[NOM_CAPTEUR]"**	
Étape_2	Régler la valeur du seuil à modifier. InviteSE_OrdinateurDistant:~# **snmpset -v3 -l [NIVEAU_AUTH] -u [NOM_UTILISATEUR] -a [PROTOCOLE_AUTH] -A [MOT_DE_PASSE] [IP_SERVEUR] KONTRON-SERVER-BASEBOARD:: [OID_SEUIL].[NUMÉRO_ID_CAPTEUR] integer [NOUVELLE_VALEUR]**	

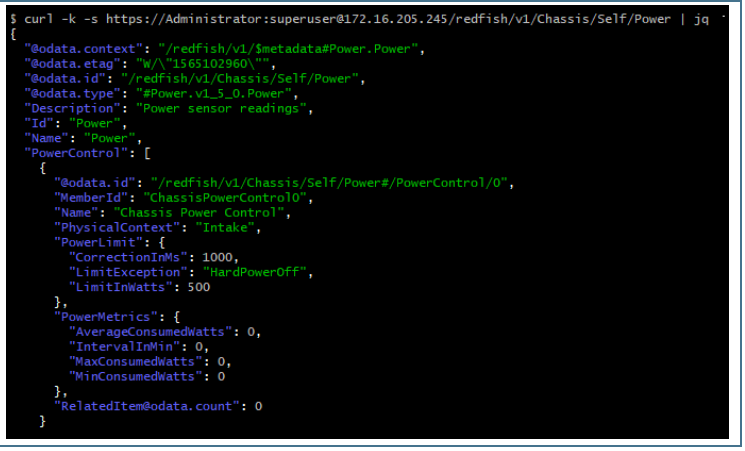
12.3.1.4. Surveiller les capteurs en utilisant Redfish

Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

12.3.1.4.1. Créer des extensions URL

Type	Capteurs	Extensions URL
Capteur d'alimentation	Tous les capteurs de type 02h (tension)	Chassis/Self/Power | jq
Thermique	Tous les capteurs de type 01h (température)	Chassis/Self/Thermal | jq ".Temperatures"
	Fan1 speed Fan2 speed Fan3 speed Fan4 speed Fan5 speed Fan6 speed	Chassis/Self/Thermal | jq ".Fans"
Santé	CPU Status	Managers/Self/HostI nterfaces/Self | jq ".Status"
	Health Status	Chassis/Self | jq ".Status"

12.3.1.4.2. Afficher les informations des capteurs

Étape_1	Ajouter à l'URL racine l'extension appropriée en fonction du type de capteur. Voir le tableau des extensions URL ci-dessus. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/[EXTENSION_URL]**	

12.3.1.5. Liste des capteurs

Pour de l'information sur le code de type de capteur (sensor type code) et le code de type d'événement/de lecture (event/reading type code), voir Interprétation des données des capteurs.

Nom du capteur [ID_CAPTEUR]	Numéro du capteur SNMP [NUMÉRO_ID _CAPTEUR]	Numéro du capteur IPMI [NUMÉRO_ID _CAPTEUR]	Code de type de capteur	Code de type d'événement/ lecture	Description
PCI Error		33h	13h	6Fh	Diverses erreurs PCI/PCIe détectées par le BIOS (GenId:21)
Memory Error		34h	0Ch	6Fh	Diverses erreurs de mémoire détectées par le BIOS (GenId:21)
Processor Error		35h	07h	6Fh	Diverses erreurs de processeur détectées par le BIOS (GenId:21)
Direct Memory Access (DMA) Error		36h	07h	6Fh	Diverses erreurs DMA détectées par le BIOS (GenId:21)

Nom du capteur [ID_CAPTEUR]	Numéro du capteur SNMP [NUMÉRO_ID _CAPTEUR]	Numéro du capteur IPMI [NUMÉRO_ID _CAPTEUR]	Code de type de capteur	Code de type d'événement/ lecture	Description
OutBound Traffic Controller (OTC) Error		37h	07h	6Fh	Diverses erreurs OTC détectées par le BIOS (GenId:21)
InBound Traffic Controller (ITC) Error		38h	07h	6Fh	Diverses erreurs ITC détectées par le BIOS (GenId:21)
Intel VT-d Error		39h	07h	6Fh	Diverses erreurs VT-d détectées par le BIOS (GenId:21)
FP NMI Diag Int	3	05h	13h	6Fh	
IPMI Watchdog	2	03h	23h	6Fh	Capteur de l'horloge de surveillance IPMI
BMC Watchdog	6	0Ah	28h	03h	Surveillance de l'état de la gestion
VR Watchdog	7	0Bh	02h	03h	
System Event Log	5	07h	10h	6Fh	
System Event	5	08h	12h	6Fh	
Front Panel Temp		21h	01h	01h	Température du panneau avant
P1 Temp	64	C7h	01h	01h	Température du processeur 1
P2 Temp	74	D2h	01h	01h	Température du processeur 2
P1 TJMAX	18	20h	01h	01h	Température du processeur 1 : température maximale avant un arrêt causé par la température
P2 TJMAX	8	0Fh	01h	01h	Température du processeur 2 : température maximale avant un arrêt causé par la température
CPU Zone Temp	57	B5h	01h	01h	Température de la zone CPU
PCH Temp	17	1Eh	01h	01h	Température du PCH
BMC Temp	61	BAh	01h	01h	Température du BMC
PCIe A Temp	59	B7h	01h	01h	Température PCIe A (câble d'extension J33) Gestion de la sonde d'extension
PCIe B Temp	60	B9h	01h	01h	Température PCIe B (câble d'extension J37) Gestion de la sonde d'extension
X557 LAN1 Temp	62	BBh	01h	01h	Température du X557 LAN 1
X557 LAN2 Temp	63	BCh	01h	01h	Température du X557 LAN 2
M.2 Temp	56	B4h	01h	01h	Température de la zone M.2

Nom du capteur [ID_CAPTEUR]	Numéro du capteur SNMP [NUMÉRO_ID _CAPTEUR]	Numéro du capteur IPMI [NUMÉRO_ID _CAPTEUR]	Code de type de capteur	Code de type d'événement/ lecture	Description
Battery Temp	58	B6h	01h	01h	Température de la batterie
P1 DIMMA1 Temp	65	C8h	01h	01h	Température du canal DIMM CPU1
P1 DIMMA2 Temp	66	C9h	01h	01h	Température du canal DIMM CPU1
P1 DIMMB1 Temp	67	CAh	01h	01h	Température du canal DIMM CPU1
P1 DIMMC1 Temp	68	CBh	01h	01h	Température du canal DIMM CPU1
P1 DIMMD1 Temp	69	CCh	01h	01h	Température du canal DIMM CPU1
P1 DIMMD2 Temp	70	CDh	01h	01h	Température du canal DIMM CPU1
P1 DIMME1 Temp	71	CEh	01h	01h	Température du canal DIMM CPU1
P1 DIMMF1 Temp	72	CFh	01h	01h	Température du canal DIMM CPU1
P2 DIMMA1 Temp	75	D3h	01h	01h	Température du canal DIMM CPU2
P2 DIMMA2 Temp	76	D4h	01h	01h	Température du canal DIMM CPU2
P2 DIMMB1 Temp	77	D5h	01h	01h	Température du canal DIMM CPU2
P2 DIMMC1 Temp	78	D6h	01h	01h	Température du canal DIMM CPU2
P2 DIMMD1 Temp	79	D7h	01h	01h	Température du canal DIMM CPU2
P2 DIMMD2 Temp	80	D8h	01h	01h	Température du canal DIMM CPU2
P2 DIMME1 Temp	81	D9h	01h	01h	Température du canal DIMM CPU2
P2 DIMMF1 Temp	82	DAh	01h	01h	Température du canal DIMM CPU2
P1 DIMMA1 T Mrgn		F0h	01h	01h	Marge de température du canal DIMM CPU1
P1 DIMMA2 T Mrgn		F1h	01h	01h	Marge de température du canal DIMM CPU1
P1 DIMMB1 T Mrgn		F2h	01h	01h	Marge de température du canal DIMM CPU1
P1 DIMMC1 T Mrgn		F3h	01h	01h	Marge de température du canal DIMM CPU1
P1 DIMMD1 T Mrgn		F4h	01h	01h	Marge de température du canal DIMM CPU1
P1 DIMMD2 T Mrgn		F5h	01h	01h	Marge de température du canal DIMM CPU1
P1 DIMME1 T Mrgn		F6h	01h	01h	Marge de température du canal DIMM CPU1
P1 DIMMF1 T Mrgn		F7h	01h	01h	Marge de température du canal DIMM CPU1
P2 DIMMA1 T Mrgn		AAh	01h	01h	Marge de température du canal DIMM CPU2
P2 DIMMA2 T Mrgn		ABh	01h	01h	Marge de température du canal DIMM CPU2
P2 DIMMB1 T Mrgn		ACh	01h	01h	Marge de température du canal DIMM CPU2
P2 DIMMC1 T Mrgn		ADh	01h	01h	Marge de température du canal DIMM CPU2

Nom du capteur [ID_CAPTEUR]	Numéro du capteur SNMP [NUMÉRO_ID _CAPTEUR]	Numéro du capteur IPMI [NUMÉRO_ID _CAPTEUR]	Code de type de capteur	Code de type d'événement/ lecture	Description
P2 DIMMD1 T Mrgn		AEh	01h	01h	Marge de température du canal DIMM CPU2
P2 DIMMD2 T Mrgn		AFh	01h	01h	Marge de température du canal DIMM CPU2
P2 DIMME1 T Mrgn		B0h	01h	01h	Marge de température du canal DIMM CPU2
P2 DIMMF1 T Mrgn		B1h	01h	01h	Marge de température du canal DIMM CPU2
Fan Failure	26	34h	04h	6Fh	Indique un ventilateur défectueux
Fan1 Speed	20	2Dh	04h	01h	Vitesse du ventilateur 1 (tr/min)
Fan2 Speed	21	2Eh	04h	01h	Vitesse du ventilateur 2 (tr/min)
Fan3 Speed	22	2Fh	04h	01h	Vitesse du ventilateur 3 (tr/min)
Fan4 Speed	23	30h	04h	01h	Vitesse du ventilateur 4 (tr/min)
Fan5 Speed	24	31h	04h	01h	Vitesse du ventilateur 5 (tr/min)
Fan6 Speed	25	32h	04h	01h	Vitesse du ventilateur 6 (tr/min)
Fan1 Present	33	61h	04h	08h	État de présence du ventilateur 1
Fan2 Present	34	62h	04h	08h	État de présence du ventilateur 2
Fan3 Present	35	63h	04h	08h	État de présence du ventilateur 3
Fan4 Present	36	64h	04h	08h	État de présence du ventilateur 4
Fan5 Present	37	65h	04h	08h	État de présence du ventilateur 5
Fan6 Present	38	66h	04h	08h	État de présence du ventilateur 6
Pwr Unit Redund	1	02h	09h	0Bh	États de redondance des blocs d'alimentation
PS1 Status	13	1Ah	08h	6Fh	État du bloc d'alimentation 1
PS2 Status	14	1Bh	08h	6Fh	État du bloc d'alimentation 2
PS1 Input Power	9	16h	08h	01h	Puissance d'entrée du bloc d'alimentation 1
PS2 Input Power	10	17h	08h	01h	Puissance d'entrée du bloc d'alimentation 2
PS1 Output Power	15	1Ch	08h	01h	Puissance de sortie du bloc d'alimentation 1
PS2 Output Power	16	1Dh	08h	01h	Puissance de sortie du bloc d'alimentation 2
PS1 Temp	11	18h	01h	01h	Température du bloc d'alimentation 1
PS2 Temp	12	19h	01h	01h	Température du bloc d'alimentation 2
CPU Missing	41	82h	07h	03h	État de présence du processeur
P1 Status	86	EDh	07h	6Fh	État du processeur 1
P2 Status	87	EEh	07h	6Fh	État du processeur 2

Nom du capteur [ID_CAPTEUR]	Numéro du capteur SNMP [NUMÉRO_ID _CAPTEUR]	Numéro du capteur IPMI [NUMÉRO_ID _CAPTEUR]	Code de type de capteur	Code de type d'événement/ lecture	Description
P1 DTS Thrm Mrgn	83	DBh	01h	01h	Marge thermique avant un arrêt du processeur 1 causé par la température
P2 DTS Thrm Mrgn	84	DCh	01h	01h	Marge thermique avant un arrêt du processeur 2 causé par la température
Voltage Fault	73	D1h	02h	01h	État de défaillance associé à la tension
V_2V5_AUX_X557	42	91h	02h	01h	Tension 2,5V AUX
V_2V1_AUX_X557	43	92h	02h	01h	Tension 2,1V AUX
V_1V2_AUX_X557	44	93h	02h	01h	Tension 1,2V AUX
V_0V83_AUX_X557	45	94h	02h	01h	Tension 0,83V AUX
V_VNN_PCH_AUX	46	95h	02h	01h	Tension VNN PCH AUX
V_1V05_PCH_AUX	47	96h	02h	01h	Tension 1,05V PCH AUX
V_1V8_PCH_AUX	48	97h	02h	01h	Tension 1,8V PCH AUX
V_1V18_AUX	49	98h	02h	01h	Tension 1,18V AUX
V_2V5_AUX	50	99h	02h	01h	Tension 2,5V AUX
V_3V3_AUX	51	9Ah	02h	01h	Tension 3,3V AUX
V_5V_AUX	52	9Bh	02h	01h	Tension 5V AUX
V_3V3	53	9Ch	02h	01h	Tension 3,3V
V_5V	54	9Dh	02h	01h	Tension 5V
V_12V	55	9Eh	02h	01h	Tension 12V
V_3V_BAT	85	DEh	02h	01h	Tension 3V de la batterie
HDD0 Status	27	50h	0Dh	6Fh	État de présence HDD0
HDD1 Status	28	51h	0Dh	6Fh	État de présence HDD1
HDD2 Status	29	52h	0Dh	6Fh	État de présence HDD2
HDD3 Status	30	53h	0Dh	6Fh	État de présence HDD3
HDD4 Status	31	54h	0Dh	6Fh	État de présence HDD4
HDD5 Status	32	55h	0Dh	6Fh	État de présence HDD5
CPU Error		EFh	07h	6Fh	Erreur interne (IERR) et exception de vérification machine (MCE)
Board Status		0Ch	C4h	6Fh	Type et sources de réinitialisation de la carte
Power State		0Dh	D1h	6Fh	État d'alimentation actuel du châssis
PWROK Capture 1		12h	08h	6Fh	État du rail d'alimentation verrouillé
PWROK Capture 2		13h	08h	6Fh	État du rail d'alimentation verrouillé

Nom du capteur [ID_CAPTEUR]	Numéro du capteur SNMP [NUMÉRO_ID _CAPTEUR]	Numéro du capteur IPMI [NUMÉRO_ID _CAPTEUR]	Code de type de capteur	Code de type d'événement/ lecture	Description
Ver Change FPGA		25h	2Bh	6Fh	Détection de changement du micrologiciel du FPGA
Ver Change BMC		27h	2Bh	6Fh	Détection de changement du micrologiciel du BMC

12.3.2. Interprétation des données des capteurs

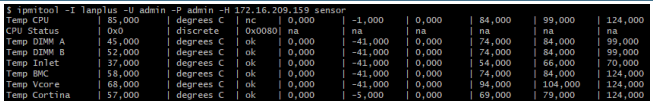
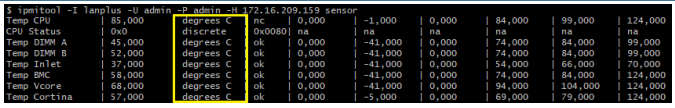
12.3.2.1. Procédure d'interprétation

Avant de commencer la procédure d'interprétation, recueillir les informations suivantes sur l'événement :

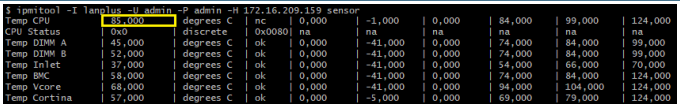
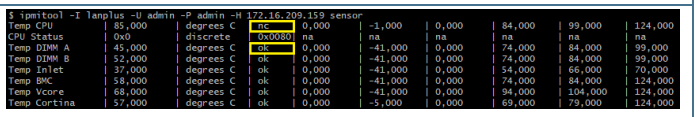
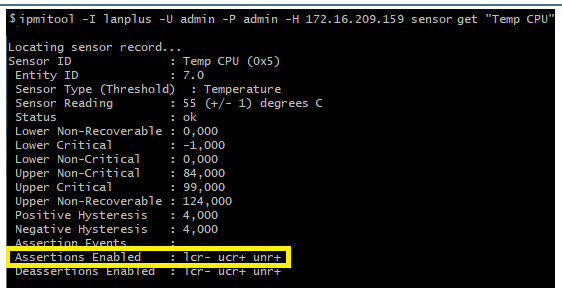
- ID de l'événement
- Capteur associé
- Description

Voir Journal des événements système pour des instructions.

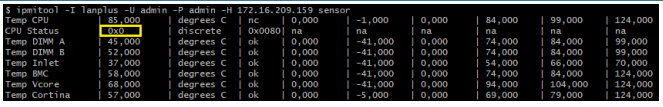
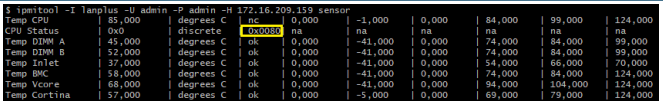
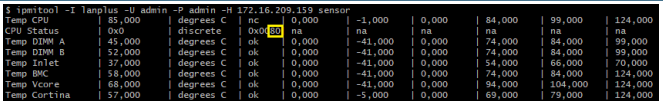
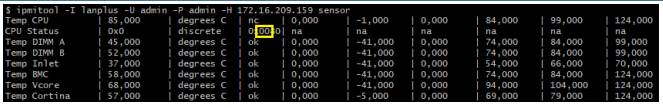
NOTE : IOL et IPMI/KCS sont les méthodes privilégiées pour l'interprétation.

Étape_1	Dans **ipmitool**, la commande sensor retourne un tableau. Les colonnes du tableau sont les suivantes : • Name (nom) • Numerical reading (lecture numérique) • Event/reading type/unit (type d'événement/de lecture/unité) • Reading bytes 3 and 4 (lecture des octets 3 et 4) • Lower non-recoverable threshold value (seuil inférieur irrécupérable) • Lower critical threshold value (seuil critique inférieur) • Lower noncritical threshold value (seuil non critique inférieur) • Upper noncritical threshold value (seuil non critique supérieur) • Upper critical threshold value (seuil critique supérieur) • Upper non-recoverable threshold value (seuil supérieur irrécupérable)	
Étape_2	Consulter la troisième colonne du tableau ou la Liste des capteurs pour savoir si un capteur est de type discret ou non discret. La troisième colonne indique « discrete » pour les capteurs discrets ou un type d'unité pour les capteurs non discrets.	
Étape_3	Consulter Interpréter des données de capteurs non discrets ou Interpréter des données de capteurs discrets en fonction du type d'événement/de lecture du capteur.	

12.3.2.1.1. Interpréter des données de capteurs non discrets

Étape_1	Si le type d'événement/de lecture du capteur est non discret, la valeur de la lecture numérique est affichée dans la deuxième colonne.	
Étape_2	La quatrième colonne indique si un seuil a été dépassé ou non par la valeur de la lecture numérique. Si la valeur de la lecture numérique se situe dans la plage prévue, la quatrième colonne affiche OK. Sinon, le dernier seuil atteint est affiché. Voir Type d'événement/de lecture basé sur des seuils pour les définitions des états de seuil.	
Étape_3	Un événement sera créé en fonction de l'assertion activée pour le capteur spécifié. InviteSE_OrdinateurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] sensor get [ID_CAPTEUR]**	

12.3.2.1.2. Interpréter des données de capteurs discrets

Étape_1	La deuxième colonne du tableau retourné par la commande sensor doit être ignorée si le capteur est de type discret. Par défaut, les capteurs discrets doivent avoir une valeur de lecture numérique de **0x0**.	
Étape_2	La quatrième colonne du tableau est une agrégation des octets 3 et 4 de la réponse retournée à la lecture du capteur. L'octet 3 est l'octet de plus faible poids dans l'agrégation des octets 3 et 4.	
Étape_3	En ce qui concerne l'octet 3, toutes les valeurs doivent être 0x80, ce qui signifie que tous les messages d'événements sont activés pour ce capteur.	
Étape_4	Quant à l'octet 4, il représente les décalages d'états/d'événements (states/event offsets) définis pour chaque type dans la spécification IPMI. Voir Type d'événement/de lecture propre au capteur pour les listes d'états possibles pour chaque capteur.	
Étape_5	Si cela est spécifié dans la description du type d'événement/de lecture (event/reading type), voir Accéder aux octets 2 (et 3 optionnel) des données d'événement pour plus de détails.	

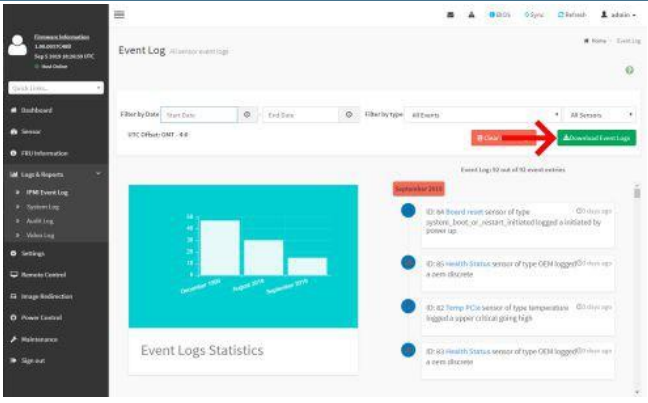
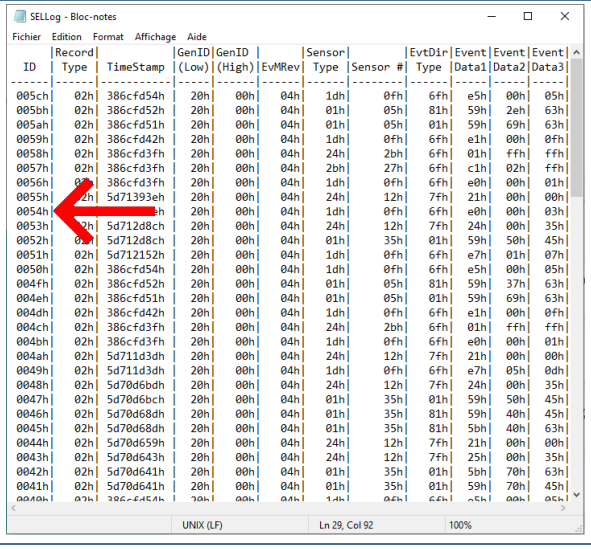
12.3.2.1.3. Accéder aux octets 2 (et 3 optionnel) des données d'événement

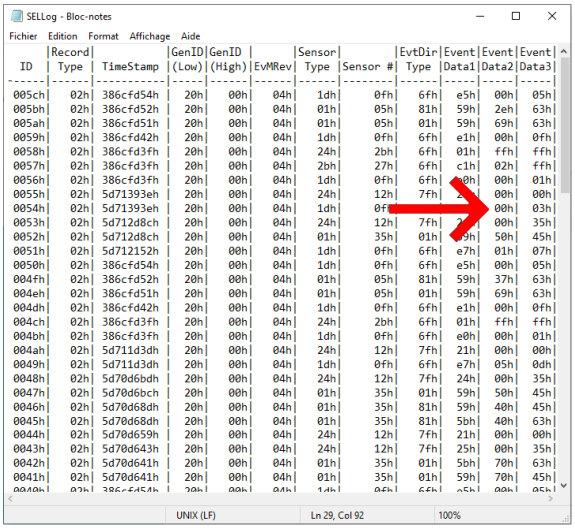
NOTE : Cette partie de la procédure n'est nécessaire que si le capteur concerné le spécifie. Voir Type d'événement/de lecture propre au capteur. Les données des événements sont accessibles :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant IPMI

12.3.2.1.3.1. Accéder à l'octet 2 des données d'événement en utilisant l'interface utilisateur Web du BMC

Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

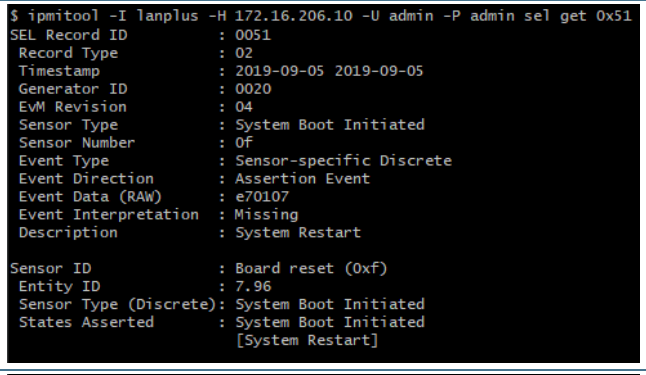
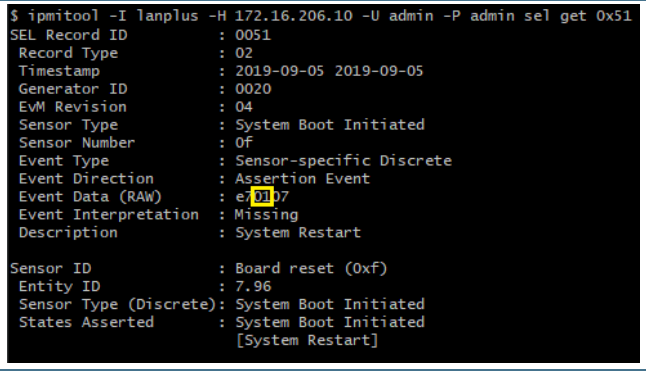
Étape_1	Convertir l'ID de l'événement en hexadécimal.	
Étape_2	Accéder à l'interface utilisateur Web du BMC du serveur.	
Étape_3	Télécharger les journaux des événements système et ouvrir le fichier avec n'importe quel éditeur de texte.	
Étape_4	Dans le fichier **SELLog**, trouver l'événement à l'aide de son ID.	

Étape_5	La colonne Event Data2 contient l'information souhaitée. Voir Accéder aux octets 2 (et 3 optionnel) des données d'événement pour interpréter l'octet des données d'événement.	

12.3.2.1.3.2. Accéder à l'octet 2 des données d'événement en utilisant IPMI

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI sur LAN (IOL), mais certaines tâches peuvent également être effectuées en utilisant KCS (Accéder au BMC en utilisant IPMI via KCS).

Pour utiliser KCS, il faut supprimer les paramètres IOL de la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

Étape_1	Convertir l'ID de l'événement en hexadécimal.	
Étape_2	Afficher les informations détaillées de l'événement en utilisant la conversion hexadécimale de l'ID. InviteSE_ServeurDistant:~$ **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] sel get [ID_ÉVÉNEMENT]**	
Étape_3	Noter l'octet 2 (et le 3 si requis) des données de l'événement et le paramètre **Sensor Number**. La ligne **Event Data (RAW)** est une agrégation des trois octets des données d'événement, où l'octet 2 est le deuxième octet de plus fort poids.	
Étape_4	Voir Accéder aux octets 2 (et 3 optionnel) des données d'événement pour interpréter l'octet des données d'événement.	

12.3.2.2. Information pour l'interprétation

Chaque capteur possède un attribut type de capteur (sensor type) et un attribut type d'événement/de lecture (sensor event/reading type). Lorsqu'un capteur génère un événement, des données supplémentaires sur l'événement peuvent être trouvées dans l'octet 2 des données d'événement (event data byte 2). Pour plus d'informations sur les capteurs IPMI, voir la documentation IPMI.

Pour une liste de tous les capteurs de la plateforme, voir Liste des capteurs.

12.3.2.2.1. Type de capteur (sensor type)

L'attribut Sensor type définit ce que le capteur surveille.

Le tableau suivant répertorie tous les types de capteurs IPMI présents dans la plateforme.

Type de capteur (sensor type)	Description
01h (Temperature)	Information générale sur les températures de différents composants.
02h (Voltage)	Information générale sur les tensions de la carte ou du bloc d'alimentation.
04h (Fan)	Information générale sur le ou les ventilateurs de la plateforme (ex. vitesse, présence, défaillance).
07h (Processor)	Information générale sur le processeur (ex. présence, défaillance, état de santé).
08h (Power supply)	Information générale sur le bloc d'alimentation (ex. présence, défaillance, état de santé).
09h (Power Unit)	Information générale sur l'unité d'alimentation.
0Ch (Memory)	Information générale sur la mémoire (erreur).
0Dh (Drive Slot/Bay)	Information générale sur les emplacements et logements des unités de stockage.
10h (Event logging disabled)	Information générale sur le Journal des événements système désactivé de la plateforme.
12h (System Event)	Information générale sur les événements système.
13h (Critical Interrupt)	Information générale sur les interruptions critiques du système.
23h (Watchdog2)	Information générale sur le mécanisme de surveillance (watchdog) IPMI.
28h (Management Subsys Health)	Information générale sur l'état de santé du sous-système de gestion (BMC).
2Bh (Version Change)	Détection des changements relatifs aux micrologiciels (FPGA et BMC).
C4h (OEM board reset)	Capteur défini par Kontron pour le type et les sources de réinitialisation de la carte.
D1h (OEM Power State)	Capteur défini de Kontron pour l'état d'alimentation.

12.3.2.2.2. Type d'événement/de lecture du capteur (sensor event/reading type)

L'attribut Event/reading type définit comment la lecture de la valeur doit être interprétée et comment les événements liés au capteur sont déclenchés. Les attributs Event/reading type peuvent être discrets ou non discrets.

Le tableau suivant décrit les attributs Event/reading type présents dans la plateforme.

Type d'événement/de lecture (Event/reading type)	Code du type d'événement à 7 bits	Description	Décalage
Threshold based	01h	Non discret, ce qui signifie qu'il dispose d'une lecture numérique et de déclencheurs d'événements.	Les décalages sont standard et définis dans le tableau Type d'événement/de lecture basé sur des seuils.
Sensor-specific	6Fh	Discret, ce qui signifie qu'il n'a pas de valeur numérique, mais qu'il a des déclencheurs d'événements.	Les décalages sont propres au type de capteur et définis dans le tableau Type d'événement/de lecture propre au capteur.

12.3.2.2.2.1. Type d'événement/de lecture basé sur des seuils

Ce type de capteur crée des événements lorsque la lecture numérique d'un capteur atteint un seuil préétabli. Les capteurs basés sur des seuils de cette plateforme peuvent retourner une tension, une température ou une vitesse de ventilateur.

Décalage de l'événement (event offset)	Déclencheur de l'événement (event trigger)	État (state)
00h	Lower noncritical - going low	nc
01h	Lower noncritical - going high	
02h	Lower critical - going low	cr
03h	Lower critical - going high	
04h	Lower non-recoverable - going low	nr
05h	Lower non-recoverable - going high	
06h	Upper noncritical - going low	nc
07h	Upper noncritical - going high	
08h	Upper critical - going low	cr
09h	Upper critical - going high	
0Ah	Upper non-recoverable - going low	nr
0Bh	Upper non-recoverable - going high	

12.3.2.2.2.2. Type d'événement/de lecture propre au capteur

Un type d'événement/de lecture propre au capteur est un type de capteur discret, ce qui signifie qu'il n'a pas de valeur numérique. Lorsqu'un capteur est de type propre au capteur, les valeurs de décalage de l'événement sont définies par le type de capteur.

NOTE : La plateforme ne prend pas en charge tous les décalages de l'événement propres aux capteurs. Le tableau suivant répertorie les décalages de l'événement propre aux capteurs mis en œuvre dans la plateforme.

NOTE : L'information dans le tableau n'est pas traduite puisqu'il s'agit des conventions IPMI.

ID	Nom du capteur (sensor name)	Type de capteur (sensor type)	Décalage spécifique (specific offset)	Déclenchement/état de l'événement (event trigger/state)
33h	PCI Error NOTE : Voir le tableau Données d'événement générées par le gestionnaire SMI ci-	13h (Critical Interrupt)	04h	PCI PERR
			05h	PCI SERR
			07h	Bus Correctable Error
			08h	Bus Uncorrectable Error
			0Ah	Bus Fatal Error

ID	Nom du capteur (sensor name)	Type de capteur (sensor type)	Décalage spécifique (specific offset)	Déclenchement/état de l'événement (event trigger/state)
	dessous pour plus de détails.		0Fh	LastBoot PCIe Error
34h	Memory Error NOTE : Voir le tableau Données d'événement générées par le gestionnaire SMI ci-dessous pour plus de détails.	0Ch (Memory)	00h	Correctable ECC / Other correctable memory error
			01h	Uncorrectable ECC / other uncorrectable memory error
			02h	Parity
			05h	Correctable ECC / other correctable memory error logging limit reached
35h	Processor Error NOTE : Voir le tableau Données d'événement générées par le gestionnaire SMI ci-dessous pour plus de détails.	07h (Processor)	05h	Configuration Error
36h	Direct Memory Access (DMA) Error NOTE : Voir le tableau Données d'événement générées par le gestionnaire SMI ci-dessous pour plus de détails.	07h (Processor)	05h	Configuration Error
37h	OutBound Traffic Controller (OTC) Error NOTE : Voir le tableau Données d'événement générées par le gestionnaire SMI ci-dessous pour plus de détails.	07h (Processor)	05h	Configuration Error
38h	InBound Traffic Controller (OTC) Error NOTE : Voir le tableau Données d'événement générées par le gestionnaire SMI ci-dessous pour plus de détails.	07h (Processor)	05h	Configuration Error
39h	Intel VT-d Error NOTE : Voir le tableau Données	07h (Processor)	05h	Configuration Error

ID	Nom du capteur (sensor name)	Type de capteur (sensor type)	Décalage spécifique (specific offset)	Déclenchement/état de l'événement (event trigger/state)
	d'événement générées par le gestionnaire SMI ci-dessous pour plus de détails.			
05h	FP NMI Diag Int	13h (Critical Interrupt)	00h	07h (Processor)
34h	Fan Failure	04h (Fan)	00h	Failure reported on fan #1
			...	
			05h	Failure reported on fan #6
03h	IPMI Watchdog NOTE : Voir le tableau Données d'événement générées par le BIOS ci-dessous pour plus de détails.	23h(Watchdog2)	00h	Timer expired
			01h	Hard reset
			02h	Power down
			03h	Power Cycle
			08h	Timer interrupt
07h	System Event Log	10h(Event Logging Disabled)	02h	System event log cleared
			04h	System event log full
			05h	System event log almost full
08h	System Event **NOTE** : Voir le tableau Données d'événement ci-dessous pour plus de détails.	12h(System Event)	04h	PEF Action
			05h	Timestamp Clock Sync
18h	P1 Status	07h (Processor)	01h	Thermal trip
19h	P2 Status		0Ah	Throttled
50h	HDD0 Status	0Dh(Drive Slot / Bay)	00h	Drive Presence
51h	HDD1 Status			
52h	HDD2 Status			
53h	HDD3 Status			
54h	HDD4 Status			
55h	HDD5 Status			
0Ch	Board Status **NOTE** : Voir le tableau Données d'événement ci-dessous pour plus de détails.	C4h (OEM board reset)	00h	Push Button
			02h	Unknown
			06h	Cold Reset
			07h	IPMI Command
			09h	Power Up Reset
			0Ah	Power Down
0Dh	Power State	D1h (OEM Power State)	00h	Power ON
			01h	Power OFF
			02h	Power ON Request
			03h	Power OFF Request
			04h	Full Reset In Progress
12h	PWROK Capture 1	08h (Power supply)	00h	Power supply presence detected

ID	Nom du capteur (sensor name)	Type de capteur (sensor type)	Décalage spécifique (specific offset)	Déclenchement/état de l'événement (event trigger/state)
13h	PWROK Capture 2		01h	Power supply failure detected
25h	Ver Change FPGA	2Bh (Version Change)	01h	Firmware change detected
27h	Ver Change BMC			
EFh	CPU Error	07h (Processor)	00h	IERR
			0Bh	Machine Check Exception

12.3.2.2.2.3. Autres types d'événements/de lecture

NOTE : L'information dans le tableau n'est pas traduite puisqu'il s'agit des conventions IPMI.

ID	Nom du capteur (sensor name)	Type de capteur (sensor type)	Décalage spécifique (specific offset)	Déclenchement/état de l'événement (event trigger/state)
0Ah	BMC Watchdog	03h ('digital' Discrete - Assert/Deassert)	01h	State asserted
0Bh	VR Watchdog			
82h	CPU Missing			
61h	Fan1 Present	08h ('digital' Discrete - Present/Absent)	00h	Device absent
62h	Fan2 Present			
63h	Fan3 Present			
64h	Fan4 Present		01h	Device present
65h	Fan5 Present			
66h	Fan6 Present			
02h	Pwr Unit Redund	0Bh (Discrete)	00h	Fully Redundant
			01h	Redundancy Lost
			03h	Non-Redundant: Sufficient from Redundant
			04h	Non-Redundant: Sufficient from Insufficient
			05h	Non-Redundant: Insufficient Resources

12.3.2.2.3. Octet 2 des données d'événement

Lorsqu'un capteur déclenche un événement dans le Journal des événements système, l'octet 2 des données d'événement pourrait contenir des informations supplémentaires sur l'événement. Cet octet des données d'événement doit être lu uniquement sur le décalage spécifique (specific offset) indiqué dans les tableaux suivants.

NOTE : L'information dans le tableau n'est pas traduite puisqu'il s'agit des conventions IPMI.

ID	Nom du capteur (sensor name)	Décalage spécifique (specific offset)	Déclenchement/état de l'événement (event trigger/state)
03h	IPMI Watchdog	00h 01h 02h 03h 08h	[7:4] - Interrupt type: • 0x00 = None • 0x10 = SMI • 0x20 = NMI • 0x30 = Messaging interrupt • 0xF0 = Unspecified [3:0] - Timer use at expiration:

ID	Nom du capteur (sensor name)	Décalage spécifique (specific offset)	Déclenchement/état de l'événement (event trigger/state)
			• 0x00 = Reserved • 0x01 = BIOS/FRB2 • 0x02 = BIOS/POST • 0x03 = OS load • 0x04 = SMS/OS • 0x05 = OEM • 0x0F = Unspecified
08h	System Event	04h PEF Action	Les bits suivants reflètent les actions PEF qui sont sur le point d'être exécutées une fois la correspondance des filtres d'événement établie. L'événement est saisi avant que les actions ne soient exécutées. [7:6] - reserved • [5] - 1b = Diagnostic Interrupt (NMI) [4] - 1b = OEM action • [3] - 1b = power cycle • [2] - 1b = reset • [1] - 1b = power off • [0] - 1b = Alert
		05h Timestamp Clock Synch	Cet événement peut être utilisé pour enregistrer le moment où des modifications sont apportées à l'horloge d'horodatage afin de déterminer les différences de date et d'heure entre les entrées du SEL. [7] - first/second • 0x0 = event is first of pair. • 0x1 = event is second of pair. [6:4] - reserved [3:0] - Timestamp Clock Type • 0x0 = SEL Timestamp Clock updated. (Également utilisé lorsque les horloges d'horodatage du SEL et des SDR sont reliées entre elles). • 0x1 = SDR Timestamp Clock updated
0Ch	Board Status	00h 02h 06h 07h	Indique des informations supplémentaires sur le type de réinitialisation : Specific offset 00h: • 0x02 = Push button reset Specific offset 02h: • 0x04 = Straight to S5 condition • 0x0d = Serial port reset • All others = Unknown reset cause Specific offset 06h: • 0x05 = Cold reset without power cycle • 0x0F = Cold reset with power cycle Specific offset 07h: • 0x01 = Power reset IPMI command
25h	Ver Change FPGA	01h	• 0x11 Version change type is FPGA.
27h	Ver Change BMC	01h	• 0x02 Version change type is BMC.

12.3.2.2.3.1. Description des octets 2 et 3 des données d'événement générées par le gestionnaire SMI

Ce tableau définit les octets 2 et 3 des données d'événement pour les capteurs définis par l'OEM générées par le gestionnaire SMI du BIOS (ID du générateur = 0x21).

ID	Capteur (sensor)	Type de capteur (sensor type)	Décalage spécifique (specific offset)	Données de l'événement 2 (event data 2)	Données de l'événement 3 (event data 2)
33h	PCI Error	13h (Critical Interrupt)	04h 05h 07h 08h 0Ah	[7:0] - PCI bus number for failed device	[7:3] - PCI device number for failed device [2:0] - PCI function number for failed device
34h	Mémoire Error	0Ch (Memory)	00h 01h 02h 05h	[2:1] - Memory Controller Number: • 0x0 = Memory Controller 0 for channels A, B, C • 0x1 = Memory Controller 1 for channels D, E, F [0] - Current/Last Boot Error: • 0x0 = Current Boot • 0x1 = Last Boot	[7:6] - CPU Socket Number: • 0x0 = CPU1 • 0x1 = CPU2 [5:4] - Channel Number: • 0x0 = Channel A if Memory Controller 0 • Channel D if Memory Controller 1 • 0x1 = Channel B if Memory Controller 0 • Channel E if Memory Controller 1 • 0x2 = Channel C if Memory Controller 0 • Channel F if Memory Controller 1 [3:0] - DIMM Number: • 0x0 = DIMM 1 • 0x1 = DIMM 2
35h	Processeur Error	07h (Processor)	05h	[7:4] - CPU Socket Number: • 0x0 = CPU1 • 0x1 = CPU2 [3:0] = Bank Type: • 0x0 = None • 0x1 = IFU • 0x2 = DCU • 0x3 = DTLB • 0x4 = MLC • 0x5 = PCU • 0x6 = IIO • 0x7 = CHA • 0x8 = UPI	[7:4] - Processor Error Type: • 0x0 = UNKNOWN • 0x1 = Cache • 0x2 = TLB (Translation Look aside Buffer) • 0x4 = Bus • 0x8 = Micro Architecture [3:1] = Error Severity: • 00 = Correctable Error • 01 = Fatal Error • 02 = Corrected Error [0] - Current/Last Boot Error: • 0x0 = Current Boot • 0x1 = Last Boot

ID	Capteur (sensor)	Type de capteur (sensor type)	Décalage spécifique (specific offset)	Données de l'événement 2 (event data 2)	Données de l'événement 3 (event data 2)
36h	Direct Memory Access (DMA) Error	07h (Processor)	05h	[7:4] - CPU Socket Number: • 0x0 = CPU1 • 0x1 = CPU2 [3:1] - CPU Stack Number [0] - Current/Last Boot Error: • 0x0 = Current Boot • 0x1 = Last Boot	[7:0] - Direct Memory Access Error codes as per Skylake-EP EDS Specification: 40h = Received_Poisoned_Data_from_DP_status 41h = DMA_internal_HW_parity_error_status 42h = Cfg_Reg_Parity_Error_status 43h = RD_Cmpl_Header_Error_status 44h = Read_address_decode_error_status 45h = Multiple errors 46h = DMA Transfer Source Address Error. 47h = DMA Transfer Destination Address Error. 48h = Next Descriptor Address Error. 49h = Error when reading a DMA descriptor 4Ah = Chain Address Value Error. 4Bh = CHANCMD Error 4Ch = Data Parity Error 4Dh = DMA Data Parity Error. 4Eh = Read Data Error. 4Fh = Write Data Error. 50h = Descriptor Control Error. 51h = Descriptor Length Error. 52h = Completion Address Error. 53h = Interrupt Configuration Error. 54h = CRC or XOR P Error 55h = XOR Q Error 56h = Descriptor Count Error 57h = DIF All F Detect Error 58h = DIF Guard Tag Error 59h = DIF Application Tag Error 5Ah = DIF Reference Tag Error 5Bh = DIF Bundle Error

ID	Capteur (sensor)	Type de capteur (sensor type)	Décalage spécifique (specific offset)	Données de l'événement 2 (event data 2)	Données de l'événement 3 (event data 2)
37h	OutBound Traffic Controller (OTC) Error	07h (Processor)	05h	[7:4] - CPU Socket Number: • 0x0 = CPU1 • 0x1 = CPU2 [3:1] - CPU Stack Number [0] - Current/Last Boot Error: • 0x0 = Current Boot • 0x1 = Last Boot	[7:0] - Outbound Traffic Controller Error codes as per Skylake-EP EDS Specification: 60h = OTC OB credit underflow 61h = OTC OB credit overflow 62h = Parity error in the OTC hdr_q RF 63h = Parity error in the OTC addr_q RF 64h = ECC uncorrected error in the OTC dat_dword RF 65h = Completer abort 66h = Master abort 67h = Multicast target error for ITC 68h = ECC corrected error in the OTC dat_dword RF 69h = Misc block request overflow 6Ah = IOAPIC RTE parity error 6Bh = Parity error on incoming data from IRP 6Ch = Parity error on incoming addr from IRP
38h	Inbound Traffic Controller (ITC) Error	07h (Processor)	05h	[7:4] - CPU Socket Number: • 0x0 = CPU1 • 0x1 = CPU2 [3:1] - CPU Stack Number [0] - Current/Last Boot Error: • 0x0 = Current Boot • 0x1 = Last Boot	[7:0] - Inbound Traffic Controller Error codes as per Skylake-EP EDS Specification: 80h = ITC IRP credit underflow 81h = ITC IRP credit overflow 82h = Parity error in the incoming data from PCIe 83h = Parity error in the ITC hdr_q RF 84h = Parity error in the ITC vtd_misc_info RF 85h = Parity error in the ITC addr_q RF 86h = ECC corrected error in the ITC dat_dword RF 87h = ECC uncorrected error in the ITC dat_dword RF 88h = Completer abort 89h = Master abort 8Ah = Multicast target error for ITC only

ID	Capteur (sensor)	Type de capteur (sensor type)	Décalage spécifique (specific offset)	Données de l'événement 2 (event data 2)	Données de l'événement 3 (event data 2)
39h	Intel VT-d Error	07h (Processor)	05h	[7:4] - CPU Socket Number: • 0x0 = CPU1 • 0x1 = CPU2 [3:1] - CPU Stack Number [0] - Current/Last Boot Error: • 0x0 = Current Boot • 0x1 = Last Boot	[7:0] - Intel VT-d Local Group error codes as per Skylake-EP EDS Specification: 90h = Data Parity Error during Context Cache Lookup 91h = Data Parity Error during L1 Lookup 92h = Data Parity Error during L2 Lookup 93h = Data Parity Error during L3 Lookup 94h = TLB0 Data Parity Error 95h = TLB1 Data Parity Error 96h = Unsuccessful completion status received in the coherent interface 97h = Illegal request to 0xFEE 98h = Protected Memory region space violated status A0h = Intel VT-d spec defined errors

12.3.3. Configuration et utilisation des traps SNMP

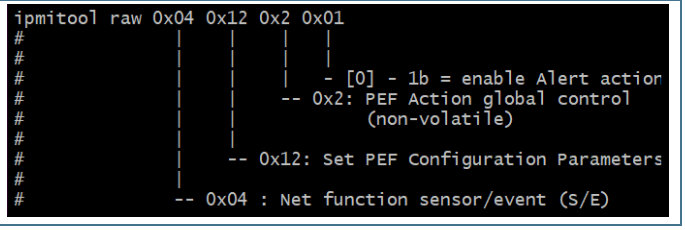
12.3.3.1. Mettre en place des alarmes SNMP en utilisant IPMI

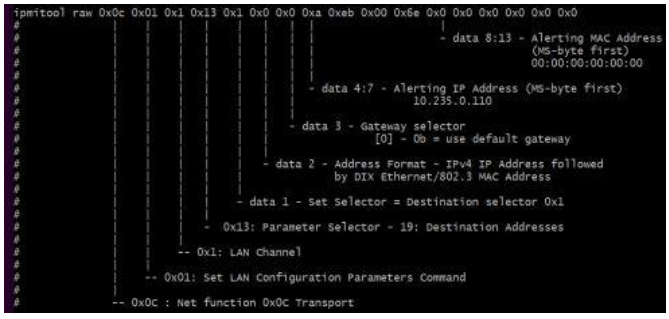
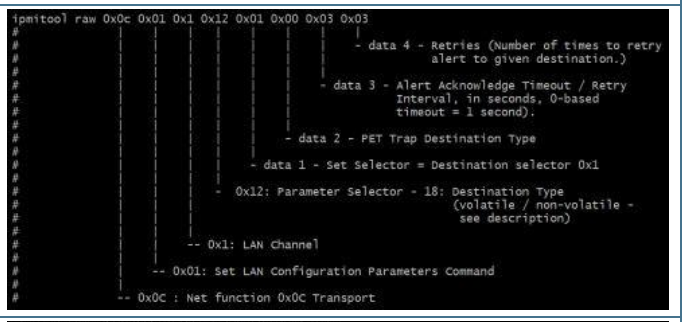
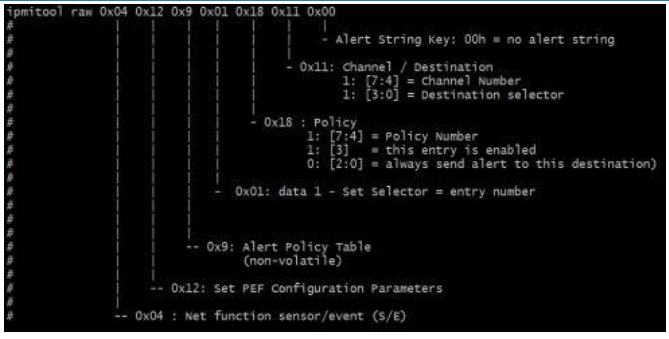
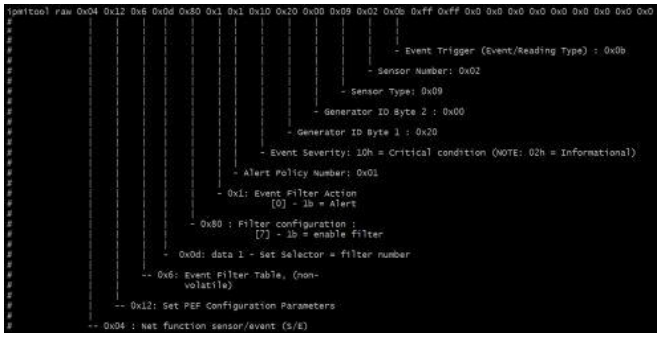
Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL (Accéder au BMC en utilisant IPMI sur LAN (IOL)). Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

NOTE : Il est fortement recommandé de se familiariser avec les sections suivantes de la spécification IPMI 2.0 :

- 17. Platform Event Filtering [filtrage des événements de la plateforme] (PEF)
- 30. PEF and Alerting Commands [commandes PEF et d'alerte]
- 23. IPMI LAN Commands [commandes IPMI LAN]

NOTE : La procédure suivante est pour une configuration typique des traps SNMP et pourrait donc nécessiter des adaptations supplémentaires.

Étape_1	Activer le filtrage des événements de la plateforme (PEF). InviteSE_ServeurLocal:~# **ipmitool raw 0x04 0x12 0x1 0x03**	
Étape_2	Activer les alertes. InviteSE_ServeurLocal:~# **ipmitool raw 0x04 0x12 0x2 0x01**	

Étape_3	Configurer l'adresse de destination. InviteSE_ServeurLocal:~# **ipmitool raw 0x0c 0x01 [CANAL] 0x13 0x1 0x0 0x0 [IP_CANAL] [ADRESSE_MAC]** **NOTE** : Dans ce cas, le plan de gestion serait sur le canal 1 et le plan des données sur le canal 2.	
Étape_4	Configurer une alerte associée à la destination. InviteSE_ServeurLocal:~# **ipmitool raw 0x0c 0x01 [CANAL]** **0x12 0x01 0x00 [DÉLAI_ATTENTE_SEC] [NOMBRE_TENTATIVES]** **NOTE** : Un maximum de 16 filtres d'événements peut être configuré.	
Étape_5	Configurer la politique d'alerte. InviteSE_ServeurLocal:~# **ipmitool raw 0x04 0x12 0x9 0x01 0x18 0x21 0x00**	
Étape_6	Configurer un nouveau filtre d'événement. Voir Exemples de configuration d'alarme. InviteSE_ServeurLocal:~# **ipmitool raw 0x04 0x12 0x6 0x0d 0x80 0x1 0x1 0x10 0x20 0x00 0x09 0x02 [ID_CAPTEUR] 0xff** **0xff 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0** **NOTE** : Un maximum de 16 filtres d'événements peut être configuré.	 

12.3.3.1.1. Exemples de configuration d'alarme

12.3.3.1.1.1. Détecter un disque dur retiré

Filtre d'événement (event filter) : 15

Politique d'alerte (alert policy) : 1

Gravité (severity) : informatif

```
InviteSE_ServeurLocal:~# ipmitool raw 0x04 0x12 0x6 0x0f 0x80 0x1 0x1 0x02 0xff 0xff 0xd 0xff 0xff 0x1 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
```

12.3.3.1.1.2. Détecter un ventilateur retiré

Filtre d'événement (event filter) : 14

Politique d'alerte (alert policy) : 1

Gravité (severity) : critique

```
InviteSE_ServeurLocal:~# ipmitool raw 0x04 0x12 0x6 0x0e 0x80 0x1 0x1 0x10 0xff 0xff 0x4 0xff 0x8 0x1 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
```

12.3.3.1.1.3. Détecter une perte d'alimentation CA ou CC

Filtre d'événement (event filter) : 13

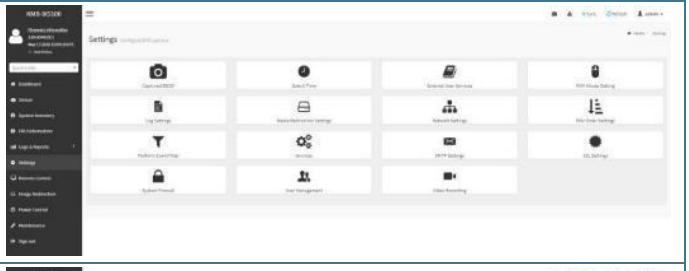
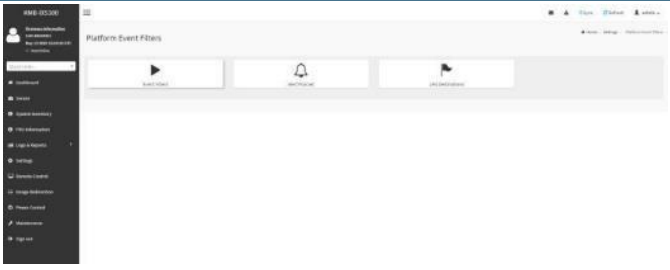
Politique d'alerte (alert policy) : 2

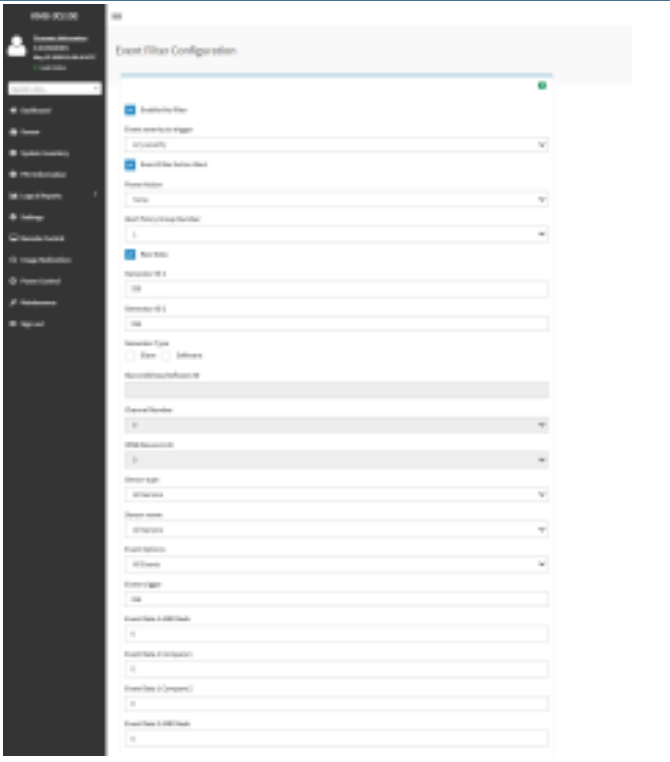
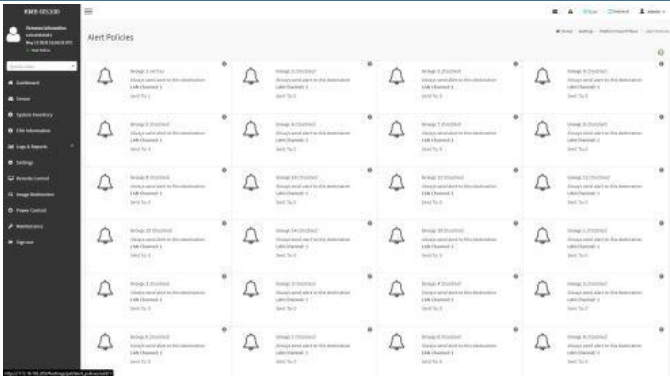
Gravité (severity) : critique

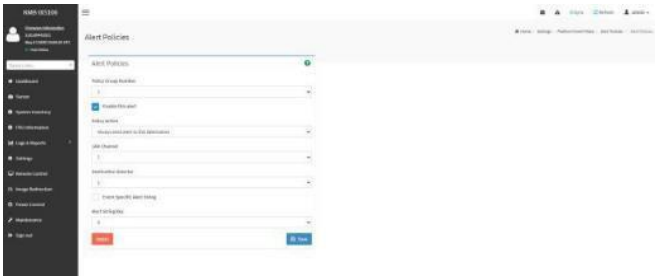
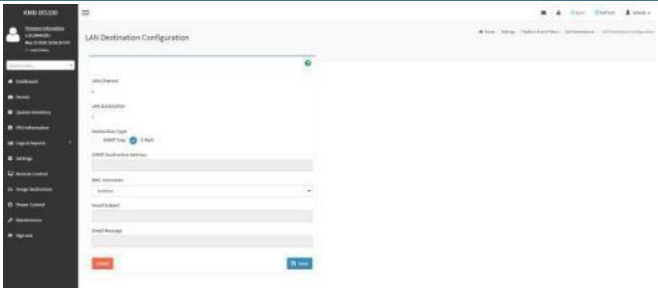
```
InviteSE_ServeurLocal:~# ipmitool raw 0x04 0x12 0x6 0x0d 0x80 0x1 0x1 0x10 0xff 0xff 0x9 0xff 0xb 0xff 0xff 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
```

12.3.3.2. Mettre en place des traps SNMP en utilisant l'interface utilisateur Web

Les procédures suivantes seront exécutées à l'aide de la méthode ayant recours à l'interface utilisateur Web.

Étape_1	Cliquer sur **Settings** puis **sur Platform Event Filter**.	
Étape_2	Cliquer sur **Event Filters**.	

Étape_3	Cette page sert à ajouter et modifier des filtres. Par défaut, 15 filtres d'événement sont configurés parmi les 40 disponibles. Choisir **All** pour afficher tous les emplacements configurés et non configurés. Choisir **Configured** pour afficher les emplacements configurés. Choisir **Unconfigured** pour afficher les emplacements non configurés. Cliquer sur le X pour supprimer un filtre d'événement de la liste. Sélectionner une carte non configurée pour ajouter un filtre.	
Étape_4	Sélectionner une carte pour modifier la configuration du filtre.	
Étape_5	Pour accéder aux Alert Policies, cliquer sur **Settings**, sur **Platform Event Filter**, puis sur **Alert Policies**. L'écran affiche toutes les politiques d'alerte configurées et les emplacements disponibles. Choisir une politique d'alerte pour la modifier ou en ajouter une nouvelle. Cliquer sur le X pour supprimer une politique d'alerte de la liste. Un maximum de 60 emplacements sont disponibles.	

Étape_6	Configurer l'alerte sélectionnée en utilisant les options disponibles dans la section Alert Policies.	
Étape_7	Pour accéder aux LAN destinations, cliquer sur **Settings**, sur **Platform Event Filter**, puis sur **LAN Destinations**. L'écran affiche tous les emplacements LAN destination. Sélectionner une carte LAN destination pour modifier la configuration ou pour en ajouter une nouvelle. Cliquer sur le X pour supprimer une entrée de la liste. Un maximum de 15 emplacements sont disponibles. Sélectionner un canal LAN applicable dans la liste Send Test Alert : Sélectionner un emplacement configuré et cliquer sur Send Test Alert pour générer un exemple de message d'alerte vers la destination configurée. NOTE : Les tests d'alerte vers des adresses de courriel ne peuvent être envoyés que lorsque la configuration SMTP est activée. Cliquer sur Settings, puis sur SMTP pour procéder à la configuration. Assurez-vous que l'adresse du serveur SMTP et les numéros de port sont configurés correctement.	
Étape_8	Configurer la destination LAN dans la page LAN Destination Configuration.	

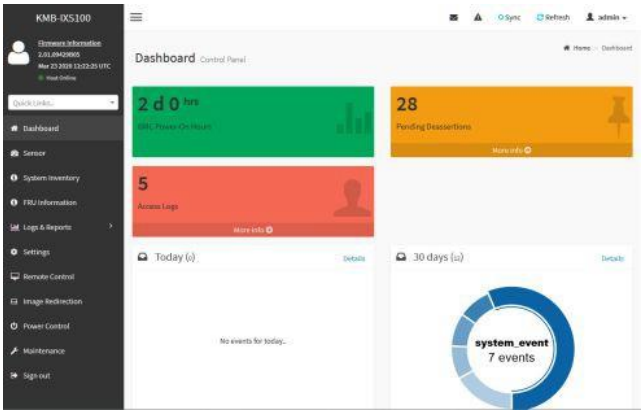
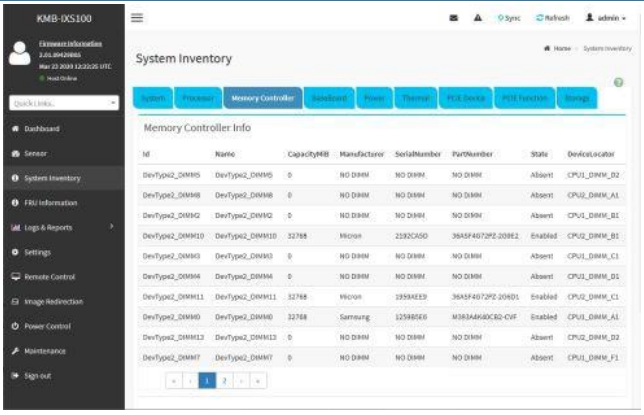
12.3.4. Inventaire du système

L'inventaire du système fournit des renseignements sur les CPU, la mémoire DIMM, le stockage, les capteurs, etc.

12.3.4.1. Accéder à l'inventaire

Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

Étape_1	Accéder à l'interface utilisateur Web du BMC.

Étape_2	Dans le menu de gauche, cliquer sur **System Inventory**.	
Étape_3	L'inventaire du système s'affiche.	

12.3.5. Gestionnaire d'alarmes de télécom

Le gestionnaire d'alarmes de télécom (TAM) est une fonctionnalité du micrologiciel du BMC. Les demandes d'alarme reçues par le BMC sont traitées et affichées sur le panneau d'alarmes de télécom en fonction du modèle de panneau d'alarmes utilisé.

12.3.5.1. Panneau d'alarmes de télécom

Le panneau est équipé de quatre indicateurs : un indicateur d'alarme d'alimentation indépendant et trois indicateurs correspondant aux trois niveaux de gravité des alarmes (critique, majeure, mineure).

CG00100

12.3.5.2. Modèles d'alarmes de télécom

La fonction TAM du BMC prend en charge deux modèles qui déterminent le mode de fonctionnement du panneau d'alarmes de télécom : modèle « la plus grave seulement » (par défaut) et modèle « tous les niveaux de gravité ».

12.3.5.2.1. Modèle « la plus grave seulement » (par défaut)

Avec ce modèle, seul l'indicateur du panneau correspondant au niveau le plus grave, à savoir une alarme critique, est actif. Tous les autres indicateurs du panneau sont inactifs. Si l'alarme la plus grave est une alarme d'alimentation, l'indicateur d'alarme d'alimentation est actif; sinon, il est inactif.

12.3.5.2.2. Modèle « tous les niveaux de gravité »

Avec ce modèle, seuls les indicateurs du panneau d'alarmes de télécom correspondant à toutes les alarmes activées sont actifs. Le panneau d'alarmes de télécom peut indiquer n'importe quelle combinaison des trois niveaux de gravité des alarmes. Si une alarme est associée à l'alimentation, l'indicateur d'alarme d'alimentation est actif; sinon, il est inactif. L'alarme d'alimentation n'a pas nécessairement à être la plus grave.

12.3.5.3. Configurer le gestionnaire d'alarmes de télécom

Le gestionnaire d'alarmes de télécom peut être configuré en utilisant IPMI et une commande commande OEM de Kontron.

12.3.5.3.1. Récupérer la configuration du gestionnaire d'alarmes de télécom

Utiliser la commande IPMI suivante pour obtenir l'octet de la configuration du TAM.

```
# ipmitool raw 0x3c 0x0B 0x00 0x00
                  |  ---------  |
                  |       |     |      -- Get TAM configuration
                  |       |
                  |       -- TAM command
                  |
                  -- Network Function (netfn): OEM command
```

12.3.5.3.2. Définir la configuration du gestionnaire d'alarmes de télécom

Utiliser la commande IPMI suivante pour définir un nouvel octet pour la configuration du TAM. Réinitialiser le BMC ou effectuer un cycle d'alimentation pour que la nouvelle configuration devienne active.

```
# ipmitool raw 0x3c 0x0B 0x00 0x01 [TAM Parameter]
                  |  ---------  |       |
                  |       |     |       |      -- Configuration byte
                  |       |     |       |
                  |       |     |       -- Set TAM configuration
                  |       |     |
                  |       |     -- TAM command
                  |       |
                  |       -- Network Function (netfn): OEM command
```

12.3.5.3.3. Octet de configuration

Position du bit	Description	Valeurs
[0]	Activé / Désactivé	0 : Le gestionnaire d'alarmes de télécom est désactivé. Les quatre indicateurs peuvent être contrôlés par l'utilisateur avec une commande IPMI dédiée. 1 : Le gestionnaire d'alarmes de télécom est activé (valeur par défaut).
[1]	Modèle d'alarmes de télécom	0 : Modèle « tous les niveaux de gravité ». 1 : Modèle « la plus grave seulement » (valeur par défaut).
[2-7]	Non utilisé	

12.3.5.3.4. Exemple

```
# Get the TAM configuration
# ipmitool raw 0x3c 0x0B 0x00 0x00
# 00
#
# Set TAM to Enable/'Most Severe Only' mode
# ipmitool raw 0x3c 0x0B 0x00 0x01 0x03
#
# Reset to BMC to apply the configuration change
# ipmitool mc reset cold
#
# Get the TAM configuration to verify
# ipmitool raw 0x3c 0x0B 0x00 0x00
# 03
```

12.4. Maintenance

12.4.1. Journal des événements système

Le journal des événements système est accessible :

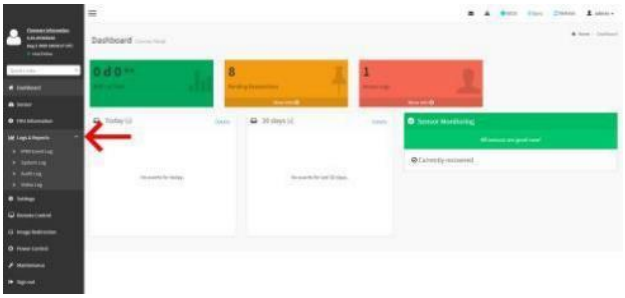
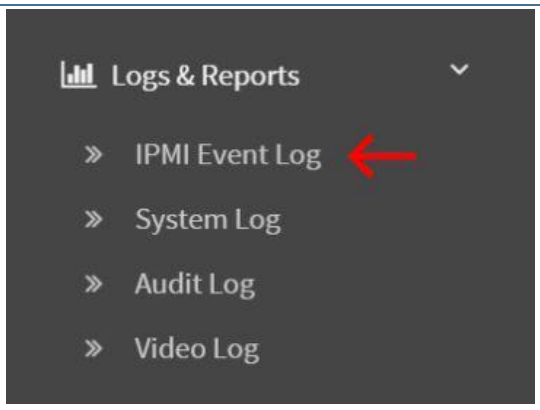
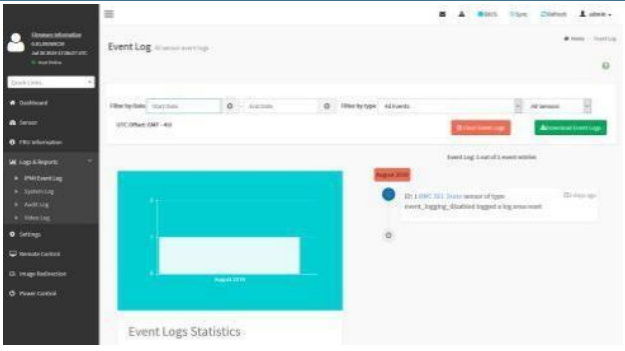
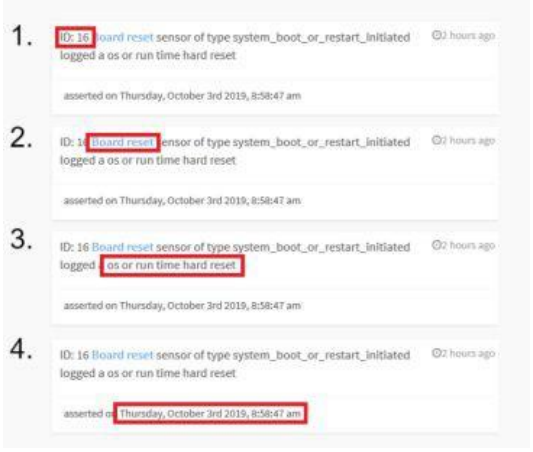
- En utilisant l'interface utilisateur Web du BMC
- En utilisant IPMI
- En utilisant Redfish

12.4.1.1. Accéder au SEL en utilisant l'interface utilisateur Web du BMC

12.4.1.1.1. Accéder au journal des événements système

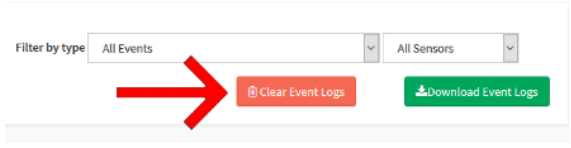
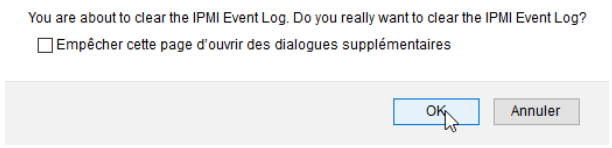
Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

Étape_1	Accéder à l'interface utilisateur Web du BMC du serveur.

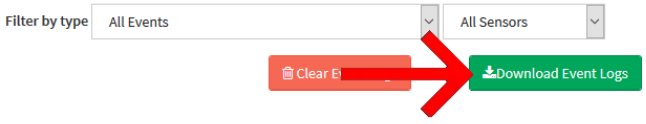
Étape_2	Sélectionner **Logs & Reports** dans le menu de gauche.	
Étape_3	Sélectionner **IPMI Event Log** dans le menu déroulant.	
Étape_4	Le journal des événements système s'affiche.	
Étape_5	Cliquer sur un événement et recueillir les informations suivantes : 1. ID de l'événement 2. Capteur associé 3. Description 4. Estampille temporelle d'assertion	

NOTE : Selon l'événement, il se peut qu'il n'y ait pas d'attribut de capteur associé. Toutefois, si cet attribut est présent, voir Interprétation des données des capteurs pour plus de détails.

12.4.1.1.2. Vider le journal des événements système

Étape_1	Dans le menu **Event Log**, sélectionner **Clear Event Logs**.	
Étape_2	Confirmer la commande en cliquant sur **OK**.	

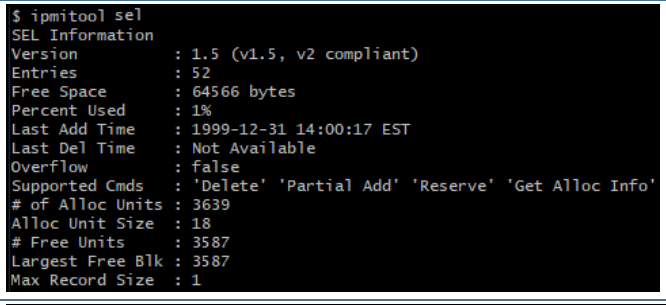
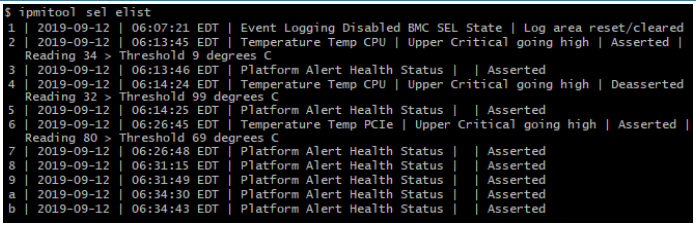
12.4.1.1.3. Télécharger le journal des événements système

Étape_1	Dans le menu **Event Log**, sélectionner Download **Event Logs**.	

12.4.1.2. Accéder au SEL en utilisant IPMI via KCS

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL (Accéder au BMC en utilisant IPMI sur LAN (IOL)). Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

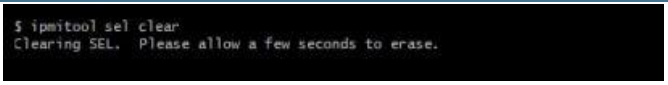
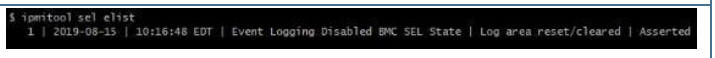
12.4.1.2.1. Accéder au journal des événements système

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, accéder aux informations du journal des événements système. InviteSE_ServeurLocal:~$ **ipmitool sel**	
Étape_2	Accéder au journal des événements système. InviteSE_ServeurLocal:~$ **ipmitool sel elist**	

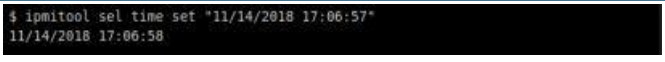
Étape_3	Recueillir les informations suivantes pour l'événement spécifié : • ID de l'événement – 1re colonne • Temps d'assertion – 2e et 3e colonne • Capteur associé – 4e colonne (optionnel) • Description – 5e colonne

NOTE : Selon l'événement, il se peut qu'il n'y ait pas d'attribut de capteur associé. Toutefois, si cet attribut est présent, voir Interprétation des données des capteurs pour plus de détails.

12.4.1.2.2. Vider le journal des événements système

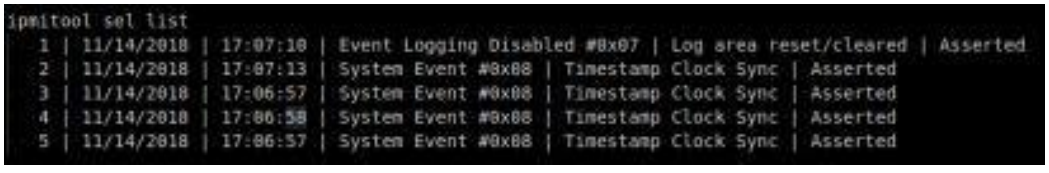
Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, vider le journal des événements système. InviteSE_ServeurLocal:~# **ipmitool sel clear**	
Étape_2	Vérifier que le journal des événements système a été correctement vidé. InviteSE_ServeurLocal:~# **ipmitool sel elist**	

12.4.1.2.3. Définir la date et l'heure du journal des événements système

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, définir la date et l'heure du journal des événements système. InviteSE_ServeurLocal:~# **ipmitool sel time set "[MM/DD/YYYY HH:MM:SS]"**	
Étape_2	Vérifier que la date et l'heure du SEL ont été correctement réglées. InviteSE_ServeurLocal:~# **ipmitool sel time get**	

12.4.1.2.3.1. Limite connue

Lorsque la date et l'heure du journal des événements système sont définis avec ipmitool, plusieurs entrées répétées d'événements système seront présentes dans la liste du SEL.



Ce comportement a été observé avec la dernière version d'ipmitool (1.8.18) publiée à ce jour. Cependant, la plus récente version non publiée corrige le problème. Pour obtenir la plus récente version non publiée :

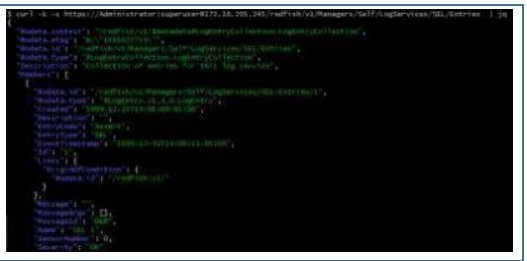
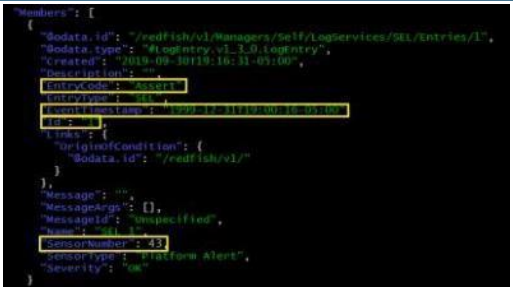
Étape_1	Envoyer les commandes suivantes : **git clone https://github.com/ipmitool/ipmitool.git cd ipmitool** **./bootstrap && ./configure && make && sudo make install**

Étape_2	Après l'installation d'ipmitool, ajouter le paramètre (flag) « -N 5 » pour utiliser la commande ipmitool sel set time. Ce paramètre définit le délai d'attente de la commande afin d'éviter que de multiples erreurs ne soient enregistrées. **ipmitool -H [IP_GESTION_ BMC] -U admin -P admin -I lanplus sel time set "11/14/2018 17:06:57" -N 5**

12.4.1.3. Accéder au SEL en utilisant Redfish

12.4.1.3.1. Accéder au journal des événements système

Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, ouvrir une invite de commande et accéder au journal des événements système. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/Managers/Self/LogServices/SEL/Entries | jq**	
Étape_2	Recueillir les informations suivantes pour l'événement spécifié : • Description ou attribut EntryCode • Estampille temporelle d'assertion ou attribut EventTimestamp • ID de l'événement ou attribut Id • Capteur associé ou attribut SensorNumber (optionnel)	

NOTE : Selon l'événement, il se peut qu'il n'y ait pas d'attribut de capteur associé. Toutefois, si cet attribut est présent, voir Interprétation des données des capteurs pour plus de détails.

12.4.1.3.2. Vider le journal des événements système

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, ouvrir une invite de commande et vider au journal des événements système. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/Managers/Self/LogServices/SEL/Actions/LogService.ClearLog -X POST -d'{"ClearType":"ClearAll"}' -H "Content-Type: application/json" | jq**
	`$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Managers/Self/LogServices/SEL/Actions/LogService.ClearLog -X POST -d'{"ClearType":"ClearAll"}' -H "Content-Type: application/json" | jq`
Étape_2	Vérifier que le journal des événements système a été correctement vidé. InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/Managers/Self/LogServices/SEL/Entries | jq**

```
$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Managers/Self/LogServices/SEL/Entries | jq
{
  "@odata.context": "/redfish/v1/$metadata#LogEntryCollection.LogEntryCollection",
  "@odata.etag": "W/\"1565101395\"",
  "@odata.id": "/redfish/v1/Managers/Self/LogServices/SEL/Entries",
  "@odata.type": "#LogEntryCollection.LogEntryCollection",
  "Description": "Collection of entries for this log service",
  "Members": [],
  "Members@odata.count": 0,
  "Name": "Log Service Entries Collection"
}
```

12.4.2. Remplacement des composants

Pour remplacer un composant sur une plateforme CG2400, voir Installation et assemblage des composants.

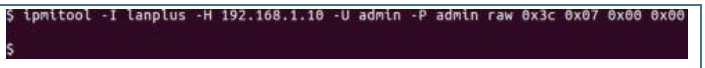
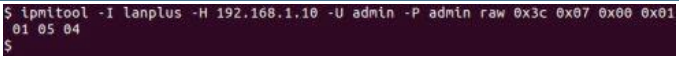
12.4.3. Sauvegarde et récupération du BIOS

Cette section décrit comment faire une sauvegarde du BIOS et une récupération à partir de la sauvegarde créée.

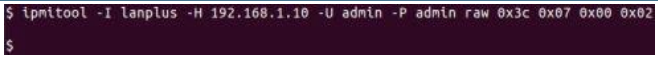
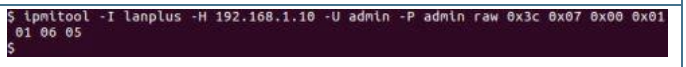
Les procédures suivantes sont exécutées en utilisant IPMI sur LAN. Voir Accéder au BMC en utilisant IPMI sur LAN (IOL).

NOTE : Lorsque des commandes brutes sont envoyées, la charge utile est désactivée. Ceci est fait afin d'empêcher le BMC d'accéder à la mémoire flash du BIOS. Une fois la procédure terminée, la plateforme demeure éteinte.

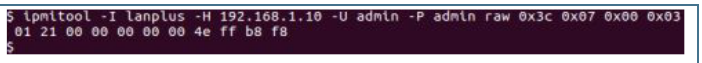
12.4.3.1. Sauvegarder le BIOS

Étape_1	Sauvegarder le BIOS (cette étape sauvegarde le BIOS et la configuration). InviteSE_ServeurDistant**:~# ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] raw 0x3c 0x07 0x00 0x00** Code d'exécution : • 0x00 : Le processus de récupération a démarré avec succès • 0xd6 : Le processus de récupération ne peut pas être lancé	
Étape_2	Vérifier l'état de la sauvegarde du BIOS. InviteSE_ServeurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] raw 0x3c 0x07 0x00 0x01** Le code d'exécution est toujours 0x00. [OCTET0] État : • 0x00 = Succès/inactif • 0x01 = En cours • 0x02 = Échec [OCTET1] Étape actuelle (voir Description des étapes de création et de rétablissement) [OCTET2] Progrès (en pourcentage) Dans l'image, l'état de la création de la copie instantanée est **En cours**, l'étape actuelle est **Snapshot MTD Flash erase** et le progrès est de 4 %.	

12.4.3.2. Rétablir le BIOS

Étape_1	Rétablir le BIOS (cette étape rétablit le BIOS et la configuration). InviteSE_ServeurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] raw 0x3c 0x07 0x00 0x02** Code d'exécution : • 0x00 : Le processus de récupération a démarré avec succès • 0xd6 : Le processus de récupération ne peut pas être lancé	
Étape_2	Vérifier l'état du rétablissement. InviteSE_ServeurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] raw 0x3c 0x07 0x00 0x01** Le code d'exécution est toujours 0x00. [OCTET0] État : • 0x00 = Succès/inactif • 0x01 = En cours • 0x02 = Échec [OCTET1] Étape actuelle (voir Description des étapes de création et de rétablissement) [OCTET2] Progrès (en pourcentage) Dans l'image, l'état du rétablissement est **En cours**, l'étape actuelle est **Snapshot MTD Flash write** et le progrès est de 5 %.	

12.4.3.3. Information sur la dernière copie instantanée du BIOS

Étape_1	Récupérer les informations BIOS sauvegardées. InviteSE_ServeurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] raw 0x3c 0x07 0x00 0x03** Code d'exécution : • 0x00 : La copie instantanée est valide • 0xd6 : La copie instantanée est invalide [OCTET0-OCTET5] Version : • [1B] Majeure • [1B] Mineure • [4B] Aux [OCTET6] État [OCTET7-OCTET10] Estampille temporelle Unix Dans l'image, la version est **1.33.00000000**, l'état est **0x00** et l'estampille temporelle est **1325381880**.	

12.4.3.4. Description des étapes de création et de rétablissement

Description de l'étape	Valeur de l'étape (OCTET1)	Description de l'étape
Snapshot validation	0x00	Vérification à savoir si la copie instantanée sauvegardée est valide pour le rétablissement.
Check BIOS end of POST	0x01	Vérification à savoir si le BIOS est valide et démarré avant de créer une copie instantanée.
MTD partition detect	0x02	Vérification à savoir si le périphérique flash et la partition sont détectés.
Server Power Off	0x03	Mise hors tension du serveur.
Force Intel ME Recovery mode	0x04	Force Intel ME à passer en mode rétablissement.
Snapshot MTD Flash erase	0x05	Effacement de la copie instantanée sur flash. Progression de l'effacement en pourcentage (%) disponible dans [OCTET2] de la commande get status (0x01).
Snapshot MTD Flash write	0x06	Écriture de la copie instantanée sur flash. Progression de l'écriture en pourcentage (%) disponible dans [OCTET2] de la commande get status (0x01).
Snapshot MTD Flash verify	0x07	Vérification de la copie instantanée sur flash. Progression de la vérification en pourcentage (%) disponible dans [OCTET2] de la commande get status (0x01).
Reset Intel ME to Normal mode	0x08	Réinitialiser Intel ME pour revenir au mode normal.

12.4.4. Mise à niveau

12.4.4.1. Considérations générales

Utiliser les plus récents micrologiciels permet d'optimiser les fonctionnalités du CG2400. Les procédures pour télécharger le paquet de micrologiciels et mettre la plateforme à niveau sont décrites ci-dessous.

12.4.4.2. Télécharger les plus récentes versions des micrologiciels

Visiter le site Web de Kontron pour télécharger les plus récentes versions des micrologiciels disponibles pour le CG2400.

Ensuite, procéder à la mise à niveau souhaitée :

- Mettre à niveau le BMC et le FPGA en utilisant ipmitool – recommandé
- Mettre à niveau le BIOS et le LAN 10GbE

12.4.4.3. Mettre à niveau le BMC et le FPGA en utilisant ipmitool

La procédure suivante permet de mettre à niveau le BMC et le FPGA simultanément.

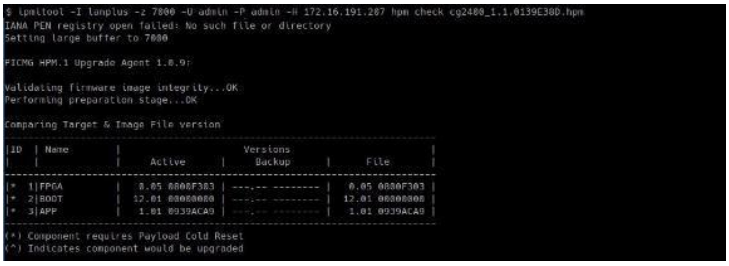
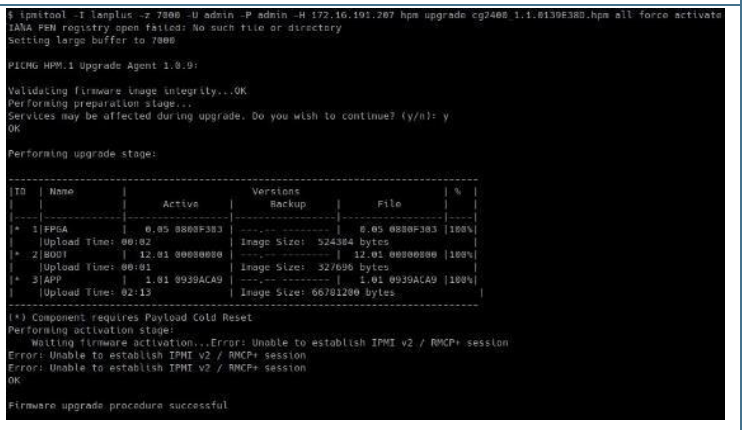
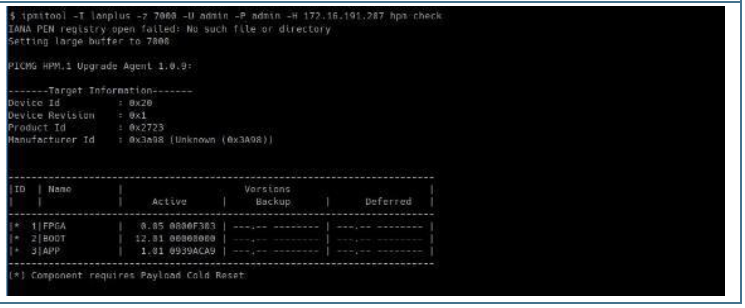
12.4.4.3.1. Préalable

1	Une version de la communauté d'ipmitool est installée sur un ordinateur distant pour permettre la surveillance à distance – il est recommandé d'utiliser la version 1.8.18 d'ipmitool. NOTE : Le processus de mise à niveau peut être effectué avec n'importe quelle version récente d'ipmitool.

NOTE : Le processus de mise à niveau peut être effectué avec n'importe quelle version récente d'ipmitool.

12.4.4.3.2. Procédure

Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, saisir la commande souhaitée. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] chassis power off** **NOTE** : La mise à niveau peut être effectuée sans éteindre la plateforme et sans vérifier l'état de l'alimentation; Cependant, lorsque la commande all activate est exécutée, le système complet redémarre.	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power off` `Chassis Power Control: Down/Off`
Étape_2	Confirmer que le serveur est éteint. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] chassis power status**	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status` `Chassis Power is off`

Étape_3	Vérifier que la version de la mise à niveau est adéquate. InviteSE_OrdinateurDistant:~# **ipmitool -z 7000 -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] hpm check [PAQUET_HPM]**	
Étape_4	Procéder à la mise à niveau des micrologiciels. InviteSE_OrdinateurDistant:~# **ipmitool -z 7000 -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] hpm upgrade [PAQUET_HPM] all activate** **NOTE** : Attendre la fin de la mise à niveau avant d'effectuer toute action sur la plateforme. Si la mise à niveau est interrompue, les données risquent d'être corrompues.	
Étape_5	Vérifier que les différents composants ont été correctement mis à niveau. InviteSE_OrdinateurDistant:~# **ipmitool -z 7000 -I lanplus -H [IP_GESTION_BMC] - U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] hpm check**	

12.4.4.4. Mettre à niveau le BIOS et le LAN 10GbE

NOTICE

- NE PAS éteindre ou redémarrer les CPU lorsque le système est en train de lire le BIOS ou de le mettre à niveau.
- Pour éviter toute erreur lors de la mise à jour de la mémoire flash, NE PAS retirer le disque dur, le périphérique USB ou tout autre périphérique de manière inappropriée. Une manipulation incorrecte entraînera un crash du BIOS et pourrait empêcher le démarrage de la carte.
- Le démarrage sécurisé doit être désactivé pour effectuer les mises à niveau.
- Une fois tous les scripts exécutés, un cycle d'alimentation complet est effectué. Ce cycle affecte également le contrôleur de gestion.

Section pertinente :

Accéder au système d'exploitation d'un serveur

12.4.4.4.1. Méthode Linux

12.4.4.4.1.1. Transférer et décompresser le paquet

Étape_1	Transférer le plus récent fichier compressé (zip ou tar.gz) du paquet de mise à niveau vers un Linux installé sur un périphérique de stockage (M.2, disque dur, disque SSD) du CG2400.
Étape_2	À partir d'une invite de commande du système d'exploitation, décompresser le fichier .zip. **NOTE** : Pour décompresser un fichier .zip, il pourrait être requis d'installer un paquet Linux supplémentaire. **tar xzvf [FICHIER PAQUET_MISE_A_NIVEAU.tar.gz]** OU **unzip [FICHIER PAQUET_MISE_A_NIVEAU.zip]**
Étape_3	Sélectionner le répertoire approprié. **cd bios-bundle-[VERSION]**

Sélectionner la mise à niveau à effectuer :

- Mettre à niveau le BIOS
- Mettre à niveau le LAN 10GbE

12.4.4.4.1.2. Mettre à niveau le BIOS

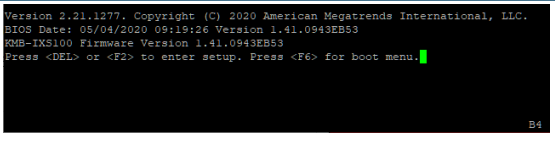
Étape_1	À partir d'une invite de commande du système d'exploitation, lancer le processus de mise à niveau. **sudo bash ./bios-update.sh**
Étape_2	Suivre les instructions à l'écran jusqu'à ce que le processus de mise à niveau soit terminé. Noter que le système redémarrera plusieurs fois.

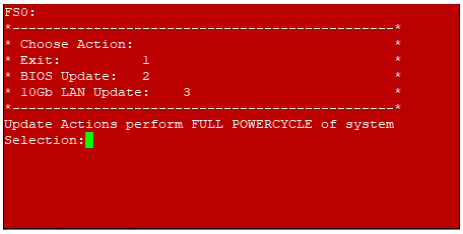
12.4.4.4.1.3. Mettre à niveau le LAN 10GbE

Étape_1	À partir d'une invite de commande du système d'exploitation, lancer le processus de mise à niveau. **sudo bash ./lan-update.sh**
Étape_2	Suivre les instructions à l'écran jusqu'à ce que le processus de mise à niveau soit terminé.

12.4.4.4.2. Méthode avec une clé USB

Cette méthode nécessite un accès physique au système.

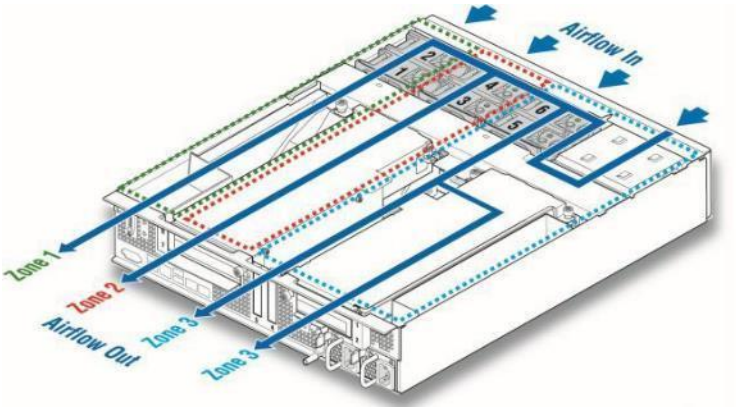
Étape_1	Décompresser et copier les fichiers à la racine d'une clé USB formatée en FAT32.	
Étape_2	Insérer la clé USB dans le port USB avant ou arrière du CG2400.	
Étape_3	Réinitialiser le système. Voir Gestion de l'alimentation de la plateforme pour les méthodes de réinitialisation.	
Étape_4	Lorsque le système a redémarré, appuyer sur F6 pour activer le menu de démarrage et sélectionner la clé USB. **NOTE** : Il est également possible d'appuyer sur F2 ou Suppr [DEL], d'entrer dans le menu BIOS, d'aller dans l'onglet **Save & Exit** et de sélectionner la clé USB sous Boot Override. Ne pas appuyer sur la touche Échap [ESC]. Cela vous amènerait dans le shell EFI, ce qui nécessiterait de redémarrer le CG2400 pour démarrer à partir de la clé USB.	

Étape_5	Un menu s'affiche. Sélectionner l'action à effectuer : • Exit (appuyer sur 1) • BIOS Update (appuyer sur 2) • Mettre à jour le LAN 10Gb (appuyer sur 3) **NOTE** : Le système effectuera un cycle d'alimentation complet après la mise à niveau du BIOS ou du LAN 10Gb.	

12.5. Refroidissement et gestion thermique de la plateforme

12.5.1. Sous-système de refroidissement de la plateforme

Le CG2400 est équipé de trois jeux de ventilateurs jumelés qui assurent un refroidissement approprié des composants les plus simples aux plus complexes. Tous les composants du système, à l'exception de la carte de distribution électrique et des blocs d'alimentation, sont refroidis par les six ventilateurs montés près de l'avant du châssis, derrière la carte du panneau avant, comme montré dans la figure ci-dessous.



La plateforme CG2400 dispose de six ventilateurs de 80 mm x 38 mm, configurés en trois paires redondantes. Il y a trois zones de refroidissement délimitées par les lignes pointillées colorées dans la figure ci-dessus.

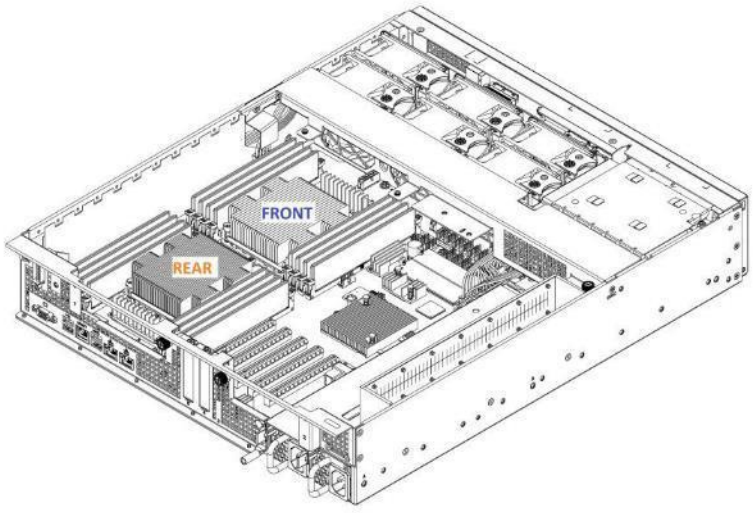
- La zone 1 (lignes pointillées vertes) contient les ventilateurs 1 et 2, qui refroidissent les deux CPU, la moitié des modules DIMM et tous les autres composants de cette zone. L'air circule à travers le panneau frontal jusqu'à l'arrière du châssis (flèche de la zone 1).
- La zone 2 (lignes pointillées rouges) contient les ventilateurs 3 et 4, qui refroidissent l'autre moitié des modules DIMM, la cage d'extension PCIe de droite et tous les autres composants de cette zone. L'air circule à travers le panneau frontal jusqu'à l'arrière du châssis (flèche de la zone 2).
- La zone 3 (lignes pointillées bleues) contient les ventilateurs 5 et 6, qui refroidissent les six disques durs, les deux adaptateurs PCI LP des emplacements 3 et 4 de la carte, la cage d'extension PCIe de gauche et tous les autres composants de cette zone. L'air circule du panneau frontal par-dessus la cage des disques vers les ventilateurs, puis emprunte deux voies pour cette zone : retour direct vers l'arrière du châssis (flèche gauche de la zone 3) et retour par-dessus les blocs d'alimentation vers l'arrière du châssis (flèche droite de la zone 3).
- Les ventilateurs internes des blocs d'alimentation ainsi que les ventilateurs 5 et 6 du système refroidissent la carte de distribution électrique (PDB) et les blocs d'alimentation.

La cage d'extension PCIe de droite (côté droit si on fait face à la plateforme) se trouve au-dessus du conduit d'air des processeurs et de la mémoire dans la zone 2. Les déflecteurs verticaux sur la surface supérieure du conduit d'air des processeurs et de la mémoire combinés à la cage d'extension PCIe et à son boîtier en tôle forment un conduit d'air pour les cartes d'expansion PCIe installées dans la cage d'extension PCIe de droite. La cage d'extension PCIe de gauche (côté gauche si on fait face à la plateforme) se trouve au-dessus de la partie la plus à gauche de la carte mère et du bloc d'alimentation 2 dans la zone 3. La cage d'extension PCIe de gauche, son boîtier en tôle et le déflecteur d'air installé à gauche de la cage d'extension PCIe forment un conduit d'air pour les cartes d'expansion PCIe installées dans la cage d'extension PCIe de gauche.

12.5.1.1. Dissipateurs thermiques des CPU

Les deux dissipateurs de chaleur des CPU sont inclus dans le système de base de la plateforme (numéro de pièce CG2400-00). Ils sont emballés dans des boîtes individuelles, avec le châssis, dans la boîte de la plateforme. Les dissipateurs ne sont pas identiques et doivent être installés dans la bonne configuration pour obtenir un comportement thermique optimal de la plateforme.

Chaque dissipateur est muni d'une étiquette indiquant sa position : « AVANT » (Front) ou « ARRIÈRE » (Rear). Voir la figure ci-dessous pour le bon positionnement des dissipateurs.



12.5.1.2. Circulation de l'air dans les blocs d'alimentation CA et CC

Chaque bloc d'alimentation est équipé d'un ventilateur de 40 mm pour l'autorefroidissement. Les ventilateurs assurent un débit d'air d'au moins 10 pi^3/min à travers le bloc d'alimentation lorsqu'il est installé dans le système et qu'il fonctionne à sa vitesse maximale. L'air de refroidissement pénètre dans le bloc d'alimentation par le côté du PDB. La vitesse variable du ventilateur est basée sur la charge de sortie et la température ambiante. En mode veille, les ventilateurs doivent fonctionner au régime minimum.

12.5.2. Gestion thermique de la plateforme

La gestion thermique de la plateforme est assurée par le BMC intégré à la carte mère.

Le BMC utilise les informations collectées par les capteurs de température embarqués pour ajuster la vitesse des ventilateurs et réguler la température de la plateforme selon un algorithme PID.

Les capteurs de température sont agrégés en tant que valeur d'entrée pour le régulateur PID de la température du système, qui fournit une commande de vitesse pour les ventilateurs.

NOTE : Pour une solution de gestion thermique sur mesure, il est possible d'inclure jusqu'à deux sondes supplémentaires optionnelles dans l'algorithme de refroidissement afin de surveiller des zones déterminées par le client. Voir Sonde thermique optionnelle pour plus de détails.

12.5.2.1. Capteurs de température agrégés du CG2400

ID (hex)	Capteur (sensor)	Description	Type de capteur (sensor type)	Code de type d'événement/de lecture (event/reading type code)
21h	Front Panel Temp	Température du panneau avant	Temperature (0x01)	0x01 (Threshold Based)
C7h	P1 Temp	Température du processeur 1	Temperature (0x01)	0x01 (Threshold Based)
D2h	P2 Temp	Température du processeur 2	Temperature (0x01)	0x01 (Threshold Based)
20h	P1 TJMAX	Température maximale/point de déclenchement thermique (throttling) pour la température du processeur 1.	Temperature (0x01)	0x01 (Threshold Based)
0Fh	P2 TJMAX	Température maximale/point de déclenchement thermique (throttling) pour la température du processeur 2.	Temperature (0x01)	0x01 (Threshold Based)
B5h	CPU Zone Temp	Température de la zone CPU	Temperature (0x01)	0x01 (Threshold Based)
1Eh	PCH Temp	Température du PCH	Temperature (0x01)	0x01 (Threshold Based)
BAh	BMC Temp	Température du BMC	Temperature (0x01)	0x01 (Threshold Based)
B7h	PCIe A Temp	Température de la carte PCIe A (câble de la sonde thermique optionnelle*)	Temperature (0x01)	0x01 (Threshold Based)
B9h	PCIe B Temp	Température de la carte PCIe B (câble de la sonde thermique optionnelle*)	Temperature (0x01)	0x01 (Threshold Based)
BBh	X557 LAN1 Temp	Température du X557 LAN 1	Temperature (0x01)	0x01 (Threshold Based)
BCh	X557 LAN2 Temp	Température du X557 LAN 1	Temperature (0x01)	0x01 (Threshold Based)
B4h	M.2 Temp	Température de la zone M.2	Temperature (0x01)	0x01 (Threshold Based)
B6h	Battery Temp	Température de la batterie	Temperature (0x01)	0x01 (Threshold Based)
C8h	P1 DIMMA1 Temp	Température du canal DIMM du processeur 1	Temperature (0x01)	0x01 (Threshold Based)
C9h	P1 DIMMA2 Temp	Température du canal DIMM du processeur 1	Temperature (0x01)	0x01 (Threshold Based)
CAh	P1 DIMMB1 Temp	Température du canal DIMM du processeur 1	Temperature (0x01)	0x01 (Threshold Based)
CBh	P1 DIMMC1 Temp	Température du canal DIMM du processeur 1	Temperature (0x01)	0x01 (Threshold Based)
CCh	P1 DIMMD1 Temp	Température du canal DIMM du processeur 1	Temperature (0x01)	0x01 (Threshold Based)
CDh	P1 DIMMD2 Temp	Température du canal DIMM du processeur 1	Temperature (0x01)	0x01 (Threshold Based)
CEh	P1 DIMME1 Temp	Température du canal DIMM du processeur 1	Temperature (0x01)	0x01 (Threshold Based)
CFh	P1 DIMMF1 Temp	Température du canal DIMM du processeur 1	Temperature (0x01)	0x01 (Threshold Based)
D3h	P2 DIMMA1 Temp	Température du canal DIMM du processeur 2	Temperature (0x01)	0x01 (Threshold Based)

ID (hex)	Capteur (sensor)	Description	Type de capteur (sensor type)	Code de type d'événement/de lecture (event/reading type code)
D4h	P2 DIMMA2 Temp	Température du canal DIMM du processeur 2	Temperature (0x01)	0x01 (Threshold Based)
D5h	P2 DIMMB1 Temp	Température du canal DIMM du processeur 2	Temperature (0x01)	0x01 (Threshold Based)
D6h	P2 DIMMC1 Temp	Température du canal DIMM du processeur 2	Temperature (0x01)	0x01 (Threshold Based)
D7h	P2 DIMMD1 Temp	Température du canal DIMM du processeur 2	Temperature (0x01)	0x01 (Threshold Based)
D8h	P2 DIMMD2 Temp	Température du canal DIMM du processeur 2	Temperature (0x01)	0x01 (Threshold Based)
D9h	P2 DIMME1 Temp	Température du canal DIMM du processeur 2	Temperature (0x01)	0x01 (Threshold Based)
DAh	P2 DIMMF1 Temp	Température du canal DIMM du processeur 2	Temperature (0x01)	0x01 (Threshold Based)
34h	Fan Failure	État de défaillance actuel des ventilateurs	Fan (0x04)	0x4
2Dh	Fan1 Speed	Vitesse actuelle du ventilateur 1 (tr/min)	Fan (0x04)	0x01 (Threshold Based)
2Eh	Fan2 Speed	Vitesse actuelle du ventilateur 2 (tr/min)	Fan (0x04)	0x01 (Threshold Based)
2Fh	Fan3 Speed	Vitesse actuelle du ventilateur 3 (tr/min)	Fan (0x04)	0x01 (Threshold Based)
30h	Fan4 Speed	Vitesse actuelle du ventilateur 4 (tr/min)	Fan (0x04)	0x01 (Threshold Based)
31h	Fan5 Speed	Vitesse actuelle du ventilateur 5 (tr/min)	Fan (0x04)	0x01 (Threshold Based)
32h	Fan6 Speed	Vitesse actuelle du ventilateur 6 (tr/min)	Fan (0x04)	0x01 (Threshold Based)
61h	Fan1 Present	État de présence du ventilateur 1	Fan (0x04)	0x8
62h	Fan2 Present	État de présence du ventilateur 2	Fan (0x04)	0x8
63h	Fan3 Present	État de présence du ventilateur 3	Fan (0x04)	0x8
64h	Fan4 Present	État de présence du ventilateur 4	Fan (0x04)	0x8
65h	Fan5 Present	État de présence du ventilateur 5	Fan (0x04)	0x8
66h	Fan6 Present	État de présence du ventilateur 6	Fan (0x04)	0x8
18h	PS1 Temp	Température du bloc d'alimentation 1	Temperature (0x01)	0x01 (Threshold Based)
19h	PS2 Temp	Température du bloc d'alimentation 2	Temperature (0x01)	0x01 (Threshold Based)
DBh	P1 DTS Thrm Mrgn	Marge thermique avant un arrêt du processeur 1 causé par la température	Temperature (0x01)	0x01 (Threshold Based)
DCh	P2 DTS Thrm Mrgn	Marge thermique avant un arrêt du processeur 1 causé par la température	Temperature (0x01)	0x01 (Threshold Based)

12.5.2.2. Protection thermique des blocs d'alimentation CA et CC

Le sous-système des blocs d'alimentation est équipé d'une protection contre la surchauffe (PCS) causée par la perte de refroidissement par les ventilateurs ou une température ambiante élevée. En cas de surchauffe, la sortie +12 V du bloc d'alimentation s'éteint. Lorsque la température du bloc d'alimentation baisse dans les limites spécifiées, le bloc d'alimentation rétablit automatiquement l'alimentation. L'alimentation de veille demeure active pendant cette transition. Le circuit de PCS utilise une hystérésis intégrée qui empêche l'alimentation d'osciller en raison des conditions de récupération de la température. Le niveau de déclenchement de la PCS est réglé pour une hystérésis d'un minimum de 4 °C de la température ambiante.

12.5.3. Gestion des capteurs propres aux clients

12.5.3.1. Sonde thermique

12.5.3.1.1. Description

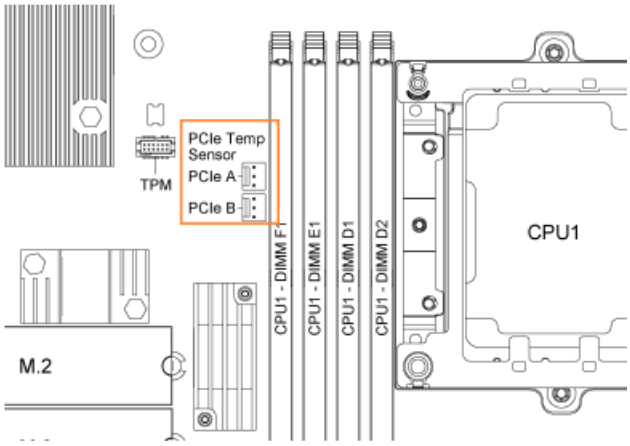
La plateforme CG2400 offre la possibilité d'ajouter jusqu'à deux points de mesure de température spécifiques en connectant des sondes thermiques optionnelles à la carte mère de la plateforme.

Les sondes doivent être installées ou fixées à proximité des points de mesure de température d'intérêt. Par exemple, un point de mesure peut être une puce particulière ou une zone chaude connue sur une carte PCIe.

Ces sondes sont incluses dans la Liste des capteurs de température de l'algorithme de refroidissement des ventilateurs et influencent la vitesse des ventilateurs de la plateforme. Le numéro de pièce d'une sonde thermique CG2400 est le 1066-0224.

12.5.3.1.2. Emplacement

Les sondes thermiques, nommées PCIe A Temp et PCIe B Temp, sont incluses dans la Liste des capteurs IPMI. Voir le diagramme ci-dessous pour connaître l'emplacement de leurs connecteurs sur la carte mère.



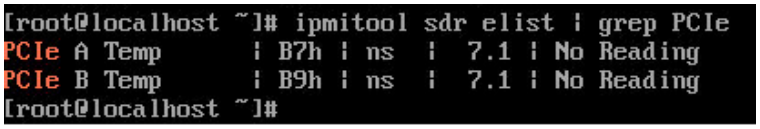
12.5.3.1.3. Installer une sonde

Pour chaque sonde :

Étape_1	Brancher le connecteur à 3 broches de la sonde sur la carte mère. **NOTE** : Le connecteur est claveté pour assurer une bonne connexion de la sonde thermique à la carte mère.
Étape_2	Fixer le transistor/l'extrémité de la sonde thermique sur l'élément à surveiller (ex. la puce). NOTE : Il est possible d'utiliser du ruban Kapton, de la colle chaude, un composé de caoutchouc de silicone résistant aux variations de température ou tout autre liant approprié.
Étape_3	Passer le câble dans la plateforme en veillant à ce qu'il n'interfère pas avec d'autres composants.

12.5.3.1.4. Lire la sonde

Les capteurs PCIe A Temp et PCIe B Temp sont toujours affichés dans la Liste des capteurs IPMI. Ils renvoient la valeur « No Reading » si aucune sonde thermique n'est installée.



Les sondes thermiques sont détectées au démarrage du BMC. Il faut donc éteindre la plateforme et débrancher les cordons d'alimentation avant d'installer les sondes thermiques.

12.5.3.1.5. Inclure les sondes thermiques dans l'algorithme de refroidissement de la plateforme

La gestion thermique de la plateforme est assurée par le BMC intégré à la carte mère. Le BMC utilise les informations collectées par les capteurs de température embarqués pour ajuster la vitesse des ventilateurs et réguler la température de la plateforme selon un algorithme PID. Les capteurs de température sont agrégés pour fournir une valeur d'entrée pour le régulateur PID de la température du système, qui fournit une commande de vitesse pour les ventilateurs.

Les sondes thermiques optionnelles, lorsqu'elles sont installées, font partie du processus d'agrégation de ces capteurs de température.

Les seuils des capteurs PCIe A Temp et PCIe B Temp doivent être ajustés en fonction de la température souhaitée pour le composant surveillé. L'algorithme de refroidissement de la plateforme régule la vitesse des ventilateurs afin de maintenir tous les composants juste en dessous de leur seuil non critique supérieur.

12.5.3.1.5.1. Directives pour définir les seuils des sondes thermiques

- Le seuil non critique supérieur doit correspondre à la température du composant à une charge de 100 %, à une température ambiante typique (ex. 20 °C).
- Le seuil critique supérieur doit correspondre à la température du composant à une charge de 100 %, à une température ambiante correspondant à la limite supérieure (ex. 35 °C).

Voir Configurer les capteurs pour plus de détails sur les méthodes de modification des seuils des capteurs.

12.5.4. Outrepasser la vitesse minimale des ventilateurs

Le CG2400 offre la possibilité d'outrepasser la vitesse minimale des ventilateurs (disponible dans la version SUP04 ou plus récente).

Cette fonction peut être utile dans des situations particulières pour éviter la surchauffe de pièces/éléments non gérés par la gestion thermique du CG2400. Par exemple, les cartes PCIe qui n'ont pas de capteurs thermiques connectés au BMC.

Une commande OEM IPMI peut être envoyée pour outrepasser la valeur de vitesse minimale utilisée par le gestionnaire des ventilateurs du BMC. La valeur peut être réglée de deux façons :

1. Via le menu BIOS, dans l'onglet Server Mgmt : La valeur actuelle de la vitesse minimale des ventilateurs est affichée et il est possible d'en définir une nouvelle. La nouvelle valeur est sauvegardée par le BMC lorsque la commande Save & Exit est exécutée dans le menu de configuration du BIOS.

2. Via une commande ipmitool, comme indiqué ci-dessous :

```
$ # Get current minimal speed (returns 0x0A = 10%)
$ ipmitool -H 192.168.1.10 -I lanplus -U admin -P admin raw 0x3c  0x0A 0x00  0x00  0x01
0A
$
$ # Set new minimal speed of 50% (0x32).
$ ipmitool -H 192.168.1.10 -I lanplus -U admin -P admin raw 0x3c  0x0A 0x00  0x01  0x32
```

Cette valeur de vitesse minimale des ventilateurs est enregistrée dans une mémoire non volatile par le BMC, ce qui signifie que lors des redémarrages du BMC et/ou des mises à niveau des micrologiciels, cette valeur est conservée.

13/ Dépannage

13.1. Collecte des diagnostics

Lorsque l'équipe du soutien est contactée, les données suivantes sont nécessaires pour établir un bon diagnostic de l'état de la carte :

- Données FRU
- Version du micrologiciel
- Journal des événements système

La collecte préalable de toutes ces données peut accélérer le processus.

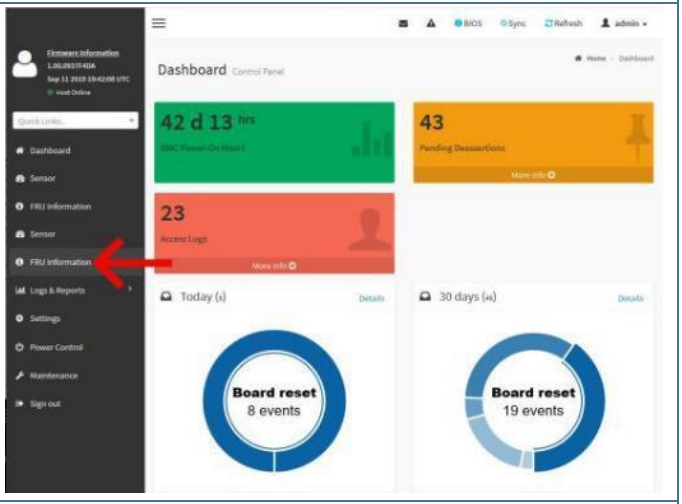
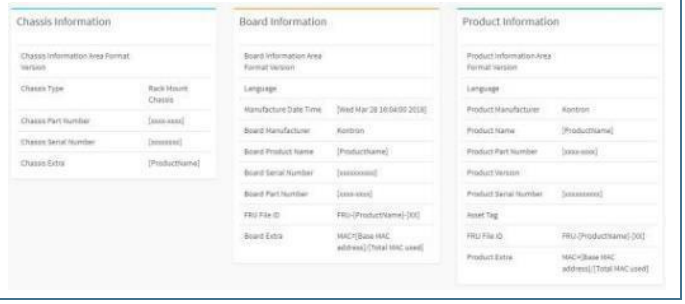
13.1.1. Recueillir les données FRU

Les données FRU peuvent être recueillies :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant IPMI

13.1.1.1. Recueillir les données FRU en utilisant l'interface utilisateur Web du BMC

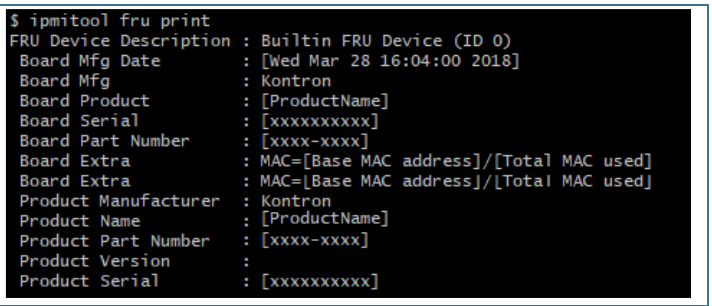
Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

Étape_1	Accéder à l'interface utilisateur Web du BMC du serveur.	
Étape_2	Sélectionner **FRU Information** dans le menu de gauche.	
Étape_3	Les données FRU s'affichent.	

13.1.1.2. Recueillir les données FRU en utilisant IPMI

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL (Accéder au BMC en utilisant IPMI sur LAN (IOL)).

Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, accéder aux données FRU. InviteSE_ServeurLocal:~$ **ipmitool fru print**	

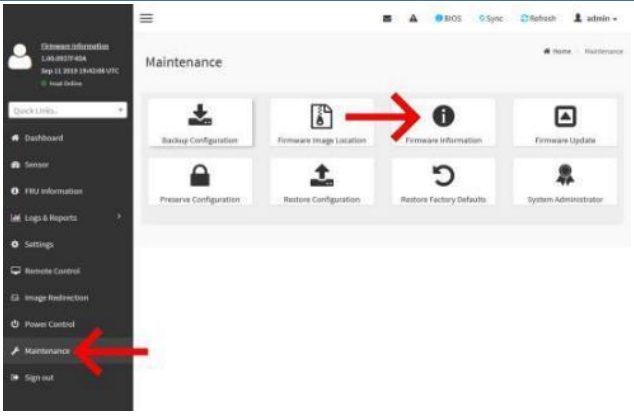
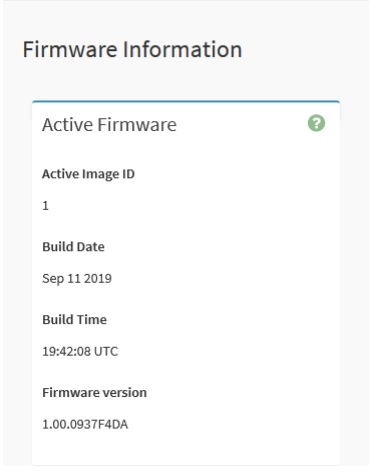
13.1.2. Recueillir la version du micrologiciel

La version du micrologiciel peut être recueillie :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant IPMI

13.1.2.1. Recueillir la version du micrologiciel en utilisant l'interface utilisateur Web du BMC

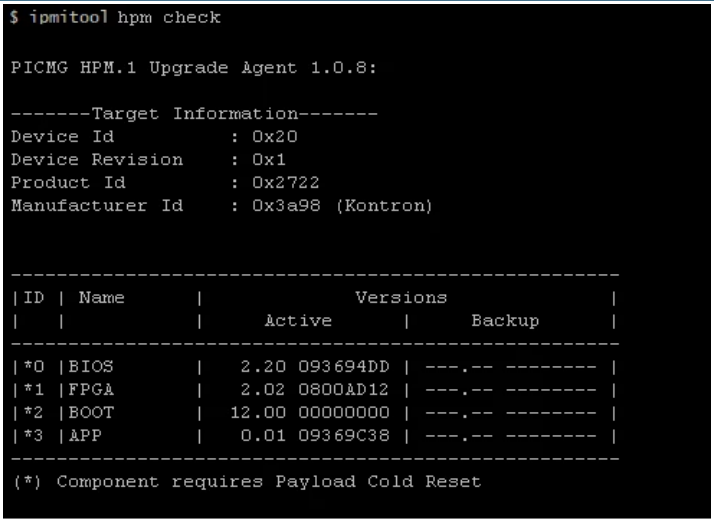
Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

Étape_1	Accéder à l'interface utilisateur Web du BMC du serveur.	
Étape_2	Dans le menu de gauche, sélectionner **Maintenance** puis **Firmware Information**.	
Étape_3	La version du micrologiciel est affichée.	

13.1.2.2. Recueillir la version du micrologiciel en utilisant IPMI

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL (Accéder au BMC en utilisant IPMI sur LAN (IOL)).

Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, accéder à l'information sur le micrologiciel. InviteSE_ServeurLocal:~$ **ipmitool hpm check**	

13.1.3. Recueillir les journaux des événements système

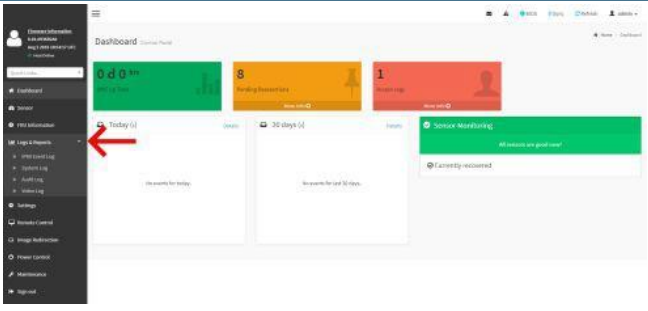
Les journaux des événements système peuvent être recueillis :

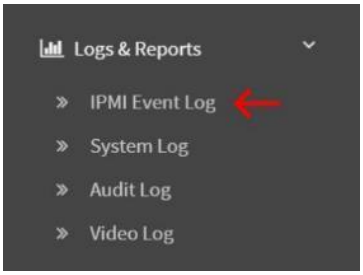
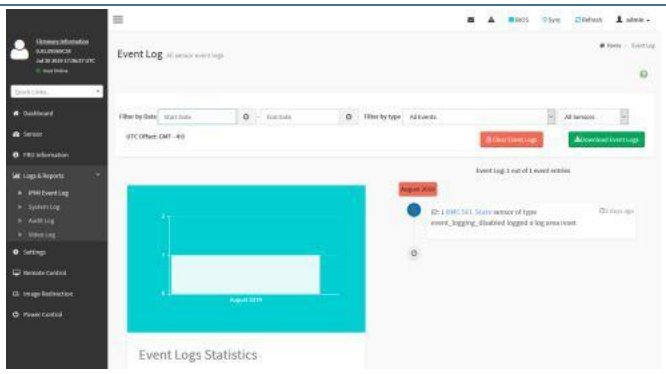
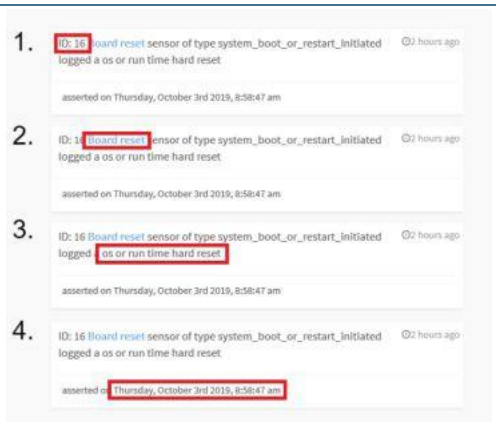
- En utilisant l'interface utilisateur Web du BMC
- En utilisant IPMI

13.1.3.1. Recueillir les journaux des événements système en utilisant l'interface utilisateur Web du BMC

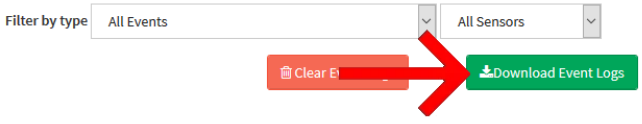
13.1.3.1.1.1. Accéder au journal des événements système

Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

Étape_1	Accéder à l'interface utilisateur Web du BMC du serveur.	
Étape_2	Sélectionner **Logs & Reports** dans le menu de gauche.	

Étape_3	Sélectionner **IPMI Event Log** dans le menu déroulant.	
Étape_4	Le journal des événements système s'affiche.	
Étape_5	Cliquer sur un événement et recueillir les informations suivantes : 1. ID de l'événement 2. Capteur associé 3. Description 4. Estampille temporelle d'assertion	

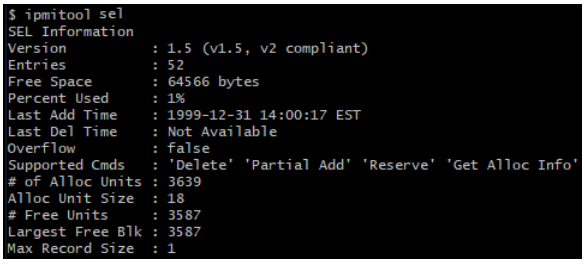
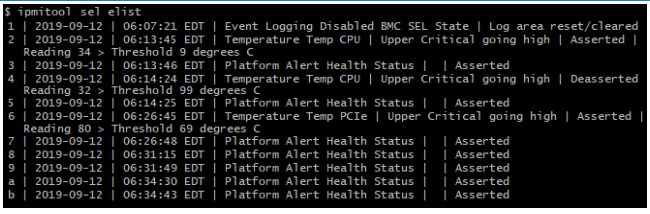
13.1.3.1.2. Télécharger les journaux des événements système

Étape_1	Dans le menu **Event Log**, sélectionner **Download Event Logs**.	

13.1.3.2. Recueillir les journaux des événements système en utilisant IPMI

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines configurations peuvent également être effectuées en utilisant IOL (Accéder au BMC en utilisant IPMI sur LAN (IOL)).

Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, accéder aux informations du journal des événements système. InviteSE_ServeurLocal:~$ **ipmitool sel**	
Étape_2	Accéder au journal des événements système. InviteSE_ServeurLocal:~$ **ipmitool sel elist**	
Étape_3	Recueillir les informations suivantes pour l'événement spécifié : • ID de l'événement – 1re colonne • Temps d'assertion – 2e et 3e colonne • Capteur associé – 4e colonne (optionnel) • Description – 5e colonne	

13.2. Récupération d'un BIOS corrompu

Le processus normal de mise à niveau du BIOS ne s'est pas achevé avec succès, le BIOS est maintenant corrompu.

Il est possible de récupérer un BIOS corrompu si une sauvegarde du BIOS a été faite. Voir Sauvegarde et récupération du BIOS pour plus de détails.

13.3. Configurations par défaut

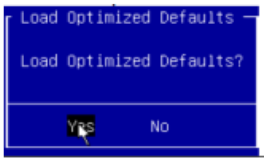
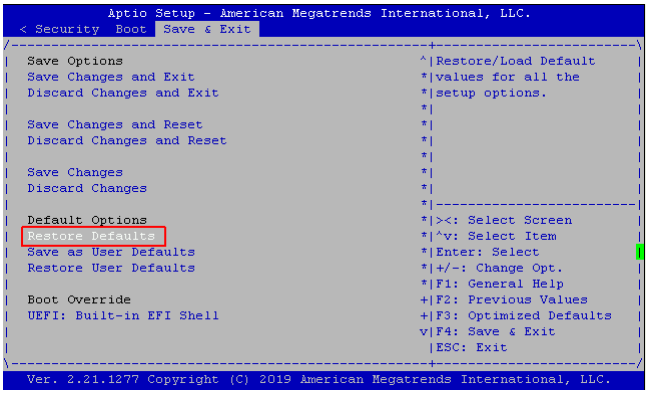
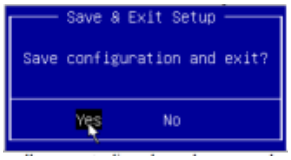
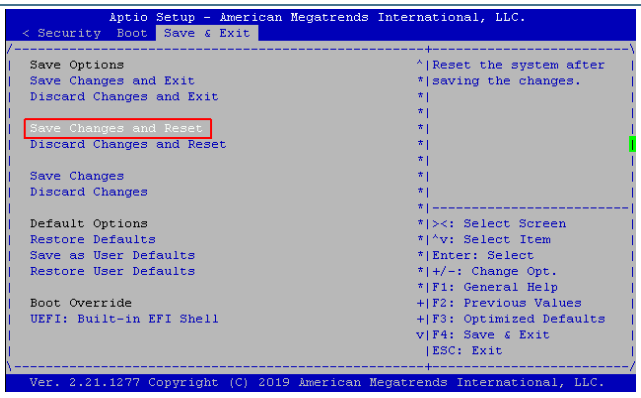
13.3.1. Rétablir les paramètres par défaut du BIOS

Les paramètres du BIOS peuvent être réinitialisés aux configurations par défaut :

- En utilisant le menu BIOS
- En utilisant IPMI
- En utilisant un cavalier

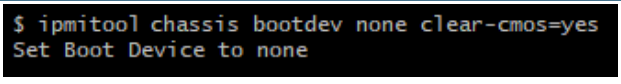
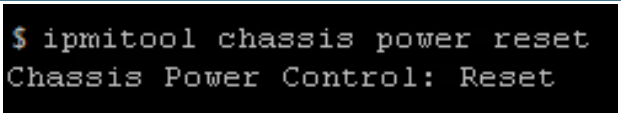
13.3.1.1. Rétablir les paramètres par défaut du BIOS en utilisant le menu BIOS

Voir Accéder au BIOS pour les instructions d'accès.

Étape_1	Dans le menu de configuration du BIOS, accéder au menu **Save & Exit** et sélectionner **Restore Defaults**. **NOTE** : Il est aussi possible d'appuyer sur F3 à partir de n'importe quel endroit du menu BIOS et de répondre **Yes** à la question **Load Optimized Defaults**. 	
Étape_2	Sélectionner **Save Changes and Reset**. **NOTE** : Il est aussi possible d'appuyer sur F4 à partir de n'importe quel endroit du menu BIOS et de répondre **Yes** à la question **Save configuration and exit?**. 	
Étape_3	Attendre que la plateforme se réinitialise. Les paramètres du BIOS devraient avoir été réinitialisés aux configurations par défaut.	

13.3.1.2. Rétablir les paramètres par défaut du BIOS en utilisant IPMI

Les procédures suivantes seront exécutées en utilisant la méthode Accéder au BMC en utilisant IPMI via KCS, mais certaines opérations peuvent également être effectuées en utilisant IOL (Accéder au BMC en utilisant IPMI sur LAN (IOL)). Pour utiliser IOL, ajouter les paramètres IOL à la commande : **-I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI]**.

Étape_1	Rétablir les paramètres par défaut. InviteSE_ServeurLocal:~$ **ipmitool chassis bootdev none clear-cmos=yes**	
Étape_2	Réinitialiser la plateforme. Les paramètres du BIOS devraient avoir été réinitialisés aux configurations par défaut. InviteSE_ServeurLocal:~$ **ipmitool chassis power reset** **NOTE** : Cette étape doit être réalisée dans la minute qui suit l'envoi de la commande IPMI. Dans le cas contraire, le BMC effacera automatiquement la commande bootdev.	

13.3.1.3. Rétablir les paramètres par défaut du BIOS en utilisant un cavalier

Sections pertinentes :

Étape_1	Mettre le CG2400 hors tension.
Étape_2	Placer un cavalier entre les broches 11-12 du connecteur J36 (appelé Clear BIOS or BIOS Default sur le CG2400).
Étape_3	Mettre le CG2400 sous tension. Le BIOS réinitialise les paramètres du BIOS à Optimized defaults (les options par défaut sont sauvegardées à la fin du POST, avant le démarrage du système d'exploitation).
Étape_4	Mettre le CG2400 hors tension.
Étape_5	Retirer le cavalier entre les broches 11-12 du connecteur J36.
Étape_6	Mettre le CG2400 sous tension. Les paramètres du BIOS devraient toujours être Optimized defaults.

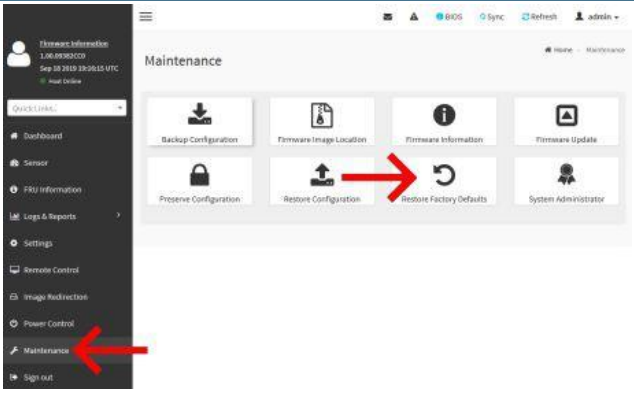
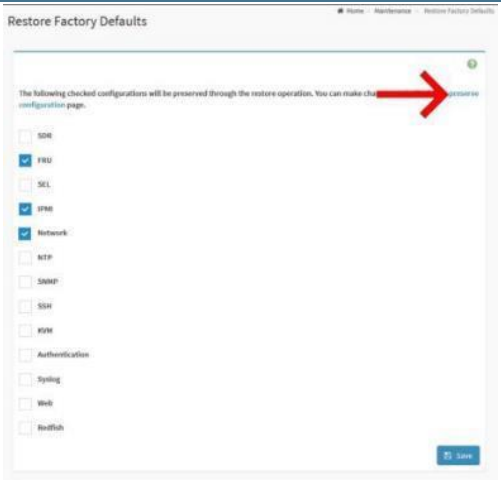
13.3.2. Rétablir les paramètres par défaut du BMC

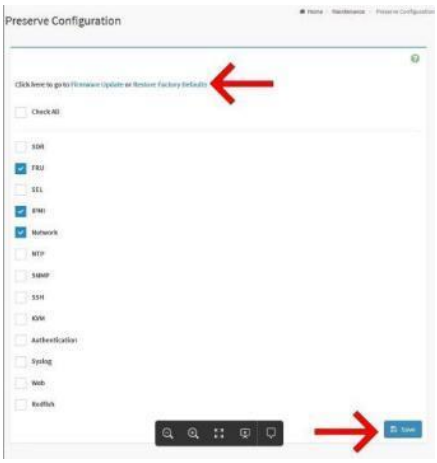
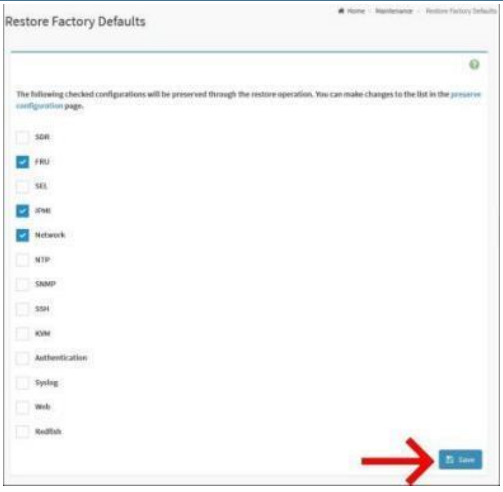
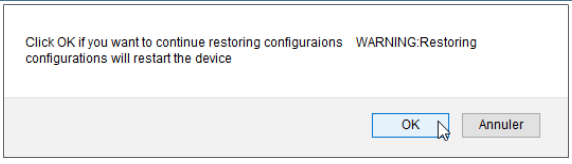
Les paramètres du BMC peuvent être réinitialisés aux configurations par défaut :

- En utilisant l'interface utilisateur Web
- En utilisant Redfish

13.3.2.1. Rétablir les paramètres par défaut du BMC en utilisant l'interface utilisateur Web du BMC

Voir Accéder au BMC pour les instructions d'accès.

Étape_1	Accéder à l'interface utilisateur Web du BMC du serveur.	
Étape_2	Dans le menu de gauche, sélectionner **Maintenance** puis **Restore Factory Defaults**.	
Étape_3	Si nécessaire, cliquer sur **preserve configuration** pour modifier la liste des configurations préservées.	

Étape_4	Modifier la liste des configurations préservées, si nécessaire. Cliquer sur **Save** puis sur **Restore Factory Defaults** pour retourner au menu précédent.	
Étape_5	Cliquer sur **Save**.	
Étape_6	Confirmer le rétablissement des configurations par défaut en cliquant sur **OK**. **NOTE** : La plateforme se réinitialise.	

13.3.2.2. Rétablir les paramètres par défaut du BMC en utilisant Redfish

Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	1 Rétablir les paramètres par défaut du BMC. InviteSE_OrdinateurDistant:~$ **curl -k -s [ROOT_URL]Managers/Actions/RedfishDBReset -X POST -d '{"FactoryResetType":"ResetAll"}' -H "Content-Type: application/json" | jq**	
Étape_2	Vérifier l'état d'alimentation. Attendre que l'état soit à On. InviteSE_OrdinateurDistant:~$ **curl -k -s [URL_RACINE]/Chassis/Self | jq .PowerState**	
Étape_3	Après la réinitialisation, les paramètres du BMC devraient avoir été rétablis à leur configuration par défaut.	

13.4. Obtenir du soutien

L'équipe du soutien technique de Kontron peut être jointe par les moyens suivants :

- Par téléphone : 1-888-835-6676
- Par courriel : support-na@kontron.com
- Via le site Web : www.kontron.com

14/ Base de connaissances

14.1. Utilisation de SNMP avec le contrôleur RAID

Les commandes peuvent varier en fonction du système d'exploitation et du gestionnaire de paquets.

Certains outils pourraient ne pas être nécessaires selon les fonctionnalités prises en charge par la plateforme.

14.1.1. Préalables

1	L'agent SNMP de Kontron pour Linux est installé et fonctionne sur la plateforme. Voir Configurer l'agent SNMP (snmp-agent) de Kontron pour Linux sur la plateforme.
2	Le paquet net-snmp-utils est installé. Voir Installation des logiciels courants.

NOTE : Il est recommandé de configurer snmpd en fonction des exigences de l'application avant de commencer à configurer SNMP pour le contrôleur RAID.

14.1.2. Installer SNMP pour le contrôleur RAID

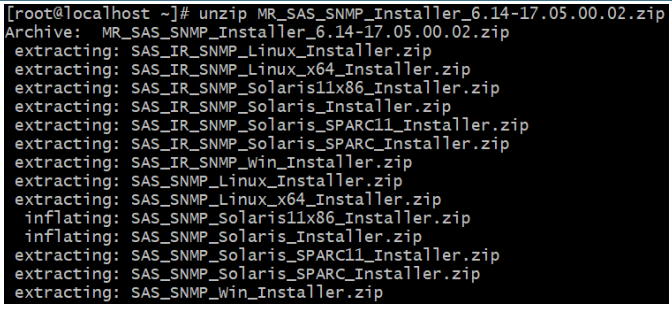
14.1.2.1. Télécharger le programme d'installation SNMP

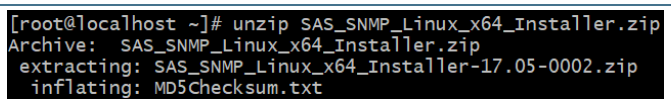
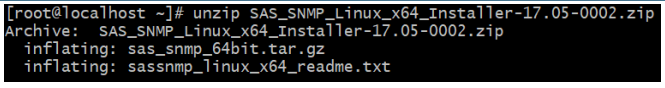
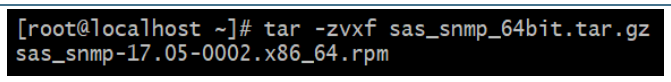
Il est recommandé d'utiliser la plus récente version du programme d'installation SNMP disponible sur le site Web de Broadcom. Dans cet exemple, cette version sera utilisée : https://docs.broadcom.com/docs-and-downloads/raid-controllers/raid-controllers-common-files/MR_SAS_SNMP_Installer_6.14-17.05.00.02.zip

Étape_1	À partir de l'invite de commande de la plateforme, télécharger le programme d'installation. InviteSE_ServeurLocal:~# **wget [URL_INSTALLATEUR_SNMP]**

14.1.2.2. Extraire le contenu

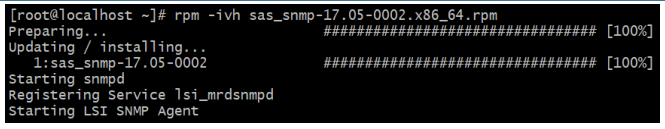
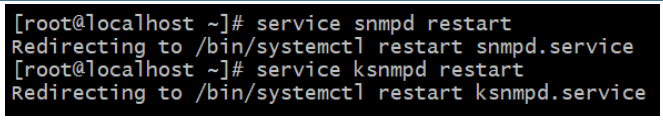
NOTE : Le système d'exploitation utilisé dans l'exemple est Centos 7.3. Les commandes peuvent varier en fonction du système d'exploitation installé.

Étape_1	Extraire le contenu de l'archive. InviteSE_ServeurLocal:~# **unzip MR_SAS_SNMP_I nstaller_6.14-17.05.00.02.zip**	

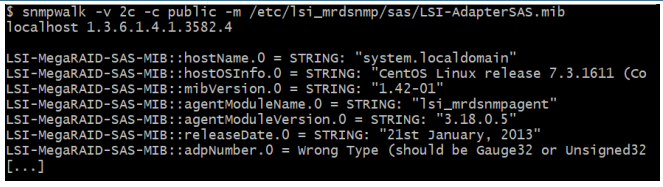
Étape_2	À partir des fichiers décompressés, extraire le contenu de l'archive générée correspondant au système d'exploitation de la plateforme. InviteSE_ServeurLocal:~# **unzip [NOM_ARCHIVE]**	
Étape_3	Extraire le fichier de l'archive générée. InviteSE_ServeurLocal:~# **unzip [NOM_ARCHIVE]**	
Étape_4	Extraire le contenu de l'archive suivante : InviteSE_ServeurLocal:~# **tar -zvxf sas_snmp_64bit.tar.gz**	

14.1.2.3. Installer le logiciel

NOTE : Les commandes peuvent varier en fonction du système d'exploitation installé.

Étape_1	Installer le logiciel. InviteSE_ServeurLocal:~# **rpm -ivh [PAQUET_RPM]**	
Étape_2	Redémarrer les services snmpd et ksnmpd à l'aide des commandes suivantes : InviteSE_ServeurLocal:~# **service snmpd restart** InviteSE_ServeurLocal:~# **service ksnmpd restart**	

14.1.3. Utiliser SNMP pour le contrôleur RAID

Étape_1	Le fichier MIP et la commande ci-dessous permettent d'obtenir toutes les informations sur le contrôleur. InviteSE_ServeurLocal:~# **snmpwalk -v 2c -c public -m /etc/lsi_mrdsnmp/sas/LSI -AdapterSAS.mib localhost 1.3.6.1.4.1.3582.4**	
Étape_2	Utiliser cette commande pour afficher le tableau des périphériques physiques. InviteSE_ServeurLocal:~# **snmptable -v 1 -c public -m /etc/lsi_mrdsnmp/sas/LSI -AdapterSAS.mib localhost 1.3.6.1.4.1.3582.4.1.4.2.1.2**	

14.1.4. Emplacement des fichiers MIB

Dans la configuration actuelle (Centos 7.3), le fichier MIB est situé ici : /etc/lsi_mrdsnmp/sas/LSI -AdapterSAS.mib

14.1.5. Différence entre SAS et SAS-IR

14.1.5.1. Définition

SAS-IR signifie SAS avec RAID intégré.

L'exemple utilise une version SAS (megaraid_sas). La carte RAID de la plateforme est physiquement branchée dans un emplacement PCIe.

14.1.5.2. Différence

Les différences entre SAS et SAS-IR lorsqu'il est question de SNMP sont les suivantes :

Si la version **SAS** est installée, l'OID suivant doit être utilisé pour obtenir les données : **1.3.6.1.4.1.3582**.

Si la version **SAS-IR** est installée, l'OID suivant doit être utilisé pour obtenir les données : **1.3.6.1.5.1.3582**.

14.2. Installer des clés de démarrage sécurisé personnalisées

14.2.1. Introduction

Cet article décrit comment installer un ensemble personnalisé de variables sécurisées utilisées avec la fonction de démarrage sécurisé (secure boot).

Le démarrage sécurisé est une fonction définie par l'UEFI qui permet d'authentifier un exécutable UEFI, tel qu'un chargeur de système d'exploitation, à l'aide de mécanismes de signature numérique basés sur le processus d'infrastructure à clé publique, réduisant ainsi les risques d'attaques de logiciels malveillants avant le démarrage. Cette fonction utilise une base de données de signatures autorisées pour confirmer l'intégrité de l'exécutable UEFI avant son exécution. Les plateformes disposent généralement d'un ensemble préchargé composé d'une clé de plateforme (PK), de clés d'échange de clés (KEK), d'une base de données de signatures autorisées (db) et d'une base de données de signatures révoquées/inscrites sur liste noire (dbx) tel que définies par le constructeur OEM, ainsi que de certains certificats standards émis par Microsoft qui permettent de démarrer Windows ou des distributions Linux bien connues telles qu'Ubuntu. Pour des raisons de sécurité, il pourrait être souhaitable pour l'utilisateur final de mettre à jour ces clés avec son propre ensemble.

Ce document suppose que le lecteur a une certaine connaissance du processus de démarrage sécurisé et que l'ensemble des clés et des certificats requis a été correctement généré. Le lien suivant fournit des lignes directrices sur la création et la gestion de ces clés et certificats :

https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-secure-boot-key-creation-and-management-guidance

14.2.2. Mettre à jour les clés de démarrage sécurisées à partir de l'utilitaire de configuration UEFI

14.2.2.1. Préalables

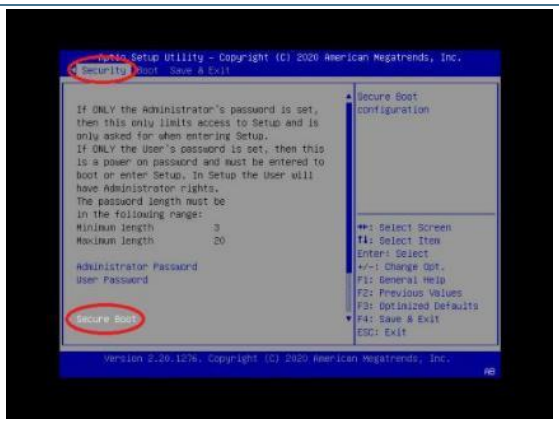
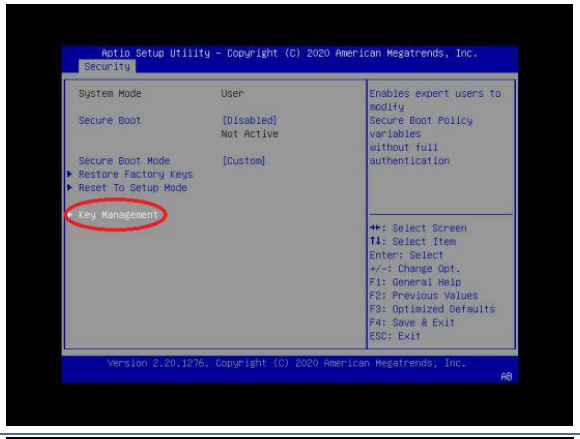
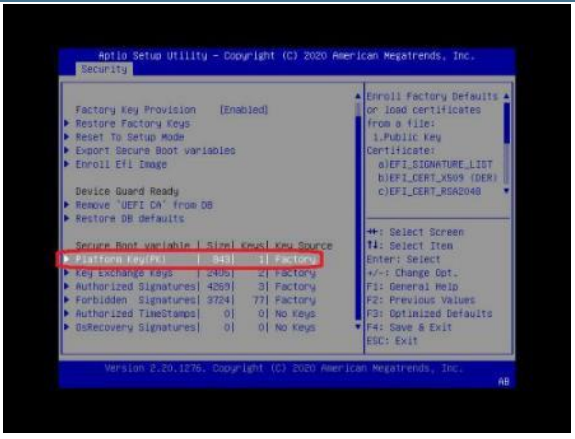
1	Un ensemble de clés de démarrage sécurisées a été créé (PK, KEK et db).
2	Les certificats de clé publique à installer sont au format DER.
3	Les certificats de clé publique sont présents sur une unité de stockage USB partitionnée en FAT qui est connectée à la plateforme. Si la redirection des supports virtuels est disponible, il est également possible d'utiliser une image ISO correspondante à la place.

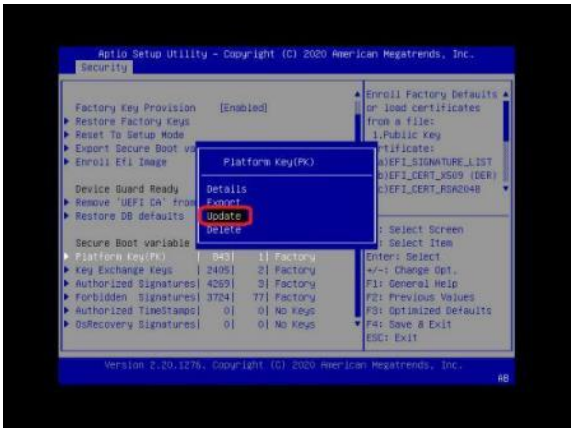
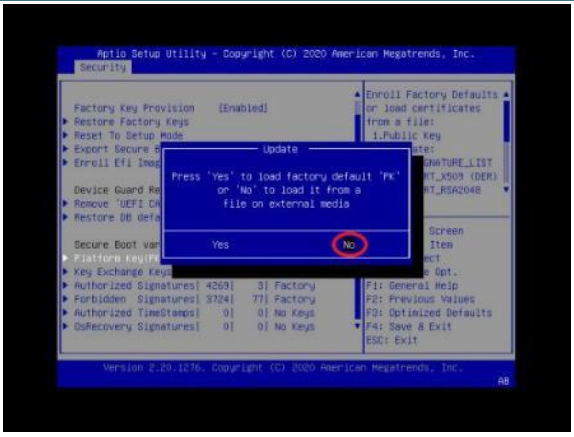
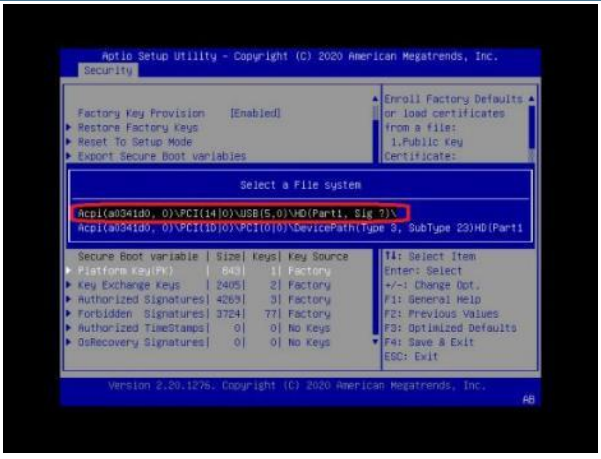
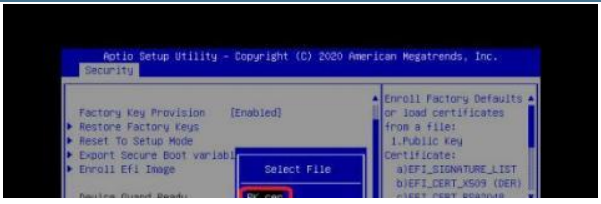
Section pertinente :

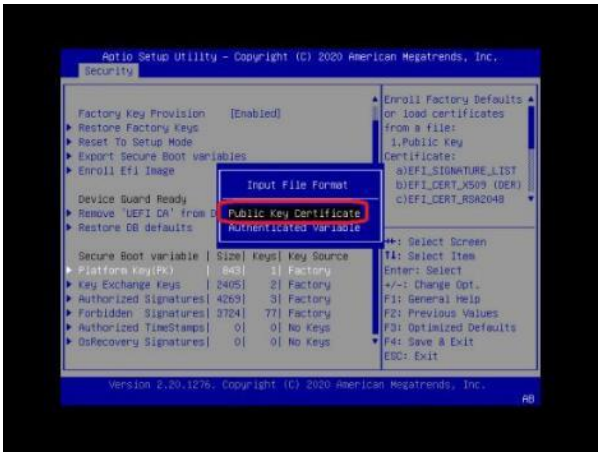
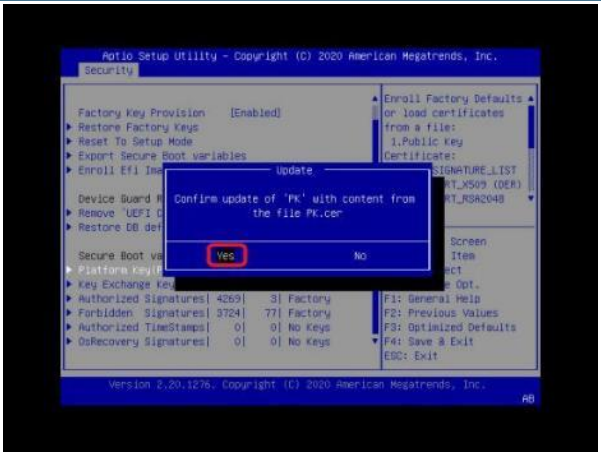
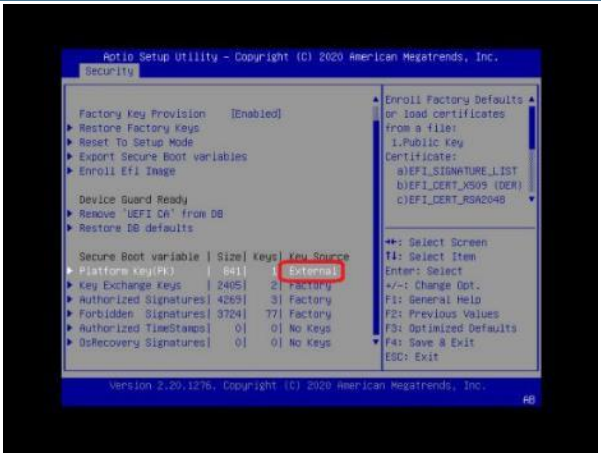
Générer des clés de démarrage sécurisé personnalisées

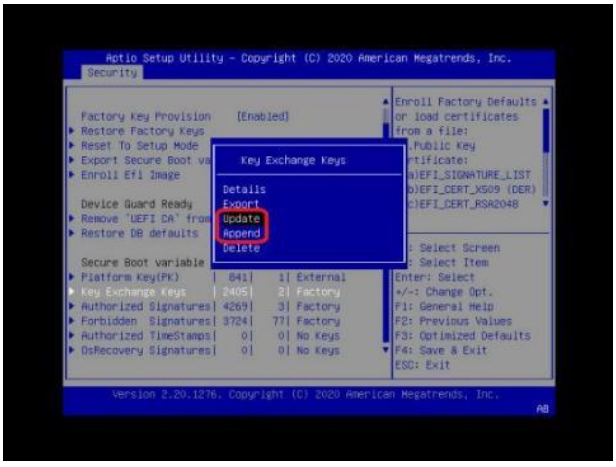
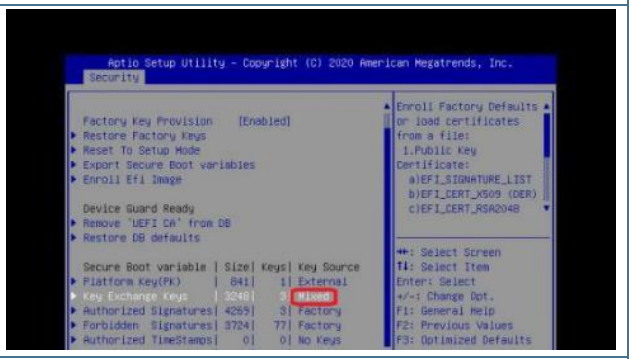
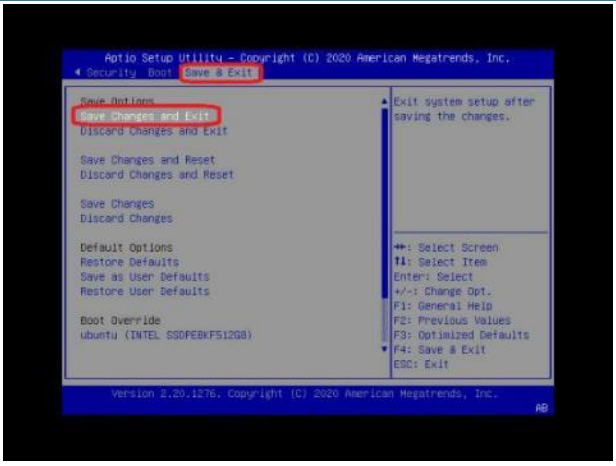
Puisque la date et l'heure actuelles sont vérifiées par rapport aux estampilles temporelles des certificats par mesure de sécurité, s'assurer que la date et l'heure du système sont valides avant de manipuler les variables du démarrage sécurisé. Si ce n'est pas le cas, une erreur de violation de la sécurité (security violation) sera obtenue et aucune modification ne sera possible.

14.2.2.2. Procédure

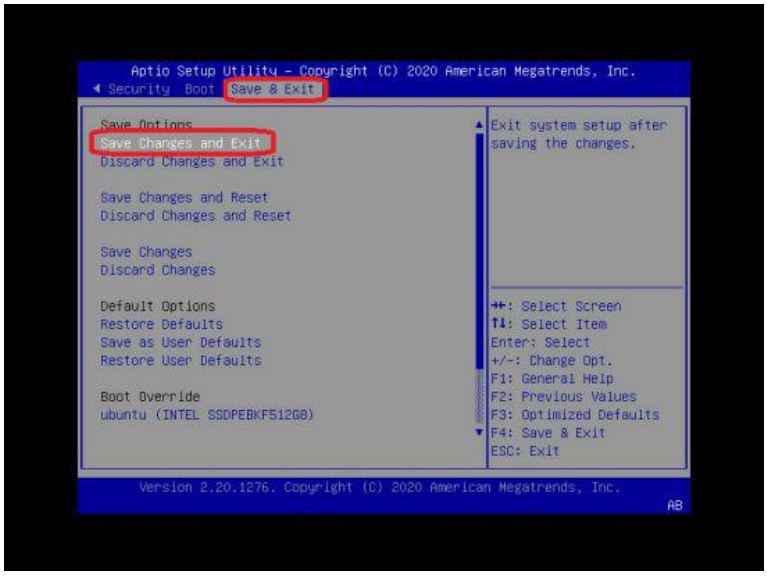
Étape_1	Accéder à l'utilitaire de configuration UEFI en appuyant sur F2 ou Suppr [DEL] lorsque l'écran d'ouverture de session s'affiche pendant le démarrage.	
Étape_2	À partir de l'onglet **Security**, accéder au sous-menu **Secure Boot**.	
Étape_3	Accéder à la page **Key Management** en sélectionnant l'élément de menu **Key Management**.	
Étape_4	Les clés installées en usine par défaut devraient déjà être installées. Voir l'attribut Factory dans la colonne Key Source du tableau Secure Boot variable. Pour remplacer la clé de plateforme par défaut par la vôtre, sélectionner **Platform Key(PK)**.	

Étape_5	Sélectionner **Update** dans la fenêtre contextuelle.	
Étape_6	Sélectionner **No** pour charger une clé à partir d'un support externe.	
Étape_7	Une liste des systèmes de fichiers disponibles s'affiche, avec le chemin d'accès au périphérique UEFI correspondant. Sélectionner l'unité de stockage USB où se trouvent les certificats de clé publique. Noter que si la redirection des supports virtuels est utilisée, l'unité sera identifiée comme un CDROM.	
Étape_8	Dans la liste des fichiers, sélectionner le fichier de certificats publics pour la clé de plateforme (PK.cer dans cet exemple).	

Étape_9	Spécifier que le format de fichier est **Public Key Certificate**.	
Étape_10	Sélectionner **Yes** pour confirmer la mise à jour de la clé de plateforme.	
Étape_11	Confirmer que la mise à jour s'est bien déroulée. Le tableau doit maintenant indiquer qu'une clé a été ajoutée à partir d'une source de clé **External**.	

<table>
<tr><td>Étape _12</td><td>Sélectionner Key Exchange Keys pour mettre à jour la base de données KEK ou pour y ajouter vos propres clés. Dans cet exemple :
Sélectionner Update dans la fenêtre contextuelle effacera les entrées KEK installées et ajoutera une nouvelle KEK en tant qu'entrée unique;
Sélectionner Append ajoutera la nouvelle KEK à la base de données.</td><td> 
</td></tr>
<tr><td>Étape _13</td><td>Suivre les étapes 4 à 11 pour ajouter une nouvelle entrée KEK. Si la KEK a été ajoutée à la base de données, le paramètre Key Source sera Mixed.</td><td> 
</td></tr>
<tr><td>Étape_14</td><td colspan="2">Sélectionner Authorized Signatures pour ajouter un certificat de clé publique autorisé à la base de données. Comme pour les KEK :
Sélectionner Update dans la fenêtre contextuelle effacera les entrées db installées et ajoutera un nouveau certificat en tant qu'entrée unique.
Sélectionner Append ajoutera le nouveau certificat à la base de données.
Suivre les étapes 4 à 11 pour ajouter une nouvelle entrée db. Si le certificat a été ajouté à la base de données, le paramètre Key Source sera Mixed.</td></tr>
<tr><td>Étape _15</td><td>Sélectionner Save Changes and Exit dans le menu.</td><td> 
</td></tr>
</table>

Pour profiter de la fonction de démarrage sécurisé, elle doit être activée (Security → sous-menu Secure Boot).



14.3. Générer des clés de démarrage sécurisé personnalisées

Section pertinente :

Installer des clés de démarrage sécurisé personnalisées

Pour installer des clés de démarrage sécurisées personnalisées, il peut être nécessaire de générer des clés. Cet article fournit un exemple utilisant CentOS 7.

14.3.1. Préalables

1	Les paquets efitools et sbsigntools doivent être disponibles. Ces paquets ne sont pas des paquets officiels de CentOS.

14.3.2. Procédure

Étape_1	Exécuter les commandes suivantes sur le système pour lequel des clés doivent être générées. mkdir make_keys cd make_keys wget https://github.com/freshautomations/efitools-centos/releases/download/2019-05-12/efitools-v1.9.2-1.x86_64.rpm wget https://github.com/freshautomations/efitools-centos/releases/download/2019-05-12/sbsigntools-v0.9.2-1.x86_64.rpm wget https://www.rodsbooks.com/efi-bootloaders/mkkeys.sh chmod +x mkkeys.sh yum install sbsigntools-v0.9.2-1.x86_64.rpm efitools-v1.9.2-1.x86_64.rpm ./mkkeys.sh
Étape_2	Les commandes génèrent un grand nombre de fichiers. Vous avez besoin du fichier *.cer dans la procédure d'installation.

14.4. Commandes IPMI prises en charge

R/O = Requise/Optionnel

14.4.1. Commandes d'application

14.4.1.1. Commandes IPMI pour l'unité

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x06	0x01	Get Device ID	Prise en charge	R
0x06	0x02	Cold Reset	Prise en charge	O
0x06	0x03	Warm Reset	Non prise en charge *	O
0x06	0x04	Get Self Test Results	Prise en charge	R
0x06	0x05	Manufacturing Test On	Non prise en charge *	O
0x06	0x06	Set ACPI Power State	Prise en charge	O
0x06	0x07	Get ACPI Power State	Prise en charge	O
0x06	0x08	Get Device GUID	Prise en charge	O
0x06	0x09	Get NetFn Support	Prise en charge	O
0x06	0x0A	Get Command Support	Prise en charge	O
0x06	0x0C	Get Configurable Commands	Prise en charge	O
0x06	0x60	Set Command Enables	Prise en charge	O
0x06	0x61	Get Command Enables	Prise en charge	O
0x06	0x64	Get OEM NetFn IANA Support	Prise en charge	O
0x06	0x0B	Get Command Sub-function Support	Prise en charge	O
0x06	0x0D	Get Configurable Command Sub-functions	Prise en charge	O
0x06	0x62	Set Command Sub-function Enables	Non prise en charge	O
0x06	0x63	Get Command Sub-function Enables	Non prise en charge	O
0x06	0x52	Master Write-Read	Prise en charge	O

* Les commandes ne sont pas rejetées et peuvent entraîner un comportement imprévisible.

14.4.1.2. Commandes de l'horloge de surveillance (watchdog timer)

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x06	0x22	Reset Watchdog Timer	Prise en charge	R
0x06	0x24	Set Watchdog Timer	Prise en charge	R
0x06	0x25	Get Watchdog Timer	Prise en charge	R

14.4.1.3. Commandes associées à l'unité et aux messages BMC

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x06	0x2E	Set BMC Global Enables	Prise en charge	R

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x06	0x2F	Get BMC Global Enables	Prise en charge	R
0x06	0x30	Clear Message Flags	Prise en charge	R
0x06	0x31	Get Message Flags	Prise en charge	R
0x06	0x32	Enable Message Channel Receive	Prise en charge	O
0x06	0x33	Get Message	Prise en charge	R
0x06	0x34	Send Message	Prise en charge	R
0x06	0x35	Read Event Message Buffer	Prise en charge	O
0x06	0x37	Get System GUID	Prise en charge	O
0x06	0x38	Get Channel Authentication Capabilities	Prise en charge	O
0x06	0x39	Get Session Challenge	Prise en charge	O
0x06	0x3A	Activate Session	Prise en charge	O
0x06	0x3B	Set Session Privilege Level	Prise en charge	O
0x06	0x3C	Close Session	Prise en charge	O
0x06	0x3D	Get Session Info	Prise en charge	O
0x06	0x3F	Get AuthCode	Prise en charge	O
0x06	0x40	Set Channel Access	Prise en charge	O
0x06	0x41	Get Channel Access	Prise en charge	O
0x06	0x42	Get Channel Info Command	Prise en charge	O
0x06	0x43	Set User Access Command	Prise en charge	O
0x06	0x44	Get User Access Command	Prise en charge	O
0x06	0x45	Set User Name	Prise en charge	O
0x06	0x46	Get User Name Command	Prise en charge	O
0x06	0x47	Set User Password Command	Prise en charge	O
0x06	0x52	Master Write-Read	Prise en charge	R
0x06	0x58	Set System Info Parameters	Prise en charge	O
0x06	0x59	Get System Info Parameters	Prise en charge	O

14.4.1.4. Commandes spécifiques à IPMI 2.0

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x06	0x48	Activate Payload	Prise en charge	O
0x06	0x49	Deactivate Payload	Prise en charge	O
0x06	0x4A	Get Payload Activation Statut	Prise en charge	O
0x06	0x4B	Get Payload Instance Info	Prise en charge	O
0x06	0x4C	Set User Payload Access	Prise en charge	O
0x06	0x4D	Get User Payload Access	Prise en charge	O
0x06	0x4E	Get Channel Payload Support	Prise en charge	O
0x06	0x4F	Get Channel Payload Version	Prise en charge	O
0x06	0x50	Get Channel OEM Payload Info	Prise en charge	O
0x06	0x54	Get Channel Cipher Suites	Prise en charge	O
0x06	0x55	Suspend/Resume Payload Encryption	Prise en charge	O
0x06	0x56	Set Channel Security Keys	Prise en charge	O

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x06	0x57	Get System Interface Capabilities	Prise en charge	O

14.4.1.5. Commandes de châssis

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x00	0x00	Get Chassis Capabilities	Prise en charge	R
0x00	0x01	Get Chassis Status	Prise en charge	R
0x00	0x02	Chassis Control	Prise en charge	R
0x00	0x04	Chassis Identify	Prise en charge	O
0x00	0x05	Set Chassis Capabilities	Prise en charge	O
0x00	0x06	Set Power Restore Policy	Prise en charge	O
0x00	0x07	Get System Restart Cause	Prise en charge	O
0x00	0x08	Set System Boot Options	Prise en charge	O
0x00	0x09	Get System Boot Options	Prise en charge	O
0x00	0x0A	Set Front Panel Button Enables	Prise en charge	O
0x00	0x0B	Set Power Cycle Interval	Prise en charge	O
0x00	0x0F	Get POH Counter	Prise en charge	O

14.4.2. Commandes de pont (bridge)

14.4.2.1. Commandes de gestion de pont

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x02	0x00	Get Bridge State	Non prise en charge	O
0x02	0x01	Set Bridge State	Non prise en charge	O
0x02	0x02	Get ICMB Address	Non prise en charge	O
0x02	0x03	Set ICMB Address	Non prise en charge	O
0x02	0x04	SetBridgeProxyAddress	Non prise en charge	O
0x02	0x05	Get Bridge Statistics	Non prise en charge	O
0x02	0x06	Get ICMB Capabilities	Non prise en charge	O
0x02	0x08	Clear Bridge Statistics	Non prise en charge	O
0x02	0x09	GetBridge Proxy Address	Non prise en charge	O
0x02	0x0A	Get ICMB Connector Info	Non prise en charge	R

14.4.2.2. Commandes de découverte de pont

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x02	0x10	Prepare For Discovery	Non prise en charge	O
0x02	0x11	Get Addresses	Non prise en charge	O
0x02	0x12	Set Discovered	Non prise en charge	O

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x02	0x13	Get Chassis Device Id	Non prise en charge	O
0x02	0x14	Set Chassis Device Id	Non prise en charge	O

14.4.2.3. Commandes de pontage (bridging)

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x02	0x20	Bridge Request	Non prise en charge	O
0x02	0x21	Bridge Message	Non prise en charge	O

14.4.2.4. Commandes d'événements de pont

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x02	0x30	Get Event Count	Non prise en charge	O
0x02	0x31	Set Event Destination	Non prise en charge	O
0x02	0x32	Set Event Reception State	Non prise en charge	O
0x02	0x33	SendICMB Event Message	Non prise en charge	O
0x02	0x34	Get Event Destination	Non prise en charge	O
0x02	0x35	Get Event Reception State	Non prise en charge	O

14.4.2.5. Commandes d'événements de capteurs (sensor)

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x04	0x00	Set Event Receiver	Prise en charge	R
0x04	0x01	Get Event Receiver	Prise en charge	R
0x04	0x02	Platform Event	Prise en charge	R
0x04	0x10	Get PEF Capabilities	Prise en charge	R
0x04	0x11	Arm PEF Postpone Timer	Prise en charge	R
0x04	0x12	Set PEF Configuration Parameters	Prise en charge	R
0x04	0x13	Get PEF Configuration Parameters	Prise en charge	R
0x04	0x14	Set Last Processed Event ID	Prise en charge	R
0x04	0x15	Get Last Processed Event ID	Prise en charge	R
0x04	0x16	Alert Immediate	Prise en charge	O
0x04	0x17	PET Acknowledge	Prise en charge	O
0x04	0x20	Get Device SDR Info	Prise en charge	O
0x04	0x21	Get Device SDR	Prise en charge	O
0x04	0x22	Reserve Device SDR Repository	Prise en charge	O
0x04	0x23	Get Sensor Reading Factors	Prise en charge	O
0x04	0x24	Set Sensor Hysteresis	Prise en charge	O
0x04	0x25	Get Sensor Hysteresis	Prise en charge	O
0x04	0x26	Set Sensor Threshold	Prise en charge	O

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x04	0x27	Get Sensor Threshold	Prise en charge	O
0x04	0x28	Set Sensor Event Enable	Prise en charge	O
0x04	0x29	Get Sensor Event Enable	Prise en charge	O
0x04	0x2A	Re-arm Sensor Events	Prise en charge	O
0x04	0x2B	Get Sensor Event Status	Prise en charge	O
0x04	0x2D	Get Sensor Reading	Prise en charge	R
0x04	0x2E	Set Sensor Type	Prise en charge	O
0x04	0x2F	Get Sensor Type	Prise en charge	O
0x04	0x30	Set Sensor Reading And Event Status	Prise en charge	O

14.4.3. Commandes de stockage

14.4.3.1. Commandes d'information FRU

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x0a	0x10	Get FRU Inventory Area Info	Prise en charge	R
0x0a	0x11	Read FRU Data	Prise en charge	R
0x0a	0x12	Write FRU Data	Prise en charge	R

14.4.3.2. Commandes du dépôt des enregistrements de données de capteurs (SDR repository)

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x0a	0x20	Get SDR Repository Info	Prise en charge	R
0x0a	0x21	Get SDR Repository Allocation Info	Prise en charge	O
0x0a	0x22	Reserve SDR Repository	Prise en charge	R
0x0a	0x23	Get SDR	Prise en charge	R
0x0a	0x24	Add SDR	Prise en charge	R
0x0a	0x25	Partial Add SDR	Prise en charge	R
0x0a	0x27	Clear SDR Repository	Prise en charge	R
0x0a	0x28	Get SDR Repository Time	Prise en charge	R
0x0a	0x2C	Run Initialization Agent	Prise en charge	O
0x0a	0x26	Delete SDR Repository	Prise en charge	R

14.4.3.3. Commandes du SEL

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x0a	0x40	Get SEL Info	Prise en charge	R
0x0a	0x41	Get SEL Allocation Info	Prise en charge	O
0x0a	0x42	Reserve SEL	Prise en charge	O
0x0a	0x43	Get SEL Entry	Prise en charge	R

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x0a	0x44	Add SEL Entry	Prise en charge	R
0x0a	0x45	Partial Add SEL Entry	Prise en charge	R
0x0a	0x47	Clear SEL	Prise en charge	R
0x0a	0x48	Get SEL Time	Prise en charge	R
0x0a	0x49	Set SEL Time	Prise en charge	R
0x0a	0x5C	Get SEL Time UTC OffSet	Prise en charge	O
0x0a	0x5D	Set SEL Time UTC OffSet	Prise en charge	O

14.4.4. Commandes de transport

14.4.4.1. Commandes IPMI pour l'unité

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x0c	0x01	Set LAN Configuration Parameters	Prise en charge	R
0x0c	0x02	Get LAN Configuration Parameters	Prise en charge	R
0x0c	0x03	Suspend BMC ARPs	Prise en charge	O

14.4.4.2. Commandes série sur LAN

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x0c	0x22	Get SOL Configuration Parameters	Prise en charge	O
0x0c	0x21	Set SOL Configuration Parameters	Prise en charge	O

14.4.5. Commandes AMI

14.4.5.1. Commande AMI pour rétablir les valeurs par défaut d'usine

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x32	0x66	Restore Defaults	Prise en charge	O

14.4.5.2. Commandes Kontron OEM

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge	R/O
0x3c	0x0A	Override Minimum Fan Speed	Prise en charge	O
0x3c	0x06	GUID provisioning	Prise en charge	O

14.5. Commandes Redfish prises en charge

Les informations sont présentées dans le format suivant : Description | Méthode | URL

Les descriptions ne sont pas traduites puisqu'il s'agit de la norme Redfish.

14.5.1. URL divers

- Root resource of the Redfish service | -GET | /redfish/v1
- Collection of DynamicExtension types | -GET | /redfish/v1/DynamicExtension
- Collection of DynamicExtensions | -GET | /redfish/v1/DynamicExtension/[DYNAMIC_EXTENSION_INSTANCE]
- Collection of log services for this system | -GET | /redfish/v1/DynamicExtension/LogServices
- Composition Service | -GET | /redfish/v1/CompositionService
- Collection of ResourceBlocks | -GET or -PATCH | /redfish/v1/CompositionService/ResourceBlocks
- Collection of ResourceZones | -GET | /redfish/v1/CompositionService/ResourceZones
- Event service | -GET or -PATCH | /redfish/v1/EventService
- Collection of event subscriptions | -GET | /redfish/v1/EventService/Subscriptions
- Task service | -GET | /redfish/v1/TaskService
- Task collection | -GET | /redfish/v1/TaskService/Tasks
- List of OEM JSON schemas and extensions | -GET | /redfish/v1/JsonSchemas
- Returns informations about a specified JSON schema | -GET | /redfish/v1/JsonSchemas/[JSON_SCHEMA_NAME]
  Collection of sessions | -GET or -POST | /redfish/v1/SessionService/Sessions
- Session service | -GET or -PATCH | /redfish/v1/SessionService
- Returns informations about a specified session | -GET or -DELETE |
  /redfish/v1/SessionService/Sessions/[SESSION_ID]
- Registry repository | -GET | /redfish/v1/Registries
- Returns the summary of a specified registry | -GET | /redfish/v1/Registries/[REGISTRY_INSTANCE]
- Returns detailed informations about a specified registry | -GET | /redfish/v1/Registries/[REGISTRY_INSTANCE.JSON]
- Redfish update service | -GET or -PATCH | /redfish/v1/UpdateService

14.5.2. URL des systèmes (Systems)

- Collection of computer systems | -GET | /redfish/v1/Systems
- Information about a specified system | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]
- Computer system reset action | -POST | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Actions/ComputerSystem.Reset
- Collection of memories for this system | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Memory
- Collection of processors | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Processors
- Collection of ethernet interfaces for this system | -GET /redfish/v1/Systems/[SYSTEM_INSTANCE]/EthernetInterfaces
- Collection of simple storage for this system | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/SimpleStorage
- Collection of log services for this system | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices
- IPMI SEL events for this manager | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices/BIOS
- Collection of entries for this log service | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices/BIOS/Entries
- Collection of network interfaces | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/NetworkInterfaces
- Collection of storage resource instances | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Storage
- A reference to the UEFI SecureBoot resource associated with this system | -GET |
  /redfish/v1/Systems/[SYSTEM_INSTANCE]/SecureBoot
- Collection of memory domains | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/MemoryDomains
- Zone capabilities | -GET | /redfish/v1/Systems/Capabilities

14.5.3. URL des gestionnaires (Managers)

- Collection of managers | -GET | /redfish/v1/Managers
- Collection of Ethernet interfaces for a specified manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/EthernetInterfaces
- Information about a specified ethernet interface | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/EthernetInterfaces/[ETHERNET_INTERFACE_INSTANCE]
- Collection of log services for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices
- Audit log service for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/AuditLog
- Collection of audit log service entries for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/AuditLog/Entries
- IPMI SEL service for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/SEL
- Collection of entries for the IPMI SEL service | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/SEL/Entries
- Event log service for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/EventLog
- Collection of event log service entries for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/EventLog/Entries
- Clear every entry of a specified log service for this manager | -POST | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/[LOG_SERVICE_INSTANCE]/Actions/LogService.ClearLog
- Information about a specified manager | -GET or -PATCH | /redfish/v1/Managers/[MANAGER_INSTANCE]
- Cold reset action for this manager | -POST | /redfish/v1/Managers/[MANAGER_INSTANCE]/Actions/Manager.Reset
- Collection of network protocol informations | -GET or -PATCH | /redfish/v1/Managers/[MANAGER_INSTANCE]/NetworkProtocol
- Collection of serial interfaces for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/SerialInterfaces
- Information about a specified serial interface | -GET or -PATCH | /redfish/v1/Managers/[MANAGER_INSTANCE]/SerialInterfaces/[SERIAL_INTERFACE_INSTANCE] Collection of virtual media | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/VirtualMedia
- Collection of host interfaces | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/HostInterfaces
- Information about a specified host interface | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/HostInterfaces/[HOST_INTERFACE_INSTANCE]
- Collection of ethernet interfaces connected to this host interface on this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/HostInterfaces/[HOST_INTERFACE_INSTANCE]/HostEthernetInterfaces
- Configures the number of CD/DVD devices that are supported for virtual media redirection | -POST |/redfish/v1/Managers/[MANAGER_INSTANCE]/Actions/Oem/Ami/VirtualMedia.ConfigureCDInstance
- Enables/disables RMedia support | -POST | /redfish/v1/Managers/[MANAGER_INSTANCE]/Actions/Oem/Ami/VirtualMedia.EnableRMedia

14.5.4. URL de télémétrie (Telemetry)

- Collection of log services for this telemetry service | -GET | /redfish/v1/TelemetryService/LogServices
- Information about the metric report log service | -GET | /redfish/v1/TelemetryService/LogServices/MetricReportLog
- Metric report log service entries | -GET | /redfish/v1/TelemetryService/LogServices/MetricReportLog/Entries
- Information about the telemetry service | -GET | /redfish/v1/TelemetryService
- Generates a test metric report | -POST | /redfish/v1/TelemetryService/Actions/ TelemetryService.SubmitTestMetricReport
- Collection of metric definitions | -GET | /redfish/v1/TelemetryService/MetricDefinitions
- Collection of metric definitions | -GET or -POST | /redfish/v1/TelemetryService/MetricReportDefinitions
- Information about a specified metric definition | -GET or -PATCH or -DELETE | /redfish/v1/TelemetryService/MetricReportDefinitions/[METRIC_REPORT_DEF]
- Collection of metric reports | -GET | /redfish/v1/TelemetryService/MetricReports
- Information about a specified metric report instance | -GET | /redfish/v1/TelemetryService/MetricReports/[METRIC_REPORT_INSTANCE]
- Collection of triggers | -GET or -POST | /redfish/v1/TelemetryService/Triggers

- Information about a specified trigger | -GET or -DELETE | /redfish/v1/TelemetryService/Triggers/[TRIGGER_INSTANCE]
- Metric report log service | -GET | /redfish/v1/TelemetryService/LogServices/MetricReportLog
- Clears the metric report log service | -POST | /redfish/v1/TelemetryService/LogServices/MetricReportLog/Actions/LogService.ClearLog
- Collection of metric report log service entries | -GET | /redfish/v1/TelemetryService/LogServices/MetricReportLog/Entries/[LOG_ENTRY]

14.5.5. URL du châssis (Chassis)

- Chassis collection | -GET | /redfish/v1/Chassis
- Information about a specified chassis instance | -GET or -PATCH | /redfish/v1/Chassis/[CHASSIS_INSTANCE]
- Resets the chassis | -POST | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/Actions/Chassis.Reset
- Collection of voltage sensors | -GET | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/Power
- Collection of thermal sensors | -GET | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/Thermal
- Collection of network adapters | -GET | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/NetworkAdapters

14.5.6. URL du service de comptes (AccountService)

- Redfish account service | -GET or -PATCH | /redfish/v1/AccountService
- Collection of Redfish user accounts | -GET or -POST | /redfish/v1/AccountService/Accounts
- Information about a specified Redfish account | -GET or -PATCH or -DELETE | /redfish/v1/AccountService/Accounts/[ACCOUNT_INSTANCE]
- Collection of available roles | -GET or -POST | /redfish/v1/AccountService/Roles
- Information about a specified role | -GET or -PATCH or -DELETE | /redfish/v1/AccountService/Roles/[ROLE_INSTANCE]
- Collection of account service configurations | -GET or -PATCH | /redfish/v1/AccountService/Configurations

14.6. Liste des OID SNMP

Le tableau ci-après présente l'information qu'il serait possible de trouver en utilisant SNMP. **NOTE** : Les descriptions ne sont pas traduites puisqu'il s'agit de la norme SNMP.

OID	Description	Action
SNMPv2-MIB::sysObjectID.0		
DISMAN-EVENT-MIB::sysUpTimeInstance	The time (in hundredths of a second) since the network management portion of the system was last re- initialized.	GET
SNMPv2-MIB::sysContact.0	The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string.	GET SET
SNMPv2-MIB::sysName.0	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.	GET SET
SNMPv2-MIB::sysLocation.0	The physical location of this node (e.g.,`telephone closet, 3rd floor').	GET SET
SNMPv2-MIB::sysORLastChange.0	The value of sysUpTime at the time of the most recent change in state or value of any instance of sysORID.	GET
SNMPv2-MIB::sysORTable	The (conceptual) table listing the capabilities of the local SNMP application acting as a command responder with respect to various MIB modules. SNMP entities having dynamically-configurable support of MIB modules will have a dynamically-varying number of conceptual rows.	GET TABLE
IF-MIB::ifNumber.0	The number of network interfaces (regardless of their current state) present on this system.	GET
IF-MIB::ifTable	A list of interface entries. The number of entries is given by the value of ifNumber. The entries consist of these fields. Index, Descr, Type, Mtu, Speed, PhysAddress, AdminStatus, OperStatus, LastChange, InOctets, InUcastPkts, InNUcastPkts, InDiscards, InErrors InUnknownProtos, OutOctets, OutUcastPkts, OutNUcastPkts, OutDiscards, OutErrors, OutQLen.	GET TABLE
1.3.6.1.2.1.3.1.1.1	The interface on which this entry's equivalence is effective. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.	GET
1.3.6.1.2.1.3.1.1.2	The media-dependent `physical' address.	GET
1.3.6.1.2.1.3.1.1.3	The NetworkAddress (e.g., the IP address) corresponding to the media-dependent `physical' address.	GET
IP-MIB::ipForwarding	The indication of whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams. IP hosts do not (except those source-routed via the host).	GET
IP-MIB::ipDefaultTTL	The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol.	GET
IP-MIB::ipInReceives	The total number of input datagrams received from interfaces, including those received in error.	GET
IP-MIB::ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways	GET

OID	Description	Action
	and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.	
IP-MIB::ipForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source- Routed via this entity, and the Source- Route option processing was successful.	GET
IP-MIB::ipInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.	GET
IP-MIB::ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.	GET
IP-MIB::ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).	GET
IP-MIB::ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.	GET
IP-MIB::ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.	GET
IP-MIB::ipOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this `no-route' criterion. Note that this includes any datagarms which a host cannot route because all of its default gateways are down.	GET
IP-MIB::ipReasmTimeout	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.	GET
IP-MIB::ipReasmReqds	Number of IP fragments received which needed to be reassembled at this entity.	GET
IP-MIB::ipReasmOKs	Number of IP datagrams successfully re-assembled.	GET
IP-MIB::ipReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.	GET
IP-MIB::ipFragCreates	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.	GET
IP-MIB::ipFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.	GET

OID	Description	Action
IP-MIB::ipFragOKs	Number of IP datagrams that have been successfully fragmented at this entity.	GET
IP-MIB::ipAddrTable	Table of addressing information relevant to this entity's IP addresses.	GET TABLE
1.3.6.1.2.1.4.21	IP Routing table.	GET
IP-MIB::ipNetToMediaTable	IP Address Translation table used for mapping from IP addresses to physical addresses.	GET TABLE
IP-MIB::ipRoutingDiscards	The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.	GET
IP-FORWARD-MIB::ipCidrRouteTable	This entity's IP Routing table.	GET TABLE
IP-FORWARD-MIB::inetCidrRouteNumber	The number of current ipCidrRouteTable entries that are not invalid.	GET
IP-FORWARD-MIB::inetCidrRouteTable	This entity's IP Routing table.	GET TABLE
IP-MIB::ipv6IpForwarding	The indication of whether this entity is acting as an IPv6 router on any interface in respect to the forwarding of datagrams received by, but not addressed to, this entity. IPv6 routers forward datagrams. IPv6 hosts do not (except those source-routed via the host). When this object is written, the entity SHOULD save the change to non-volatile storage and restore the object from non-volatile storage upon re-initialization of the system.	GET
IP-MIB::ipv6IpDefaultHopLimit	The default value inserted into the Hop Limit field of the IPv6 header of datagrams originated at this entity whenever a Hop Limit value is not supplied by the transport layer protocol. When this object is written, the entity SHOULD save the change to non-volatile storage and restore the object from non-volatile storage upon re-initialization of the system.	GET
IP-MIB::ipSystemStatsTable	The table containing system wide, IP version specific traffic statistics. This table and the ipIfStatsTable contain similar objects whose difference is in their granularity. Where this table contains system wide traffic statistics, the ipIfStatsTable contains the same statistics but counted on a per-interface basis.	GET TABLE
IP-MIB::ipIfStatsTableLastChange	The value of sysUpTime on the most recent occasion at which a row in the ipIfStatsTable was added or deleted. If new objects are added to the ipIfStatsTable that require the ipIfStatsTableLastChange to be updated when they are modified, they must specify that requirement in their description clause.	GET
IP-MIB::ipIfStatsTable	The table containing per-interface traffic statistics. This table and the ipSystemStatsTable contain similar objects whose difference is in their granularity. Where this table contains per-interface statistics, the ipSystemStatsTable contains the same statistics, but counted on a system wide basis.	GET TABLE
IP-MIB::ipAddressPrefixTable	This table allows the user to determine the source of an IP address or set of IP addresses, and allows other tables to share the information via pointer rather than by copying.	GET TABLE

OID	Description	Action
	More information can be found here http://oidref.com/1.3.6.1.2.1.4.32	
IP-MIB::ipAddressSpinLock	An advisory lock used to allow cooperating SNMP managers to coordinate their use of the set operation in creating or modifying rows within this table. More information can be found here http://oidref.com/1.3.6.1.2.1.4.33	GET
IP-MIB::ipAddressTable	This table contains addressing information relevant to the entity's interfaces. More information can be found here http://oidref.com/1.3.6.1.2.1.4.34	GET TABLE
IP-MIB::ipNetToPhysicalTable	The IP Address Translation table used for mapping from IP addresses to physical addresses. The Address Translation tables contain the IP address to 'physical' address equivalences. Some interfaces do not use translation tables for determining address equivalences (e.g., DDN-X.25 has an algorithmic method); if all interfaces are of this type, then the Address Translation table is empty, i.e., has zero entries. While many protocols may be used to populate this table, ARP and Neighbor Discovery are the most likely options.	GET TABLE
IP-MIB::ipv6ScopeZoneIndexTable	The table used to describe IPv6 unicast and multicast scope zones. For those objects that have names rather than numbers, the names were chosen to coincide with the names used in the IPv6 address architecture document.	GET TABLE
IP-MIB::ipDefaultRouterTable	The table used to describe the default routers known to this entity.	GET TABLE
IP-MIB::icmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.	GET
IP-MIB::icmpInErrors	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).	GET
IP-MIB::icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.	GET
IP-MIB::icmpInTimeExcds	Number of ICMP Time Exceeded messages received.	GET
IP-MIB::icmpInParmProbs	Number of ICMP Parameter Problem messages received.	GET
IP-MIB::icmpInParmProbs	Number of ICMP Parameter Problem messages received.	GET
IP-MIB::icmpInSrcQuenchs	Number of ICMP Source Quench messages received.	GET
IP-MIB::icmpInRedirects	Number of ICMP Redirect messages received.	GET
IP-MIB::icmpInEchos	Number of ICMP Echo (request) messages received.	GET
IP-MIB::icmpInEchoReps	Number of ICMP Echo Reply messages received.	GET
IP-MIB::icmpInTimestamps	Number of ICMP Timestamp (request) messages received.	GET
IP-MIB::icmpInTimestampReps	Number of ICMP Timestamp Reply messages received.	GET
IP-MIB::icmpInAddrMasks	Number of ICMP Address Mask Request messages received.	GET
IP-MIB::icmpInAddrMaskReps	Number of ICMP Address Mask Reply messages received.	GET
IP-MIB::icmpOutMsgs	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.	GET
IP-MIB::icmpOutErrors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of	GET

OID	Description	Action
	buffers. This value should notinclude errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.	
IP-MIB::icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.	GET
IP-MIB::icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.	GET
IP-MIB::icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.	GET
IP-MIB::icmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.	GET
IP-MIB::icmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.	GET
IP-MIB::icmpOutEchos	The number of ICMP Echo (request) messages sent.	GET
IP-MIB::icmpOutEchoReps	The number of ICMP Echo Reply messages sent.	GET
IP-MIB::icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.	GET
IP-MIB::icmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.	GET
IP-MIB::icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.	GET
IP-MIB::icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.	GET
IP-MIB::icmpStatsTable	The table of generic system-wide ICMP counters.	GET TABLE
IP-MIB::icmpMsgStatsTable	The table of system-wide per-version, per-message type ICMP counters.	GET TABLE
TCP-MIB::tcpRtoAlgorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.	GET
TCP-MIB::tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.	
TCP-MIB::tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.	GET
TCP-MIB::tcpMaxConn	The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.	GET
TCP-MIB::tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.	GET
TCP-MIB::tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.	GET
TCP-MIB::tcpAttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN- SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.	GET

OID	Description	Action
TCP-MIB::tcpEstabResets	The number of times that TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times that TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.	GET
TCP-MIB::tcpCurrEstab	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.	GET
TCP-MIB::tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.	GET
TCP-MIB::tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.	GET
TCP-MIB::tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.	GET
TCP-MIB::tcpConnTable	A table containing TCP connection-specific information.	GET TABLE
TCP-MIB::tcpInErrs	The total number of segments received in error (e.g., bad TCP checksums).	GET
TCP-MIB::tcpOutRsts	The number of TCP segments sent containing the RST flag.	GET
TCP-MIB::tcpConnectionState	The state of this TCP connection. More information can be found here https://oidref.com/1.3.6.1.2.1.6.12	GET
TCP-MIB::tcpConnectionProcess	The number of packets received on this connection. This count includes retransmitted data.	GET
TCP-MIB::tcpListenerTable	A table containing information about TCP listeners. More information can be found here https://oidref.com/1.3.6.1.2.1.6.20	GET TABLE
UDP-MIB::udpInDatagrams	The total number of UDP datagrams delivered to UDP users.	GET
UDP-MIB::udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.	GET
UDP-MIB::udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port	GET
UDP-MIB::udpOutDatagrams	The total number of UDP datagrams sent from this entity.	GET
UDP-MIB::udpTable	A table containing UDP listener information.	GET TABLE
UDP-MIB::udpEndpointTable	A table containing UDP listener information.	GET TABLE
SNMPv2-MIB::snmpInPkts	The total number of messages delivered to the SNMP entity from the transport service.	GET
SNMPv2-MIB::snmpOutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.	GET
SNMPv2-MIB::snmpInBadVersions	The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.	GET
SNMPv2-MIB::snmpInBadCommunityNames	The total number of SNMP Messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity.	GET

OID	Description	Action
SNMPv2-MIB::snmpInBadCommunityUses	The total number of community-based SNMP messages (for example, SNMPv1) delivered to the SNMP entity which represented an SNMP operation that was not allowed for the SNMP community named in the message. The precise conditions under which this counter is incremented (if at all) depend on how the SNMP entity implements its access control mechanism and how its applications interact with that access control mechanism. It is strongly RECOMMENDED that the documentation for any access control mechanism which is used to control access to and visibility of MIB instrumentation specify the precise conditions that contribute to this value.	GET
SNMPv2-MIB::snmpInASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.	GET
SNMPv2-MIB::snmpInTooBigs	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `tooBig'.	GET
SNMPv2-MIB::snmpInNoSuchNames	The total numb er of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `noSuchName'.	GET
SNMPv2-MIB::snmpInBadValues	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `badValue'.	GET
SNMPv2-MIB::snmpInReadOnlys	The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `readOnly'. It should be noted that it is a protocol error to generate an SNMP PDU which contains the value `readOnly' in the error-status field, as such this object is provided as a means of detecting incorrect implementations of the SNMP.	GET
SNMPv2-MIB::snmpInGenErrs	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `genErr'.	GET
SNMPv2-MIB::snmpInTotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.	GET
SNMPv2-MIB::snmpInTotalSetVars	The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.	GET
SNMPv2-MIB::snmpInGetRequests	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpInGetNexts	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpInSetRequests	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpInGetResponses	The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpInTraps	The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutTooBigs	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field was `tooBig.'	GET

OID	Description	Action
SNMPv2-MIB::snmpOutNoSuchNames	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status was `noSuchName'.	GET
SNMPv2-MIB::snmpOutBadValues	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field was `badValue'.	GET
SNMPv2-MIB::snmpOutGenErrs	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field was `genErr'.	GET
SNMPv2-MIB::snmpOutGetRequests	The total number of SNMP Get-Request PDUs which have been generated by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutGetNexts	The total number of SNMP Get-Next PDUs which have been generated by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutSetRequests	The total number of SNMP Set-Request PDUs which have been generated by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutGetResponses	The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutTraps	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpEnableAuthenTraps	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authenticationFailure traps may be disabled. Note that it is strongly recommended that this object be stored in non-volatile memory so that it remains constant across re-initializations of the network management system.	GET
SNMPv2-MIB::snmpSilentDrops	The total number of Confirmed Class PDUs (such as GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs) delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response Class PDU (such as a Response-PDU) with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.	GET
SNMPv2-MIB::snmpProxyDrops	The total number of Confirmed Class PDUs (such as GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs) delivered to the SNMP entity which were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a time-out) such that no Response Class PDU (such as a Response-PDU) could be returned.	GET
HOST-RESOURCES-MIB::hrSystemUptime	The amount of time since this host was last initialized. Note that this is different from sysUpTime in MIB-II [3] because sysUpTime is the uptime of the network management portion of the system.	GET
HOST-RESOURCES-MIB::hrSystemDate	The host's notion of the local date and time of day.	GET
HOST-RESOURCES-MIB::hrSystemInitialLoadDevice	The index of the hrDeviceEntry for the device from which this host is configured to load its initial operating system configuration.	GET

OID	Description	Action
HOST-RESOURCES-MIB::hrSystemInitialLoadParameters	This object contains the parameters (e.g. a pathname and parameter) supplied to the load device when requesting the initial operating system configuration from that device.	GET
MTA-MIB::mtaTable	The table holding information specific to an MTA.	GET TABLE
MTA-MIB::mtaGroupTable	The table holding information specific to each MTA group.	GET TABLE
IF-MIB::ifXTable	A list of interface entries. The number of entries is given by the value of ifNumber. This table contains additional objects for the interface table.	GET TABLE
IF-MIB::ifTableLastChange	The value of sysUpTime at the time of the last creation or deletion of an entry in the ifTable. If the number of entries has been unchanged since the last re-initialization of the local network management subsystem, then this object contains a zero value.	GET
IPV6-MIB::ipv6Forwarding	The indication of whether this entity is acting as an IPv6 router in respect to the forwarding of datagrams received by, but not addressed to, this entity. IPv6 routers forward datagrams. IPv6 hosts do not (except those source-routed via the host). More information can be found here https://oidref.com/1.3.6.1.2.1.55.1.1	GET
IPV6-MIB::ipv6DefaultHopLimit	The default value inserted into the Hop Limit field of the IPv6 header of datagrams originated at this entity, whenever a Hop Limit value is not supplied by the transport layer protocol.	GET
IPV6-MIB::ipv6Interfaces	The number of IPv6 interfaces (regardless of their current state) present on this system.	GET
IPV6-MIB::ipv6IfTable	The IPv6 Interfaces table contains information on the entity's internetwork-layer interfaces.An IPv6 interface constitutes a logical network layer attachment to the layer immediately below IPv6 including internet layer 'tunnels', such as tunnels over IPv4 or IPv6 itself.	GET TABLE
DISMAN-EVENT-MIB::mteResourceSampleMinimum	The minimum mteTriggerFrequency this system will accept. A system may use the larger values of this minimum to lessen the impact of constant sampling. For larger sampling intervals the system samples less often and suffers less overhead. This object provides a way to enforce such lower overhead for all triggers created after it is set. More information can be found here https://oidref.com/1.3.6.1.2.1.88.1.1.1	GET
DISMAN-EVENT-MIB::mteResourceSampleInstanceMaximum	The maximum number of instance entries this system will support for sampling. More information can be found here https://oidref.com/1.3.6.1.2.1.88.1.1.2	GET
DISMAN-EVENT-MIB::mteResourceSampleInstances	The number of currently active instance entries as defined for mteResourceSampleInstanceMaximum.	GET
DISMAN-EVENT-MIB::mteResourceSampleInstancesHigh	The highest value of mteResourceSampleInstances that has occurred since initialization of the management system.	GET
DISMAN-EVENT-MIB::mteResourceSampleInstanceLacks	The number of times this system could not take a new sample because that allocation would have exceeded the limit set by mteResourceSampleInstanceMaximum.	GET
DISMAN-EVENT-MIB::mteTriggerFailures	The minimum mteTriggerFrequency this system will accept. A system may use the larger values of this minimum to lessen the impact of constant sampling. For larger sampling intervals the	GET

OID	Description	Action
	system samples less often and suffers less overhead. This object provides a way to enforce such lower overhead for all triggers created after it is set.	
DISMAN-EVENT-MIB::mteObjectsTable	A table of objects that can be added to notifications based on the trigger, trigger test, or event, as pointed to by entries in those tables.	GET TABLE
DISMAN-EVENT-MIB::mteEventTable	A table of management event action information.	GET TABLE
DISMAN-EVENT-MIB::mteEventNotificationTable	A table of information about notifications to be sent as a consequence of management events.	GET TABLE
NOTIFICATION-LOG-MIB::nlmConfigGlobalEntryLimit	The maximum number of notification entries that may be held in nlmLogTable for all nlmLogNames added together. A particular setting does not guarantee that much data can be held. More information can be found here https://oidref.com/1.3.6.1.2.1.92.1.1.1	GET
NOTIFICATION-LOG-MIB::nlmConfigGlobalAgeOut	The number of minutes a Notification SHOULD be kept in a log before it is automatically removed. If an application changes the value of nlmConfigGlobalAgeOut, Notifications older than the new time MAY be discarded to meet the new time. A value of 0 means no age out. Please be aware that contention between multiple managers trying to set this object to different values MAY affect the reliability and completeness of data seen by each manager.	GET
NOTIFICATION-LOG-MIB::nlmStatsGlobalNotificationsLogged	The number of Notifications put into the nlmLogTable. This counts a Notification once for each log entry, so a Notification put into multiple logs is counted multiple times.	GET
NOTIFICATION-LOG-MIB::nlmStatsGlobalNotificationsBumped	The number of log entries discarded to make room for a new entry due to lack of resources or the value of nlmConfigGlobalEntryLimit or nlmConfigLogEntryLimit. This does not include entries iscarded due to the value of nlmConfigGlobalAgeOut.	GET
SNMPv2-SMI::enterprises.3582		GET
NET-SNMP-AGENT-MIB::nsModuleName	The module name that registered this OID.	GET
NET-SNMP-AGENT-MIB::nsModuleModes	The modes that the particular lower level handler can cope with directly.	GET
NET-SNMP-AGENT-MIB::nsModuleTimeout	The registered timeout. This is only meaningful for handlers that expect to return results at a later date (subagents, etc)	GET
NET-SNMP-EXTEND-MIB::nsExtendNumEntries	The number of rows in the nsExtendConfigTable.	GET
NET-SNMP-AGENT-MIB::nsCacheDefaultTimeout	Default cache timeout value (unless overridden for a particular cache entry).	GET
NET-SNMP-AGENT-MIB::nsCacheEnabled	Whether data caching is active overall.	GET
NET-SNMP-AGENT-MIB::nsCacheTimeout	The length of time (?in seconds) for which the data in this particular cache entry will remain valid.	GET
NET-SNMP-AGENT-MIB::nsCacheStatus	The current status of this particular cache entry. Acceptable values for Set requests are 'enabled(1)',	GET

OID	Description	Action
	'disabled(2)' or 'empty(3)' (to clear all cached data). Requests to read the value of such an object will return 'disabled(2)' through to 'expired(5)'.	
NET-SNMP-AGENT-MIB::nsDebugEnabled	Whether the agent is configured to generate debugging output	GET
NET-SNMP-AGENT-MIB::nsDebugOutputAll	Whether the agent is configured to display all debugging output rather than filtering on individual debug tokens. Nothing willbe generated unless nsDebugEnabled is also true(1)	GET
NET-SNMP-AGENT-MIB::nsDebugDumpPdu	Whether the agent is configured to display raw packet dumps. This is unrelated to the nsDebugEnabled setting.	GET
NET-SNMP-AGENT-MIB::nsLogType	The (minimum) priority level for which this logging entry should be applied.	GET
NET-SNMP-AGENT-MIB::nsLogMaxLevel	The maximum priority level for which this logging entry should be applied.	GET
NET-SNMP-AGENT-MIB::nsLogStatus	Whether to generate logging output for this entry. Note that is valid for an instance to be left with the value notInService(2) indefinitely - i.e. the meaning of 'abnormally long' (see RFC 2579, RowStatus) for this table is infinite.	GET
NET-SNMP-VACM- MIB::nsVacmContextMatch	If the value of this object is exact(1), then all rows where the contextName exactly matches vacmAccessContextPrefix are selected. If the value of this object is prefix(2), then all rows where the contextName whose starting octets exactly match vacmAccessContextPrefix are selected. This allows for a simple form of wildcarding. The value of this object should be consistent across all nsVacmAccessEntries corresponding to a single row of the vacmAccessTable.	GET
NET-SNMP-VACM-MIB::nsVacmViewName	The MIB view authorised for the appropriate style of processing (as indicated by nsVacmToken). The interpretation of this value is the same as for the standard VACM ViewName objects.	GET
NET-SNMP-VACM- MIB::nsVacmStorageType	The storage type for this (group of) conceptual rows. Conceptual rows having the value 'permanent' need not allow write-access to any columnar objects in the row. The value of this object should be consistent across all nsVacmAccessEntries corresponding to a single row of the vacmAccessTable.	GET
NET-SNMP-VACM-MIB::nsVacmStatus	The status of this (group of) conceptual rows. The RowStatus TC [RFC2579] requires that this DESCRIPTION clause states under which circumstances other objects in this row can be modified: The value of this object has no effect on whether other objects in this conceptual row can be modified. The value of this object should be consistent across all nsVacmAccessEntries corresponding to a single row of the vacmAccessTable.	GET
SNMPv2-SMI::enterprises.20974.554.1	AMI SNMP Hostname Extension	GET
SNMPv2-SMI::enterprises.20974.554.2	AMI SNMP MIB library to return the system health status like power and sensor status.	GET
SNMPv2-SMI::enterprises.20974.554.3	AMI SNMP Platform Info Extension	GET

14.7. CG2400 SNMP – Guide d'utilisation du BMC

SNMP est un protocole utilisé pour échanger des informations de gestion entre différents appareils connectés sur un réseau. Ce guide explique la procédure à suivre pour obtenir un accès de base au BMC.

NOTE : Seule la version 3 de SNMP est prise en charge.

14.7.1. Installation

Il est possible d'accéder au BMC via SNMP sur n'importe quel nœud Linux, mais ce tutoriel se concentre sur Ubuntu. Tout d'abord, installer SNMP.

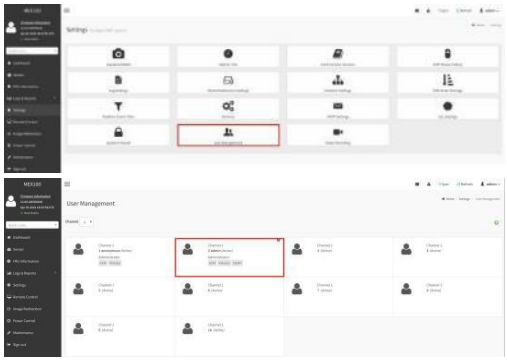
```
$ apt–get install snmp
```

Pour pouvoir voir la base d'information de gestion (MIB) lisible en clair (au lieu de voir l'identificateur d'objet [OID]), installer également le progiciel suivant.

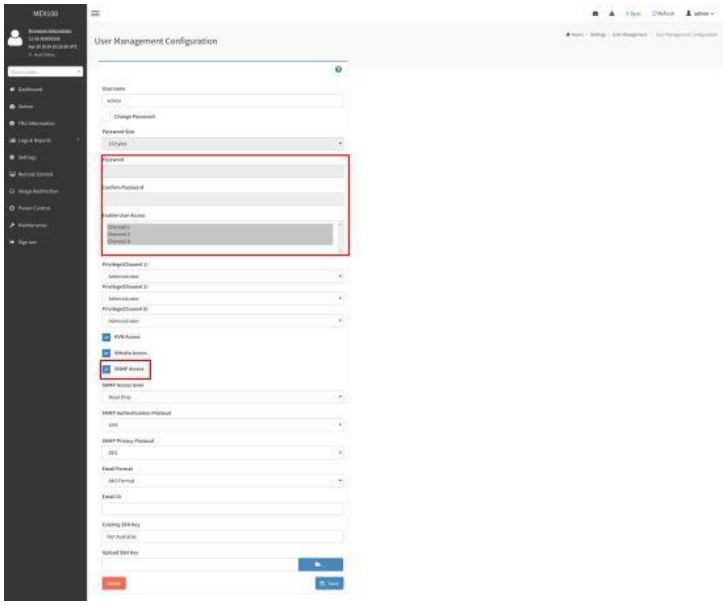
```
$ apt-get install snmp-mibs-downloader
```

14.7.2. Configuration

Maintenant que SNMP est installé, modifier un utilisateur pour activer SNMP.



IMPORTANT : Modifier le mot de passe pour qu'il soit plus long que admin (minimum 8 caractères) et activer l'accès SNMP.



14.7.3. Opération

Pour voir un OID spécifique, utiliser la commande suivante avec l'utilisateur créé à l'étape précédente :

```
snmpwalk -v3 -l authPriv -u admin -a SHA -A "superuser" -x DES -X "superuser" <host_IP> <OID>
```

Pour accéder aux capteurs du BMC, utiliser la commande suivante :

```
$ snmpwalk -v3 -l authPriv -u admin -a SHA -A "superuser" -x DES -X "superuser" <host_IP> SNMPv2-SMI::enterprises.20974.554
```

Vous pouvez aussi faire grep pour le capteur de votre choix :

```
$ snmpwalk -v3 -l authPriv -u admin -a SHA -A "superuser" -x DES -X "superuser" <host_IP> SNMPv2-SMI::enterprises.20974.554 | grep 2\.1\..\.21

SNMPv2-SMI::enterprises.20974.554.2.1.1.21 = INTEGER: 21

SNMPv2-SMI::enterprises.20974.554.2.1.2.21 = STRING: "Fan1 Speed"

SNMPv2-SMI::enterprises.20974.554.2.1.3.21 = INTEGER: 45

SNMPv2-SMI::enterprises.20974.554.2.1.4.21 = Opaque: Float: 1640,00000
```

14.8. Démon mcelog – identification d'un module DIMM défectueux à partir du journal des erreurs

Des exceptions de vérification de machine (MCE) peuvent se produire pour diverses raisons, telles que des tensions indésirables provenant du bloc d'alimentation, des radiations cosmiques inversant des bits dans la mémoire

DIMM ou le CPU, ou d'autres défauts divers, y compris un logiciel défectueux déclenchant des erreurs matérielles.

14.8.1. Démon mcelog

Sur les systèmes Linux x86 modernes, mcelog enregistre et comptabilise les erreurs et les exceptions de vérification de machine. Toutes les erreurs sont enregistrées dans /var/log/mcelog ou syslog ou dans le journal dans le format suivant :

Hardware event. This is not a software error.

MCE 0

CPU 0 BANK 18

MISC 90840080008228c ADDR 9ce494000

TIME 1499161840 Tue Jul 4 09:50:40 2021

MCG status:

MCi status:

Corrected error

MCi_MISC register valid

MCi_ADDR register valid

MCA: MEMORY CONTROLLER MS_CHANNEL2_ERR

Transaction: Memory scrubbing error

MemCtrl: Corrected patrol scrub error

STATUS 8c000051000800c2 MCGSTATUS 0

MCGCAP 7000c16 APICID 0 SOCKETID 0

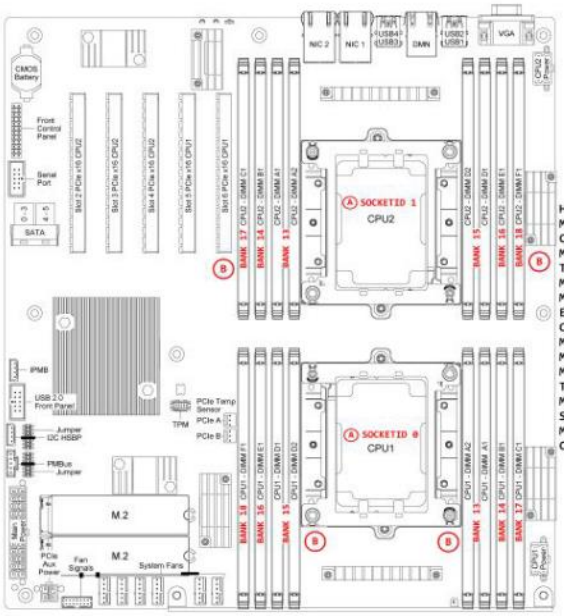
CPUID Vendor Intel Family 6 Model 85

Pour la famille de processeurs utilisée sur le CG2400, les banques de contrôle machine suivantes sont associées à des erreurs provenant de l'un des contrôleurs de mémoire interne (IMC).

Numéro de banque de machines	Unité de processeur
7	IMC 0, Main
8	IMC 1, Main
13	IMC 0, channel 0
14	IMC 0, channel 1
15	IMC 1, channel 0
16	IMC 1, channel 1
17	IMC 0, channel 2
18	IMC 1, channel 2

14.8.2. Emplacement des DIMM

Il y a 8 emplacements DIMM par CPU, mais seulement 6 canaux par CPU – A1 et A2 sont sur le même canal et D1 et D2 sont sur le même canal. Par conséquent, si l'erreur provient de la banque de machines 13 ou 15, il ne sera pas possible d'identifier exactement le module DIMM défectueux si A2 et/ou D2 sont remplis.




```
Hardware event. This is not a software error.
MCE 3
CPU 15 BANK 17 (B)
MISC 908101011010086 ADDR 2bb4aab0c0
TIME 1632454812 Fri Sep 24 03:40:12 2021
MCG status:
MCi status:
Error overflow
Corrected error
MCi_MISC register valid
MCi_ADDR register valid
MCA: MEMORY CONTROLLER MS_CHANNEL2_ERR
Transaction: Memory scrubbing error
MemCtrl: Corrected patrol scrub error
STATUS cc001900000800c2 MCGSTATUS 0
MCGCAP f000c14 APICID 30 SOCKETID 1 (A)
CPUID Vendor Intel Family 6 Model 85
```

Annexe A: Liste d’acronymes

Tableau 24. Liste d’acronymes

Acronyme	Définition
ACPI	Interface avancée de configuration et de courant électrique
IA	Intelligence artificielle
API	Interface de programmation d'applications
ASIC	Circuit intégré spécifique
BIOS	Système d'entrée-sortie de base
BMC	Contrôleur de gestion de carte mère
BSP	Package de support de carte
CBIT	Test intégré continu
CE	Communauté européenne (marquage CE)
CLI	Interface de ligne de commande
CPU	Unité centrale de traitement
SCME	Serveurs de communication montables en étagère
CSA	Association canadienne de normalisation
CC	Courant continu
DDR4	Double débit de données 4
DHCP	Protocole de configuration dynamique des hôtes
DIMM	Module de mémoire à double rangée de connexions
DRAM	Mémoire vive dynamique
DTS	Capteur thermique numérique
DU	Unité distribuée
ECC	Code de correction d'erreurs
EEPROM	Mémoire morte effaçable et programmable électriquement
CEM	Compatibilité électromagnétique
EMI	Perturbation électromagnétique
ESD	Décharge électrostatique
ETSI	Institut européen des normes de télécommunication
ETSI	Institut européen des normes de télécommunication
eUSB	Bus série universel intégré
FCC	Federal Communications Commission
FH/FL	Pleine hauteur/pleine longueur
FPGA	Réseau prédiffusé programmable par l'utilisateur
FRU	Unité remplaçable par l'utilisateur
Gb	Gigabit
Go	Gigaoctet – 1024 Mo
GbE	Gigabit Ethernet
GPI	Entrée à usage général
GPIO	Entrée/sortie à usage général
GPO	Sortie à usage général
GPS	Système de localisation GPS
GPU	Processeur graphique

Acronyme	Définition
IUG	Interface utilisateur graphique
Disque dur	Disque dur
Hz	Hertz – 1 cycle/seconde
E/S	Entrée/sortie
Bus I2C	Bus de circuit inter-intégré
iBMC	Contrôleur de gestion de carte mère intégré
IEC	Commission électrotechnique internationale
IEEE	Institute of Electrical and Electronics Engineers
UMI	Unité de mesure inertielle
IOL	IPMI sur LAN
IPMB	Bus de gestion de plateforme intelligente
IPMI	Interface de gestion intelligente de matériel
IRQ	Ligne d'interruption
Ko	Kilo-octet – 1024 octets
KCS	Style de contrôleur de clavier
KEAPI	Interface de programmation d'applications emboitée de Kontron
KVM	Écran-clavier-souris
LAN	Réseau local
DEL	Diode électroluminescente
LP	Profil bas
LPC	Nombre de broches réduit
LVDS	SCSI différentiel à basse tension
TAM	Température ambiante maximale
Mo	Mégaoctet – 1024 Ko
MCU	Microcontrôleur
MEC	Informatique en périphérie multi-accès
MXM	Module PCI Express mobile
NCSI	Interface de services de communication réseau
NEBS	Système de construction d'équipement réseau
CIR	Carte d'interface réseau ou contrôleur d'interface réseau
NMI	Interruption non masquable
NOS	Système d'exploitation de réseau
NVMe	Mémoire non volatile express
OCXO	Oscillateur à quartz thermostaté
PCS	Protection contre la surchauffe
PBIT	Test intégré à la mise sous tension
PCH	Contrôleur de plateforme
PCI	Interconnexion de composants périphériques
PCIe	Interconnexion de composants périphériques express
PECI	Interface de contrôle de l'environnement de la plateforme
PIRQ	Ligne d’interruption PCI
PMbus	Bus de gestion de l'alimentation
PMM	Gestionnaire de mémoire POST

Acronyme	Définition
PnP	Prêt à l'emploi
POST	Auto-test de démarrage
PTP	Protocole de temps de précision
PXE	Environnement d'exécution avant démarrage
RAID	Réseau redondant de disques indépendants
RAN	Réseau d'accès radioélectrique
RAS	Fiabilité-disponibilité-facilité de service
RDIMM	Module de mémoire à double rangée de connexions avec registre
RDP	Protocole de bureau à distance
RMM	Module de gestion à distance
RoHS	Restriction de l'utilisation de certaines substances dangereuses
SAS	SCSI à attachement série
SATA	Attachement de technologie avancée en série
Mémoire SDRAM	Mémoire vive dynamique synchrone
SEL	Journal des événements système
SFP+	Émetteur-récepteur enfichable à faible encombrement qui supporte un débit allant jusqu'à 10,0 Gbps
SMBus	Bus de gestion système
SMS	Logiciel de gestion du système
SNMP	Protocole de gestion de réseau simple
SOC	Système sur puce
SOL	Série sur LAN
Disque SSD	Disque à circuits intégrés
SSH	Protocole Secure Shell
THOL	Liste du matériel et des systèmes d'exploitation testés
TPM	Module de plateforme sécurisée
TUV	Technischer Uberwachungs-Verein (laboratoire d'essais de sécurité dont le siège social est en Allemagne)
UART	Récepteur-émetteur universel asynchrone
UEFI	Interface micrologicielle extensible unifiée
UL	Underwriters' Laboratories, Inc.
USB	Bus série universel
ST	Sous-tension
V	Volt
VA	Voltampère (volts multipliés par des ampères)
VCA	Volt en courant alternatif
VCC	Volt en courant continu
VDE	Verband Deutscher Electrotechniker (Institut allemand des ingénieurs en électricité)
Carte VGA	Carte vidéographique
vRAN	Réseau d'accès radioélectrique virtualisé
W	Watt
DEEE	Déchet d’équipements électrique et électronique
Ω	Ohm

BUREAUX CHEFS

EUROPE, MOYEN-ORIENT ET AFRIQUE

Lise-Meitner-Str. 3-5
86156 Augsburg
Germany
Tél. : + 49 821 4086-0
Télec. : + 49 821 4086-111
info@kontron.com

AMÉRIQUE DU NORD

4555 Ambroise-afortune
Boisbriand, QC
Canada J7H 0A4
Tel.:+1 450 437-5682
Tel: +1 800-387-4223
info.americas@kontron.com

ASIE PACIFIQUE

1~2F, 10 Building, No. 8 Liangshuihe
2nd Street, Economical &
Technological Development Zone,
Beijing, 100176, P.R. China
Tél. : + 86 10 63751188
Télec. : + 86 10 83682438
info@kontron.cn