GUIDE D'UTILISATION

ME1310

kontron

Table des matières

Description du produit

ME1310 – serveur de périphérie flexible pour un déploiement rapide des services de télécommunication et 5G.

Le serveur de périphérie 1U haute performance ME1310 de Kontron est une unité distribuée conçue pour opérer dans de larges plages de température. Le ME1310 est utilisé pour les réseaux d'accès radioélectrique (RAN) ou l'informatique en périphérie multi-accès (MEC). Cette plateforme dispose de plus de cœurs, de plus de mémoire et d'une densité accrue.

Applications principales

- Résoudre les problèmes d'espace restreint et d'alimentation en permettant aux applications complexes d'être déployées plus près de la périphérie du réseau
- Diminuer l'encombrement du réseau et améliorer le rendement des applications en rapprochant le traitement des tâches de l'utilisateur
- Permettre le fonctionnement d'applications telles que les réseaux d'accès radioélectrique (RAN), l'intelligence artificielle, la mise en cache des données, la latence ultra-faible et les applications périphériques à haut taux de transfert

Caractéristiques principales

- Processeur Intel® Xeon® D de 3^{e} génération
- Deux emplacements d'extension PCIe pour l'accélération matérielle
- Commutateur Ethernet embarqué avec PTP/SyncE et maintien de synchronisation par OCXO
- Long cycle de vie
- Configuration en chaîne pour connecter plusieurs unités distribuées entre elles
- Compatible avec tous les principaux logiciels vRAN
- Alimentation CC ou AC
- Huit emplacements DIMM DDR4, 4 canaux à un maximum de 3200 MHz supportant jusqu'à 512 Go
- Option de stockage :
    - Deux M.2-2230 allant jusqu'à 512 Go chacun et deux M.2-2280 allant jusqu'à 2 To chacun (NVMe)
    - Quatre M.2-2230 allant jusqu'à 512 Go chacun (NVMe)

Historique des révisions

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

Garantie et soutien

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.

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.

Soutien à la clientèle

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

Pour obtenir des informations sur les ventes, y compris sur les options de produits actuelles et futures, veuillez contacter le soutien des ventes de Kontron au Canada par les moyens suivants :

- Par téléphone : 1-800-387-4222
- Par courriel : gss-com@kontron.com

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 www.kontron.com/support-and-services.

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

⚠CAUTION

Risque d'explosion si la pile est remplacée par un type inadéquat.

Se débarrasser des piles usées selon les instructions.

⚠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.

1.1.1 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.

1.1.2 Circulation d'air réduite

Lors de l'installation de ce produit dans une étagère, s’assurer de prévoir une circulation d'air adéquate pour un fonctionnement optimal. Les dégagements latéraux doivent être respectés.

1.1.3 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.

1.1.4 Marquage CE

Le marquage CE sur ce produit indique qu'il est conforme aux directives de l’Union européenne applicables : exigences en matière de basse tension, de CEM, d'équipements radioélectriques et de RoHS.

1.1.5 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.

Logo de la directive DEEE

1.2 Avertissements et précautions de sécurité d'ordre général relatifs à l’alimentation

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.

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

1.2.1 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.

1.2.2 Sécurité – blocs d'alimentation CC

Les plateformes équipées de blocs d'alimentation CC doivent être installées dans une zone d'accès restreint. 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 20 A. La source de courant continu doit être isolée électriquement de toute source de courant alternatif dangereuse par une isolation double ou renforcée.

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).

Toutes les conditions suivantes doivent être remplies :

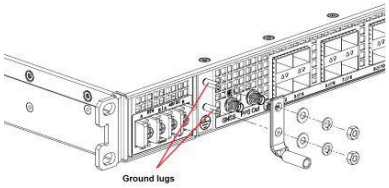
1. Cet équipement doit être raccordé directement au conducteur de mise à la terre du système d’alimentation CC ou à un conducteur de liaison provenant d’une barre ou d’un bus de mise à la terre auquel le conducteur de mise à la terre du système d’alimentation CC est raccordé.
2. Cet équipement doit être installé dans la même zone immédiate (par exemple dans des étagères adjacentes) que tout autre équipement qui comporte une connexion entre le conducteur mis à la terre du même circuit d’alimentation CC et le conducteur de mise à la terre, ainsi qu’au point de mise à la terre du système CC. Le système CC ne doit pas être mis à la terre ailleurs.

3. La source d'alimentation CC doit être située dans les mêmes locaux que cet équipement.
4. Aucun dispositif de commutation ou de sectionnement ne doit être installé dans le conducteur de circuit mis à la terre entre la source CC et le point de connexion du conducteur de l'électrode de mise à la terre.

1.2.3 Mise à la terre fiable

Toujours maintenir une mise à la terre fiable pour les équipements montés en étagère.

Emplacement de la cosse de mise à la terre



1.3 Spécifications réglementaires

警告 此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对干扰采取切实可行的措施。

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

1.3.1 Conformité en matière de sécurité

États-Unis/Canada	Ce produit porte la marque cCSAus.
Europe	Ce produit 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.

1.3.2 Compatibilité électromagnétique

États-	Ce produit est conforme à la norme FCC Part 15/ICES-003 Class A. Il est conçu pour répondre aux
Europe	Ce produit est conforme à la directive 2014/30/UE relative à la compatibilité électromagnétique et à la norme EN 300 386. La version GPS est conforme à la directive 2014/53/UE relative aux équipements radioélectriques, à la norme EN 301 489-1 et à la norme EN 303 413.
International	Ce produit est conforme à la Classe A de la norme CISPR 32 et à la norme CISPR 35.
Japon	Ce produit est conforme à la norme VCCI Classe A. Noter que pour le Japon l'entrée CA est de 90 à

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。
VCCI－A

2/ Aperçu

2.1 Spécifications

2.1.1 Principales caractéristiques matérielles du ME1310

Caractéristique	Description
Plateforme matérielle	• Serveur haute performance pour les réseaux d'accès radioélectrique (RAN) et l'informatique en périphérie multi-accès (MEC) • Montage en étagère (rack), hauteur 1U, profondeur de 13,5 pouces, largeur de 19 pouces • Accès par l'avant uniquement (E/S de la carte mère, bloc d'alimentation, E/S des cartes d'expansion PCIe)

E/S	• Deux ports USB 3.0
	• Un port de gestion RJ45 10/100/1000Base-T
	• Un port série RJ45
	• Un port d'entrée d'alarmes RJ45
	• Options du module d'E/S avec :
	  ○ Module de commutation (switch) Ethernet intégré à 12 ports (4x SFP28, 8x SFP+)
	  ○ Module de connexion directe avec quatre SFP28 25 GbE (Le développement de cette option est envisagé. Veuillez contacter le service des ventes de Kontron.)

Synchronisation	Avec l'option module d'E/S de commutation Ethernet : • Une entrée SMA d'antenne GNSS • Une sortie SMA de signal de synchronisation PPS
Carte d'expansion PCIe	• Deux cartes d'expansion PCIe x16 FHHL ou FH¾L optionnelles sont prises en charge (des restrictions thermiques et de puissance peuvent s'appliquer) • La puissance consommée maximale supportée est de 75 W par carte • PCIe 4.0 (16 GT/s) Voir Liste de compatibilité du matériel
CPU	La famille de processeurs Intel® Xeon® D-2700 est prise en charge, y compris les processeurs suivants : • Xeon® D-2796NT, 20 cœurs à 2,00 GHz avec QAT, 120 W • Xeon® D-2776NT, 16 cœurs à 2,10 GHz avec QAT, 117 W • Xeon® D-2776NT, 14 cœurs à 2,00 GHz avec QAT, 97 W
Stockage	Deux disques SSD M.2 : • PCIe 3.0 x4 NVMe • Types pris en charge : 2230 et 2280 Deux disques SSD M.2 : • PCIe 3.0 x2 NVMe • Types pris en charge : 2230 Voir Liste de compatibilité du matériel
Mémoire	DIMM DDR4 avec ECC • Taux de transfert allant jusqu'à 3 200 MT/s (la vitesse minimale de la mémoire prise en charge est de 2 400 MT/s) • Quatre canaux de mémoire • Deux emplacements DIMM par canal Voir Liste de compatibilité du matériel
Entrée d'alimentation	Une alimentation à double entrée de -57 VCC à -40 VCC ou Une alimentation à entrée unique de 90 VCA à 264 VCA 47/63 Hz
Puissance consommée	Voir Puissance consommée et budget énergétique
Ventilateurs	• Huit ventilateurs en configuration N+1 • Régulation automatique de la vitesse des ventilateurs
Supports pour montage en étagère	Montage frontal dans une étagère de 19 pouces de large

2.1.2 Principales caractéristiques logicielles du ME1310

Caractéristique	Description
Gestion de la plateforme	• BMC basé sur OpenBMC • UEFI basé sur AptioV d'AMI

Connectivité	• Interface LAN dédiée ou partagée (NC-SI)
	• Interface hôte LAN USB (pour Redfish)
	• Interface hôte IPMI (via KCS)
	• Gestion à distance
	  ○ Schéma Redfish 1.9 + 2020.1
	  ○ IPMI 2.0 RMCP+
	  ○ Interface utilisateur Web
	• Accès à distance
	  ○ KVM/VM
	  ○ Interface série sur IPMI et SSH

Surveillance et contrôle de l'alimentation	• Contrôle de l'alimentation
	  ○ Contrôle de l'alimentation
	  ○ État
	  ○ Forçage du périphérique de démarrage
	  ○ Refroidissement et chauffage
	• Surveillance
	  ○ Thermique
	  ○ Alimentation
	  ○ Humidité
	  ○ Surveillance des cartes/périphérique
	  ○ Alarmes de télécom
	• Journalisation et alertes (journaux et événements)

Configuration	• Gestion des utilisateurs (interne, LDAP)
	• Gestion des micrologiciels
	  ○ Version
	  ○ Mise à jour
	  ○ Validation des signatures
	  ○ Processus sans échec grâce à deux banques (disponible via Redfish et l'interface utilisateur Web)
	• Gestion du réseau (DHCP et statique, VLAN)

Sécurité	• Chiffrement (chiffrement des mots de passe, protocole de sécurité de la couche transport (TLS), IPMI Cipher 17) • Authentification (LDAP / Active Directory) • Signature des micrologiciels • Démarrage sécurisé • CSM (legacy) (disponible, mais désactivé par défaut)
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 processeur et de la mémoire

2.1.3 Dimensions physiques du ME1310

Châssis	Mesures (mm [po])	Notes
Profondeur	343 [13,5]	Châssis
Largeur	449 [17,6] max.	Châssis
	483 [19] max.	Largeur totale : supports de montage avant inclus (2 fois 17,2 mm [0,7 po])
	465 [18,3]	Entre les points de montage dans l'étagère
Hauteur	43,5 [1,7] max.	Châssis
Dégagement latéral	Aucune	
Dégagement avant	100 [4]	Recommandé
Dégagement arrière	70 [2,8]	

2.1.4 Dimensions physiques de l'emballage du ME1310

Profondeur (mm [po])	Largeur (mm [po])	Hauteur (mm [po])
489 [19,25]	571,5 [22,5]	190,5 [7,5]

2.1.5 Poids à l'expédition du ME1310

Composant	Poids (kg [lb])
Poids du système avec un bloc d'alimentation CA – avec quatre DIMM et un disque SSD M.2-2280	6,93 [15,3]
Poids du système avec un bloc d'alimentation CC – avec quatre DIMM et un disque SSD M.2-2280	6,79 [15,0]
Emballage (boîte + mousse + sac)	1,59 [3,5]

2.1.6 Spécifications environnementales du ME1310

Environnement	Spécifications
Température, en fonctionnement	**Alimentation CC :** -40 °C à +65 °C (-40 °F à +149 °F) **Alimentation CA :** -5 °C à +50 °C (23 °F à +122 °F) La défaillance d'un ventilateur n'aura pas d'incidence sur le fonctionnement pendant au moins 4 heures à 65 °C. Certaines limites peuvent s'appliquer. Ces limites peuvent être dues à la plage de température de fonctionnement des composants configurables installés (ex. module SFP, disque SSD et carte d'expansion PCIe). Kontron prend uniquement en charge l'utilisation de modules SFP28/SFP+/SFP et de disques SSD conçus pour une plage de température de fonctionnement industrielle (-40 °C à +85 °C).
Température, hors fonctionnement	-40 °C à +70 °C (-40 °F à +158 °F)
Humidité, en fonctionnement	5 % à 95 %, sans condensation
Altitude/pression, en fonctionnement	-60 m à 1 800 m d'altitude sans déclassement thermique Jusqu'à 4 000 m d'altitude avec un déclassement thermique de 1 degré Celsius par 300 m au-dessus de 1 800 m
Altitude/pression, hors fonctionnement	Jusqu'à 4 570 m
Vibrations, en fonctionnement	Ce produit est conforme aux normes en matière de vibrations aléatoires en fonctionnement. Profil d'essai basé sur ETSI EN 300 019-2-3 class 3.2 • 5 Hz à 10 Hz à +12 dB/octave (pente ascendante) • 10 Hz à 50 Hz à 0,02 m2/s3 (0,0002 g^2/Hz) (plat) • 50 Hz à 100 Hz à -12 dB/octave (pente descendante) • 30 minutes pour chacun des trois axes

Environnement	Spécifications
Vibrations, hors fonctionnement	Ce produit est conforme aux normes en matière de vibrations aléatoires lors du transport et du stockage. Profil d'essai basé sur GR-63, clause 5.4.3 et ETSI EN 300 019-2-2 class 2.3 • 5 Hz à 20 Hz à 1 m2/s3 (0,01 g^2/Hz) (plat) • 20 Hz à 200 Hz à -3 dB/octave (pente descendante) • 30 minutes pour chacun des trois axes
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 • 11 ms demi-sinusoïdales, 3 g, trois chocs dans chaque direction
Chute libre	Ce produit est conforme à la norme GR-63, section 5.3 de Bellcore. Emballé = 1 000 mm, six surfaces, trois bords et quatre coins Non emballé = 100 mm, deux côtés et deux coins inférieurs
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.
RoHS et DEEE	Ce produit est conçu pour répondre à la norme RoHS Chine Phase 1 (autodéclaration et étiquetage). Ce produit est conforme à la directive européenne 2012/19/UE (DEEE). Ce produit est conforme à la directive RoHS 2011/65/UE telle que modifiée par l'UE 2015/863.

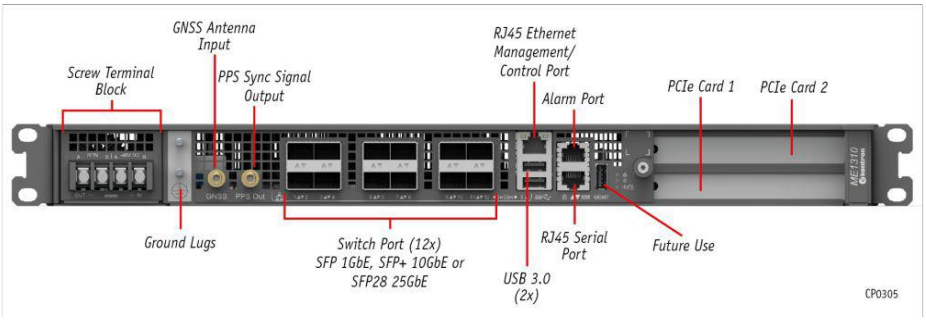
2.2 Composants de la plateforme

2.2.1 Panneau avant de la plateforme

La plateforme ME1310 est offerte avec un bloc d'alimentation CC ou CA. Pour simplifier la documentation, seule la version CC est illustrée ici. Pour de l'information sur le brochage des composants, voir Brochage et caractéristiques électriques des connecteurs.

Pour de l'information sur le câblage, voir Câblage.

2.2.1.1 Option module d'E/S de commutation Ethernet

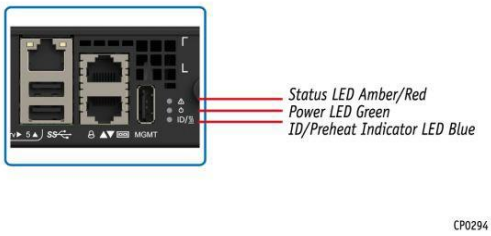


2.2.1.2 Option module d'E/S de connexion directe

Le développement de cette option est envisagé. Veuillez contacter le service des ventes de Kontron.

2.2.2 DEL de la plateforme

2.2.2.1 DEL générales de la plateforme



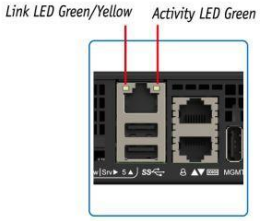
Condition (ambre/rouge)	État
Éteint	Aucune notification d'erreur active (fonctionnement normal)
Ambre allumé	Alarme majeure active
Rouge allumé	Alarme critique active (service/entretien requis)

Indicateur d'ID/préchauffage (bleu)	Alimentation (vert)	État
Éteint	Éteint	Les deux entrées d'alimentation sont HORS TENSION ou hors de la plage de fonctionnement normal
Allumé	Éteint	Une entrée d'alimentation ou les deux sont SOUS TENSION – État logiciel éteint ACPI (S5)
Clignotement lent	Éteint	Préchauffage de la plateforme avant l'activation du serveur
Clignotement normal	Toutes les conditions	Le BMC exécute une demande d'identification
Éteint	Clignotement rapide	Activation du processeur du serveur terminée et en cours d'exécution – État alimenté ACPI (S0)
Éteint	Clignotement normal	L'UEFI/BIOS a démarré le POST
Éteint	Clignotement normal ou allumé[1]	Transfert de l'UEFI/BIOS au chargeur de démarrage du système d'exploitation
Éteint	Allumé[1]	Application démarrée/en cours d'exécution OK

[1] Par défaut, la DEL d'alimentation clignote normalement jusqu'à ce que l'application du client confirme qu'elle fonctionne en activant un bit du registre d'E/S. Grâce à un réglage UEFI/BIOS, la DEL d'alimentation peut être réglée afin de rester allumée après le POST (avant le démarrage du système d'exploitation ou de l'application), mais le réglage UEFI/BIOS par défaut laisse cette tâche à l'application. Voir Configurer l'option Application Ready LED dans la section Configuration des options UEFI/BIOS pour configurer l'option UEFI/BIOS appropriée et Ressources de la plateforme destinées à l'application client pour voir un exemple de script à intégrer dans l'application.

- Clignotement lent : 1 impulsion courte toutes les 2 secondes
- Clignotement normal : 1 impulsion par seconde
- Clignotement rapide : 2 impulsions par seconde

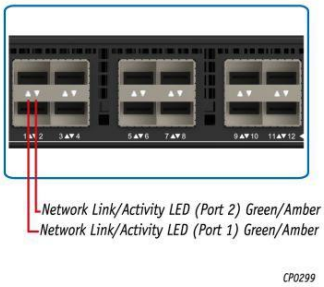
2.2.2.2 DEL du port réseau Srv 5



Liaison (gauche – vert/jaune)	Activité (droite – vert)	État
Éteint	Éteint	Aucune liaison
Éteint	Allumé (pas d'activité) Clignotement (activité)	Liaison 10Base-T établie
Jaune allumé	Allumé (pas d'activité) Clignotement (activité)	Liaison 100Base-TX établie
Vert allumé	Allumé (pas d'activité) Clignotement (activité)	Liaison 1000Base-T établie

2.2.2.3 DEL des ports réseau du module d’E/S

2.2.2.3.1 Module de commutation Ethernet



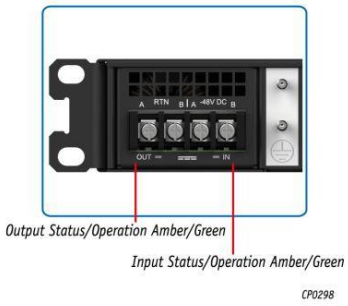
Liaison/activité réseau (vert/ambre)	État
Vert allumé	Liaison établie à la vitesse maximale du port (10 ou 25 Gbps), pas d'activité
Ambre allumé	Liaison établie à une vitesse inférieure à la vitesse maximale du port (ex. la liaison est à 1 Gbps sur un port à 10 Gpbs), pas d’activité
Clignotement (vert ou ambre en fonction de la vitesse du port)	Activité
Éteint	Aucune liaison

2.2.2.3.2 Module de connexion directe

Le développement de cette option est envisagé. Veuillez contacter le service des ventes de Kontron.

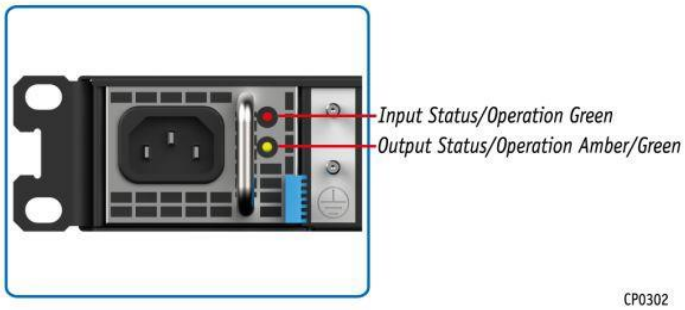
2.2.2.4 DEL du bloc d'alimentation

2.2.2.4.1 Alimentation CC



État/fonctionnement de la sortie (ambre/vert)	État
Éteint	Contrôleur d'alimentation désactivé
Ambre allumé	Temps de maintien insuffisant ou tension trop basse pour le démarrage
Vert allumé	Maintien de tension prêt
État/fonctionnement de l'entrée (ambre/vert)	**État**
Éteint	Pas de 48 V
Ambre allumé	Contrôleur d'alimentation désactivé (tension d'entrée faible ou défaillance)
Vert allumé	Contrôleur d'alimentation activé

2.2.2.4.2 Alimentation CC



État/fonctionnement de l'entrée (vert)	État
Allumé	Tension d'entrée dans la plage normale spécifiée
Clignotement	Tension d'entrée en fonctionnement en : 1) alarme de surtension, ou 2) alarme de sous-tension
Éteint	Tension d'entrée en fonctionnement : 1) au-dessus de la plage de surtension, ou 2) en dessous de la plage de sous-tension, ou 3) non présente
État/fonctionnement de la sortie (ambre/vert)	État
Vert allumé	Alimentation en mode bon fonctionnement : Tension de sortie principale et tension de veille activées sans défaillance ou avertissement associé au bloc d'alimentation détecté
Clignotement vert	Mode veille : Tension de veille activée sans avertissement associé au bloc d'alimentation ou de défaillance détecté
Clignotement ambre	Mode d'avertissement : Avertissement associé au bloc d'alimentation détecté selon les octets rapportant le statut « STATUS_X » du PMbus
Ambre allumé	Mode de défaillance : Défaillance associée au bloc d'alimentation détectée selon les octets rapportant le statut « STATUS_X » du PMbus

2.2.3 Ventilateurs de la plateforme

La plateforme comporte 8 ventilateurs.

Voir Installation et assemblage des composants pour savoir comment remplacer un ventilateur.

2.2.4 Étiquette de la plateforme

La plateforme possède une étiquette de fabrication et une étiquette avec un code QR.

L'étiquette de fabrication inclut ce qui suit :

- Numéro de pièce
- Description du produit, y compris les options configurables
- Numéro du lot de fabrication

Voici un exemple de ce qui pourrait être affiché :

Kontron part # = 1069-1291

Kontron product name = ME1210BX-BCDDBXX

ZZXX1234HH (XX) = 01A0001100

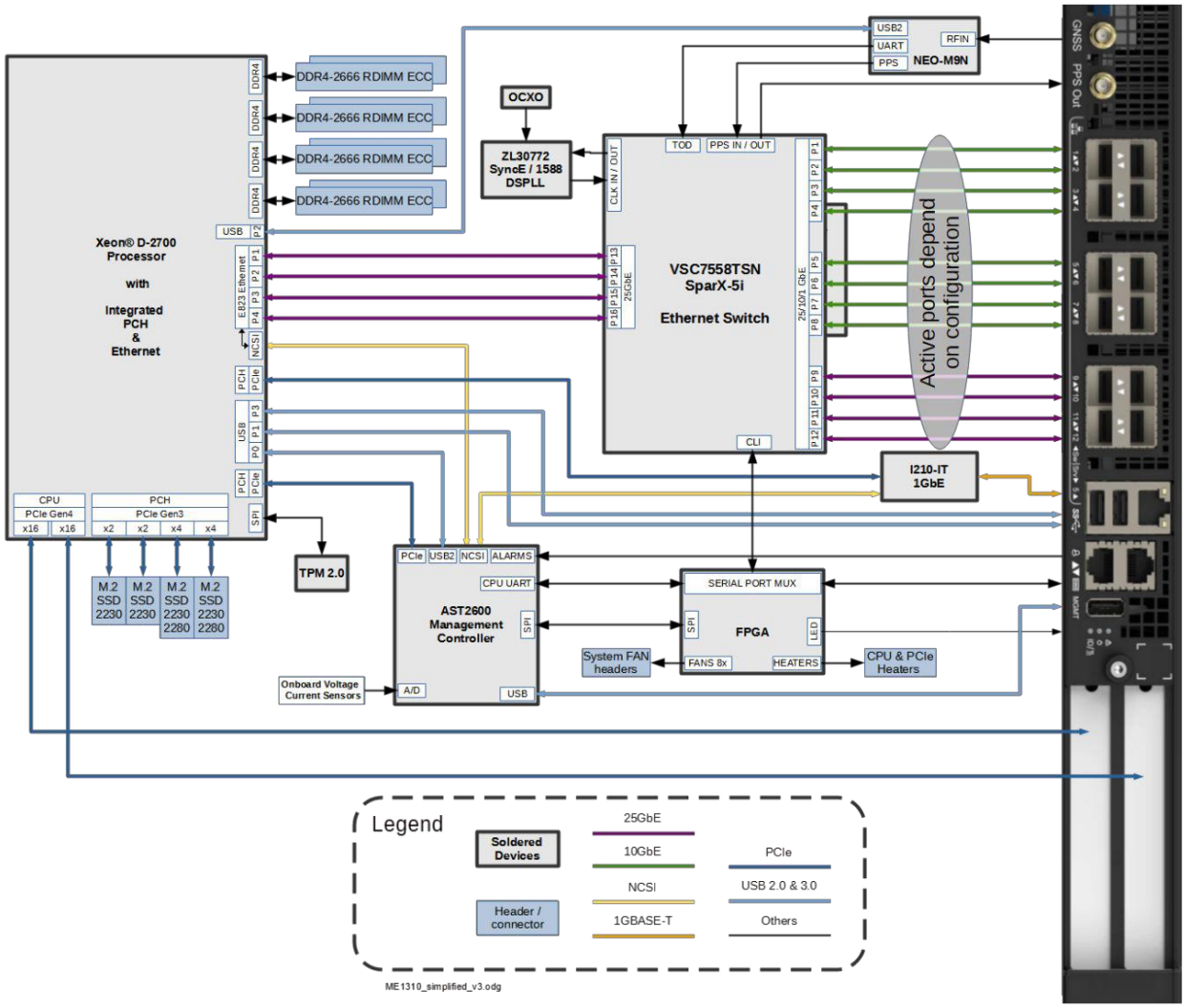
Section pertinente :

Adresses MAC (pour l'information fournie par code QR, qui inclut le numéro de série)

2.3 Architecture du produit

2.3.1 Schémas fonctionnels

2.3.1.1 Schéma fonctionnel avec l'option module d'E/S de commutation Ethernet



2.3.1.2 Schéma fonctionnel avec l'option module d'E/S de connexion directe

Le développement de cette option est envisagé. Veuillez contacter le service des ventes de Kontron.

2.3.2 Couches réseau

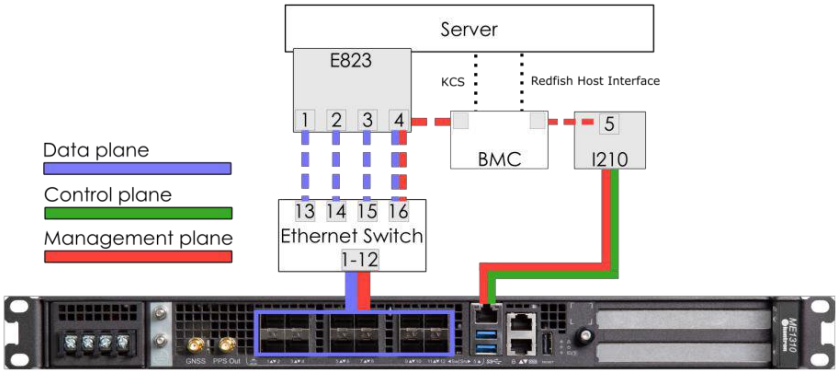
La plateforme ME1310 comprend :

- 3 couches réseau (couche de gestion, couche de contrôle, couche des données)

Couches réseau	Description	Vitesse (GbE)	Accès aux composants
Couche de gestion	La couche de gestion achemine le trafic administratif de la plateforme. Cette couche est utilisée 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
Couche de contrôle	La couche de contrôle achemine le trafic de signalisation de l'application client. Cette couche est utilisée pour contrôler les applications clients.	1	Serveur
Couche des données	La couche des données achemine le trafic des applications clients. Cette couche est utilisée pour fournir des services aux utilisateurs finaux.	1/10/25	Serveur, BMC, NOS

2.3.3 Connexions internes

2.3.3.1 Connexions internes avec l'option module d'E/S de commutation Ethernet



2.3.3.2 Connexions internes avec l'option module d'E/S de connexion directe

Le développement de cette option est envisagé. Veuillez contacter le service des ventes de Kontron.

2.4 Description des méthodes d'accès au système

Pour configurer, surveiller et dépanner la plateforme ME1310 et ses composants, plusieurs interfaces peuvent être utilisées :

- **Interface de gestion (BMC) –** via la couche de gestion et la couche des données de la plateforme
- **Système d'exploitation –** via la couche de gestion, la couche de contrôle, la couche des données ou le port série de la plateforme
- **UEFI/BIOS –** via la couche de gestion ou le port série de la plateforme
- **Système d'exploitation réseau (NOS) du commutateur** (sur les plateformes équipées du module d'E/S de commutation Ethernet) – via la couche de gestion et la couche des données

2.4.1 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.

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 de la couche de gestion du BMC.	• Contrôle et surveillance à distance du serveur • Accès vidéo au système d'exploitation • Mises à niveau des micrologiciels
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 de la couche de gestion du BMC, et localement à partir du système d'exploitation du serveur via l'interface hôte Redfish.	• Surveillance à distance du serveur • Contrôle à distance du serveur • 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 de la couche de gestion du BMC.	• Contrôle et surveillance à distance du serveur
IPMI via KCS Accessible localement à partir du système d'exploitation du serveur.	• Accès local au BMC à partir du système d'exploitation pour la surveillance du serveur • Configuration initiale du BMC

2.4.2 Méthodes d'accès au système d'exploitation

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

Méthodes d'accès au système d'exploitation	
Description de la méthode	Principales raisons de l'utiliser
KVM Il s'agit de la méthode recommandée pour la configuration initiale d'un système sorti de son emballage. Méthode sans échec* pour accéder au serveur si un composant (système d'exploitation, UEFI/BIOS, etc.) est mal configuré. Accessible à partir de la couche de gestion du BMC.	• Installation initiale du système d'exploitation • Configuration de l'interface réseau du système d'exploitation • Accès vidéo au système d'exploitation • Accès à distance au système d'exploitation • Incapacité d'établir une session réseau sur le système d'exploitation

Méthodes d'accès au système d'exploitation	
Description de la méthode	Principales raisons de l'utiliser
Série sur LAN en utilisant l'interface utilisateur Web Méthode sans échec* pour accéder au serveur si un composant (système d'exploitation, UEFI/BIOS, etc.) est mal configuré. Accessible à partir de la couche de gestion du BMC.	• Configuration de l'interface réseau du système d'exploitation • Incapacité d'établir une session réseau sur le système d'exploitation • Accès à la console série du système d'exploitation
Série sur LAN en utilisant SSH à partir d'un ordinateur distant Accessible à partir de la couche de gestion du BMC.	• Configuration de l'interface réseau du système d'exploitation • Incapacité d'établir une session réseau sur le système d'exploitation • Accès à la console série du système d'exploitation
Série sur LAN via IPMI à partir d'un ordinateur distant Accessible à partir de la couche de gestion du BMC.	• Configuration de l'interface réseau du système d'exploitation • Incapacité d'établir une session réseau sur le système d'exploitation • Accès à la console série du 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 via la couche de contrôle et la couche des données.	• Faire fonctionner la plateforme dans des conditions normales • Accès à distance au système d'exploitation
Console série (connexion physique) Méthode sans échec pour accéder à tous les composants du serveur (système d'exploitation, BMC, UEFI/BIOS, etc.) 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 le BMC • Dépannage

* Noter que la communication avec la couche de gestion du BMC via le commutateur intégré peut être perdue en raison de configurations appliquées dans le NOS.

2.4.3 Méthodes d'accès à l'UEFI/BIOS

Pour accéder à l'UEFI/BIOS par l'une des méthodes, voir Accéder à l'UEFI/BIOS.

Méthodes d'accès à l'UEFI/BIOS	
Description de la méthode	Principales raisons de l'utiliser
Série sur LAN en utilisant l'interface utilisateur Web Il s'agit de la méthode recommandée pour la configuration initiale d'un système sorti de son emballage. Méthode sans échec* pour accéder au serveur si un composant (système d'exploitation, UEFI/BIOS, etc.) est mal configuré. Accessible à partir de la couche de gestion du BMC.	• Configuration initiale de l'UEFI/BIOS • Accès vidéo à l'UEFI/BIOS
KVM Méthode sans échec* pour accéder au serveur si un composant (système d'exploitation, UEFI/BIOS, etc.) est mal configuré. Accessible à partir de la couche de gestion du BMC.	• Configuration initiale de l'UEFI/BIOS • Accès vidéo à l'UEFI/BIOS
Série sur LAN en utilisant SSH à partir d'un ordinateur distant	• Configuration initiale de

Méthodes d’accès à l’UEFI/BIOS	
Description de la méthode	Principales raisons de l’utiliser
Accessible à partir de la couche de gestion du BMC.	l’UEFI/BIOS • Accès à la console série de l’UEFI/BIOS • Interfaces réseau du système d'exploitation non configurées, mais accès au réseau du BMC disponible
Série sur LAN via IPMI à partir d'un ordinateur distant Accessible à partir de la couche de gestion du BMC.	• Configuration initiale de l’UEFI/BIOS • Accès à la console série de l’UEFI/BIOS • Interfaces réseau du système d'exploitation non configurées, mais accès au réseau du BMC disponible
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 de la couche de gestion du BMC, et localement à partir du système d'exploitation du serveur via l'interface hôte Redfish.	• Configuration de base de l’UEFI/BIOS
Console série (connexion physique) Méthode sans échec pour accéder à tous les composants du serveur (système d’exploitation, BMC, UEFI/BIOS, etc.) s’ils sont mal configurés. Accessible à partir du port physique.	• Configuration initiale de l’UEFI/BIOS • Aucune configuration n'est effectuée sur le BMC • Dépannage

* Noter que la communication avec la couche de gestion du BMC via le commutateur intégré peut être perdue en raison de configurations appliquées dans le NOS.

2.4.4 Méthodes d'accès au système d'exploitation réseau (NOS) du commutateur

Pour accéder au système d'exploitation réseau du commutateur par l'une des méthodes, voir Accéder au NOS.

Méthodes d'accès au système d'exploitation réseau (NOS) du commutateur	
Description de la méthode	Principales raisons de l’utiliser
Interface utilisateur Web du NOS Il s’agit de la méthode recommandée pour la configuration initiale d'un système sorti de son emballage. Accessible à partir de la couche des données.	• Contrôle et surveillance du NOS • Mises à niveau des micrologiciels
Série sur LAN en utilisant l’interface utilisateur Web du BMC Accessible à partir de la couche de gestion du BMC.	• Configuration de l'interface réseau du NOS • Configuration initiale du NOS
Série sur LAN en utilisant SSH à partir d'un ordinateur distant Accessible à partir de la couche de gestion du BMC.	• Configuration de l'interface réseau du NOS • Configuration initiale du NOS
SSH à partir d'un ordinateur distant 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 de la couche des données.	• Contrôle et surveillance du NOS • Mises à niveau des micrologiciels
SSH à partir du serveur intégré Accessible localement à partir du système d'exploitation du serveur.	• Accès local au NOS pour le contrôle et la surveillance

2.4.5 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.

3/ Planification

3.1 Considérations environnementales

La plateforme ME1310 a été conçue pour fonctionner dans une plage de température étendue de -40 °C à +65 °C (-40 °F à +149 °F) avec un bloc d'alimentation CC ou de -5 °C à +50 °C (23 °F à +122 °F) avec un bloc d'alimentation CA et pour résister à des taux d'humidité sans condensation allant jusqu'à 95 %. Cet équipement ne doit pas être exposé directement aux éléments (soleil, pluie, vent, poussière). Pour les installations extérieures ou dans d'autres environnements difficiles et non contrôlés, un cabinet approprié doit être utilisé.

Si des composants qui ne supportent pas la plage de température du ME1310 sont installés, le client est responsable de configurer les seuils des capteurs et la gestion thermique en conséquence. Voir Configurer les capteurs et les paramètres thermiques et Refroidissement et gestion thermique de la plateforme.

Lorsque le ME1310 est démarré à l'extrémité inférieure de la plage de température étendue, il est normal que le système prenne un certain temps de préchauffage avant de terminer la séquence de démarrage initiale. Une fois démarré et en fonctionnement, le système dissipe suffisamment d'énergie pour rester chaud. Il est très rare que la plateforme nécessite un long préchauffage visant à pallier des conditions très froides. Cet événement ne survient que très rarement et se produit uniquement lors du démarrage initial ou après une panne de courant dans un environnement froid.

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'intérieur 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.

Si la plateforme est installée dans un environnement chaud, 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.

La plateforme ME1310 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.

3.2 Puissance consommée et budget énergétique

3.2.1 Exigences en matière de courant et de tension d'entrée – bloc d'alimentation CC

Section pertinente :

Câblage

Connecteur homologue : Voir Câblage pour fabriquer les câbles appropriés.

Description :

L'entrée d'alimentation CC est conçue conformément aux normes Telcordia GR-1089 et ATIS-0600315 et présente les caractéristiques suivantes :

- Entrées d'alimentation redondantes (avec diodes OR-ing actives)
- Plage de tension de fonctionnement en courant continu de -40,0 V à -56,7 V
- Fusibles internes (30 A sur RTN_A et RTN_B; 25 A sur -48V_A, -48V_B)
- Protection contre l'appel de courant transitoire et les surintensités grâce à un contrôleur d'alimentation
- Protection contre les surtensions (IEC 61000-4-5 class 2, 1 kV)

NOTICE

L'interface d'alimentation CC est protégée contre les surtensions et la longueur du câble n'est pas limitée à 6 mètres. Cette interface convient à une connexion aux systèmes locaux d'alimentation CC (GR-1089 type 8) et à une alimentation CC à l'intérieur d'un site cellulaire, avec exposition limitée à l'extérieur (type 8b).

3.2.2 Exigences en matière de courant et de tension d'entrée – bloc d'alimentation CA

Tension d'entrée CA	
Nominal	115/230 VCA
Minimum	90 VCA
Maximum	264 VCA
Courant d'entrée CA	
Maximum	8,5 Arms à 90 VCA
Entrée d’alimentation	
Maximum	700 W

3.2.3 Exemples de puissance consommée

Cette section présente les valeurs de puissance consommée obtenues dans un environnement de test. Les valeurs réelles dépendent grandement de l'application qui sera utilisée. Les valeurs fournies ne doivent donc être utilisées qu'à titre de référence générale, et des tests doivent être effectués avec la configuration matérielle et l'application réelles qui seront utilisées.

3.2.3.1 Puissance consommée par le système

La configuration suivante du ME1310 a été utilisée pour obtenir les valeurs typiques de puissance consommée indiquées dans le tableau ci-dessous :

- Processeur Xeon® D-2796NT
- Module d'E/S de commutation Ethernet avec OCXO standard
  Huit LRDIMM 64 Go
- Un module SATA M.2 128 Go
- Deux modules SFP28 25GBASE-LR
- Deux modules SFP+ 10GBASE-SR
- Deux cartes d'expansion PCIe : gabarits de tests de puissance de 75 W
- Bloc d'alimentation CC
- 8 ventilateurs standards

État	Consommation typique (W)	Notes
Sans activité	78	La puissance consommée à l’état sans activité a été mesurée avec CentOS 7 une fois le démarrage de la plateforme terminé
Application au maximum	342	La puissance maximale a été mesurée avec CentOS 7 qui exécutait « mprime -t » en tant qu’application de test de stress
Ventilateurs et application au maximum	500	La puissance maximale a été mesurée avec CentOS 7 qui exécutait « mprime -t » en tant qu’application de test de stress et les ventilateurs à vitesse maximale

NOTE :

- La tension d’entrée de l'alimentation CC est à -48 VDC.
- Le test a été effectué à température ambiante. La puissance consommée a varié au cours du test.
- La puissance consommée a été mesurée à l'entrée de l'alimentation CC.

3.2.3.2 Exemples de puissance consommée par les composants

Les puissances indiquées par composant dans le tableau ont été mesurées à la sortie de l'alimentation CC (côté 12 V). Ils ne tiennent donc pas compte du rendement d’efficacité du bloc d'alimentation. La puissance à l'entrée de l'alimentation CC (côté 48 V) est typiquement supérieure de 5 %.

Composants	Consommation typique (W)	Notes
Intel® Xeon® D-2796NT	120	TDP
Intel® Xeon® D-2776NT	117	TDP
Intel® Xeon® D-2766NT	97	TDP
Module d'E/S de commutation Ethernet avec OCXO standard	23	Le commutateur Ethernet dispose de 4 interfaces SFP avec liaison établie
Ventilateurs	23	À vitesse maximale
LRDIMM 64 Go	6	En utilisation active
RDIMM 16 Go	3,5	En utilisation active
Disque SSD NVMe M.2 de 128 Go, 512 Go, 1 To ou 2 To	7	En utilisation active. La puissance à l’état sans activité est de 1 W.
SFP28 25GBASE-LR	1	La liaison est établie avec l’appareil partenaire
SFP+ 10GBASE-SR	1	La liaison est établie avec l’appareil partenaire

NOTICE

Si tous les composants optionnels sont utilisés et fonctionnent à la puissance maximale, le système pourrait dépasser sa puissance maximale.

3.3 Adresses MAC

Section pertinente :

Architecture du produit

3.3.1 Option module d'E/S de commutation Ethernet

Adresse MAC	Description de l'interface	Composant	Note
MAC_BASE	Panneau avant Srv 5	BMC	Connecteur partagé avec le serveur.
MAC_BASE + 1	Port interne du serveur 4	BMC	Interface interne 1/16 du commutateur. Connexion partagée avec le serveur.
MAC_BASE + 2	Interface hôte Redfish du serveur	Serveur	Interface interne du BMC via une interface USB vers LAN intégrée.
MAC_BASE + 3	Port interne du serveur 1	Serveur	Interface interne 1/13 du commutateur.
MAC_BASE + 4	Port interne du serveur 2	Serveur	Interface interne 1/14 du commutateur.
MAC_BASE + 5	Port interne du serveur 3	Serveur	Interface interne 1/15 du commutateur.
MAC_BASE + 6	Port interne du serveur 4	Serveur	Interne à l'interface de commutation 1/16. Connexion partagée avec le BMC.
MAC_BASE + 7	Panneau avant Srv 5	Serveur	Couche de contrôle du serveur. Connexion partagée avec le BMC.
SW_MAC_BASE	N’importe quelle interface du commutateur	NOS	Adresse MAC utilisée par le système d'exploitation réseau du commutateur pour l'accès à la configuration/surveillance.
SW_MAC_BASE + 1 à SW_MAC_BASE + 17	Réservé	NOS	Adresse MAC réservée pour le système d'exploitation réseau du commutateur.

3.3.2 Option module d'E/S de connexion directe

Le développement de cette option est envisagé. Veuillez contacter le service des ventes de Kontron.

3.3.3 Découvrir les adresses MAC de la plateforme

Les adresses MAC de la plateforme peuvent être découvertes :

- En utilisant le code QR
- En utilisant l’UEFI/BIOS

3.3.3.1 Découvrir une adresse MAC en utilisant le code QR

Étape_1	À l'aide d'une application de code QR, scanner le code QR de la plateforme. Enregistrer les informations obtenues dans votre appareil (par exemple en faisant une capture d'écran). S/N:9017020001 = Numéro de série de la plateforme P/N:1065-2823 = Numéro de pièce de la plateforme BATCH:0A00000001 = Numéro de lot de production de la plateforme MAC : 00A0A5D6402A = Première adresse MAC attribuée au BMC/serveur. Valeur à utiliser pour remplacer MAC_BASE. 00A0A5E1B934 = Première adresse MAC attribuée au commutateur Ethernet intégré. Valeur à utiliser pour remplacer SW_MAC_BASE. Cette information n'est présente que pour une plateforme configurée avec le module d'E/S de commutation Ethernet.	S/N:9017020001 P/N:1065-2823 BATCH:0A00000001 MAC: 00A0A5D6402A 00A0A5E1B934

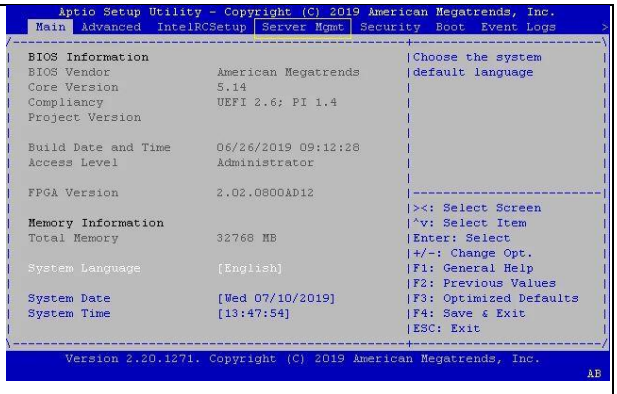
3.3.3.2 Découvrir une adresse MAC en utilisant l'UEFI/BIOS

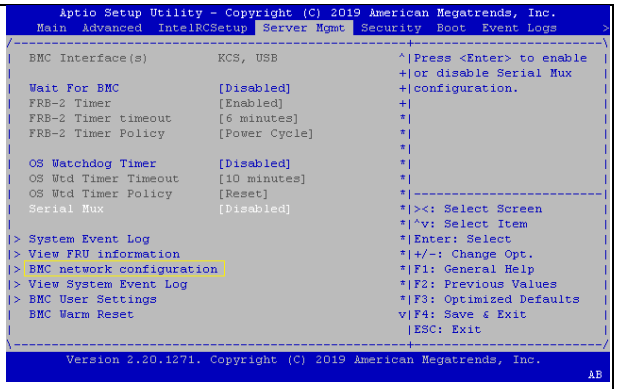
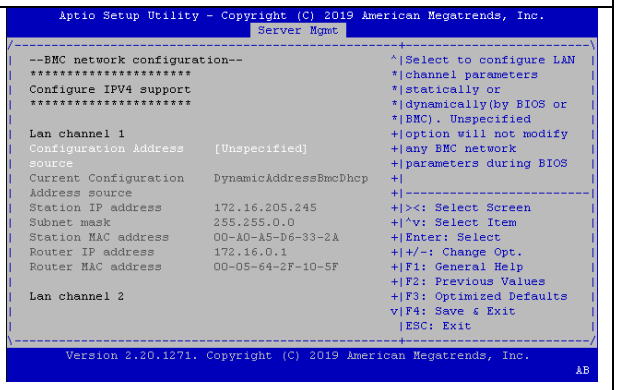
3.3.3.2.1 Préalables

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 : Aucune • Mode émulation recommandé : VT100+ **NOTE :** PuTTY est recommandé.

3.3.3.2.2 Accéder au menu BMC network configuration

Voir Accéder à l'UEFI/BIOS pour les instructions d'accès.

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.	

3.4 Mappage PCI

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**.

3.5 Brochage et caractéristiques électriques des connecteurs

Les clients peuvent fabriquer des câbles personnalisés sur la base des informations fournies dans cette section.

Sections pertinentes :

Composants de la plateforme

Câblage

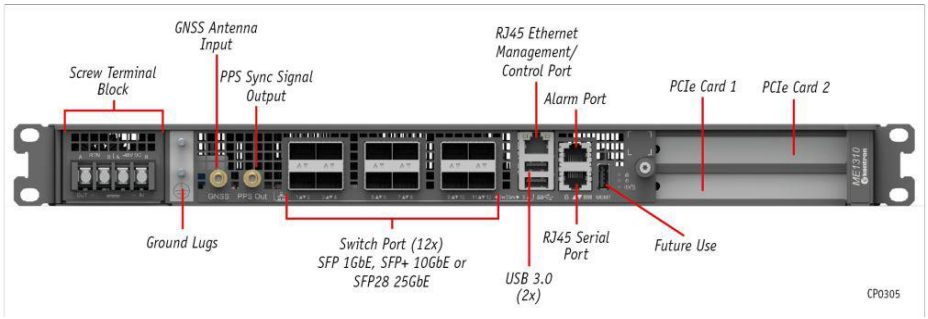
Tous les connecteurs et interfaces sont protégés contre les décharges électrostatiques (ESD) (IEC 61000-4-2, 15 kV (air), 8 kV (décharge)), sauf indication contraire.

NOTICE

Tous les connecteurs et interfaces sont prévus pour une connexion courte (moins de 6 mètres) à l'intérieur d'une même armoire, sauf indication contraire.

3.5.1 Connecteurs externes de la plateforme

3.5.1.1 Option module d'E/S de commutation Ethernet



3.5.1.2 Option module d'E/S de connexion directe

Le développement de cette option est envisagé. Veuillez contacter le service des ventes de Kontron.

3.5.2 Description, brochage et caractéristiques électriques des connecteurs externes

Cette section décrit les connecteurs suivants et présente leur brochage et leurs caractéristiques électriques :

- Entrée RF SMA GNSS – disponible uniquement sur les plateformes équipées du module d'E/S de commutation Ethernet
- Sortie SMA PPS – disponible uniquement sur les plateformes équipées du module d'E/S de commutation Ethernet
- Port d’alarmes RJ45
- Port série RJ45
- Ports SFP, SFP+ et SFP28
- Port de gestion Ethernet RJ45
- Interfaces USB
- Connecteur d’entrée du bloc d'alimentation CC
- Connecteur d’entrée du bloc d'alimentation CA

3.5.2.1 Entrée RF SMA GNSS

Connecteur homologue : SMA mâle

Description :

- Entrée d'antenne pour le module GNSS NEO-M9N intégré
- Peut être utilisé avec des antennes passives et actives (l'antenne doit être adaptée aux 50 ohms requis) Convient pour la connexion à des antennes extérieures externes
- Entrée RF
    - Puissance d'entrée maximale < 0 dBm
    - Bonne antenne avec gain > 4 dBic recommandée
    - Bon amplificateur à faible bruit (LNA) avec un facteur de bruit inférieur à 2 dB recommandé
    - Gain d'antenne active de 15 à 35 dB (maximum) recommandé
- Sortie de polarisation continue
    - 5 V ± 5 %
    - Jusqu'à 150 mA
    - Protection contre les surintensités (< 350 mA)
    - Protection thermique
- Protection contre les surtensions (IEC 61000-4-5 class 2, 1 kV)

Section pertinente :

Câblage

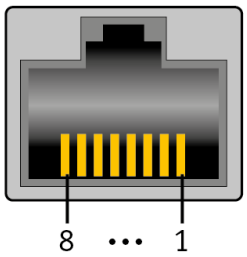
3.5.2.2 Sortie SMA PPS

Connecteur homologue : SMA mâle

Description :

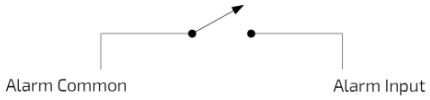
- Conforme à la norme ITU-G.703, section 19.2
- La sortie est une source de 3,3 V terminée (50 ohms)
- Le facteur d'utilisation de la sortie est de 10 % (100 ms)
- Convient à une utilisation avec des charges non terminées :
    - V_{OH} > 2,6 V à I_{OH} = -12 mA
    - V_{OL} < 0,7 V à I_{OH} = 12 mA
- Convient à une utilisation avec des charges terminées de 50 ohms à la masse :
    - V_{OH} > 1,2 V
    - V_{OL} < 0,3 V
- Front montant du signal PPS (au SMA) aligné à ± 5 ns du compteur ToD interne

3.5.2.3 Port d’alarmes RJ45



Description :

Le port d'alarmes est destiné à être utilisé uniquement avec des contacts secs normalement fermés. Il utilise un tampon RS-232 pour son interface électrique et est donc entièrement protégé contre les courts-circuits.



Tension en circuit ouvert :

- ALARM_CM : 5 V à 7 V, courant limité à < 60 mA
- ALARM_IN[7:1] : -7 V à -5 V, impédance de 10 kiloohms

Brochage du connecteur externe

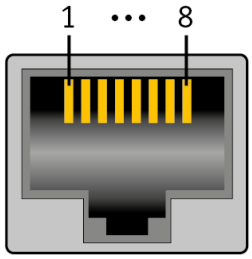
Broche	Description du signal	Broche	Description du signal
1	ALARM_IN[1]	5	ALARM_IN[5]
2	ALARM_IN[2]	6	ALARM_IN[6]
3	ALARM_IN[3]	7	ALARM_IN[7]
4	ALARM_IN[4]	8	ALARM_CM

Sections pertinentes :

Procédure de surveillance des capteurs discrets

Interprétation des données des capteurs

3.5.2.4 Port série RJ45



Description :

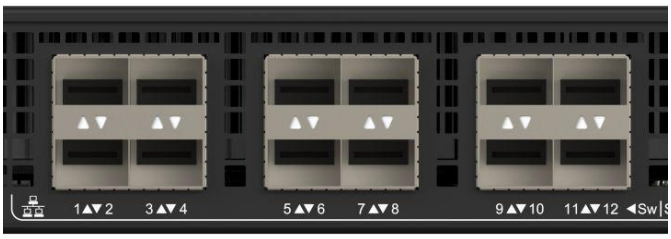
Le port série est électriquement compatible avec la norme RS-232.

Brochage du connecteur externe :

Broche	Description du signal	Broche	Description du signal
1	RTS	5	Masse
2	DTR	6	RX#
3	TX#	7	DSR
4	Masse	8	CTS

3.5.2.5 SFP, SFP+ et SFP28

3.5.2.5.1 Option module d'E/S de commutation Ethernet



Le mappage des ports déterminera si le port est un port SFP+ ou SFP28. Voir Configuration du commutateur pour savoir comment configurer le mappage des ports.

Connecteur homologue : Modules SFP+ ou SFP28

3.5.2.5.2 Option module d'E/S de connexion directe

Le développement de cette option est envisagé. Veuillez contacter le service des ventes de Kontron.

Description :

Les interfaces SFP+ et SFP28 sont normalisées et conformes aux normes suivantes, sans s'y limiter :

- SFF-8431, SFF-8432 (SFP+)
- SFF-8402 (SFP28)
- 1000BASE-LX/SX, SFP-MSA, SFF INF-8074i (toutes les options de module d'E/S)
- 10GBASE-CR/LR/SR, IEEE802.3 clause 52 (toutes les options de module d'E/S)
- 25GBASE-CR/LR/SR, IEEE802.3 clauses 110 et 112 (module d'E/S de commutation Ethernet)

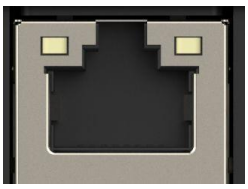
NOTICE

Utiliser toujours des modules optiques avec de la fibre optique pour les connexions longues (> 6 mètres) ou extérieures.

Section pertinente :

Liste de compatibilité matérielle

3.5.2.6 Port de gestion Ethernet RJ45



Description :

Cette interface est un port standard 10/100/1000Base-T et est conforme aux normes suivantes, sans s'y limiter :

- IEEE 802.3 clause 40

NOTICE

Une longueur de câble allant jusqu'à 100 mètres est acceptable pour les connexions à l'intérieur d'un bâtiment si l'installation est conforme à la norme Telcordia GR-1089 issue 6 pour un port de type 2 exempté du test de surtension longitudinale due à la foudre (section 4.5.3.1).

3.5.2.7 Interfaces USB

Connecteur homologue : USB

Description :

Les interfaces USB sont des connecteurs hôtes standard de type A et sont conformes aux spécifications USB 3.1 et USB 2.0, disponibles à USB Implementers Forum.

3.5.3 Connecteur d’entrée du bloc d'alimentation CC

Connecteur homologue : Voir Câblage pour fabriquer les câbles appropriés.

Description :

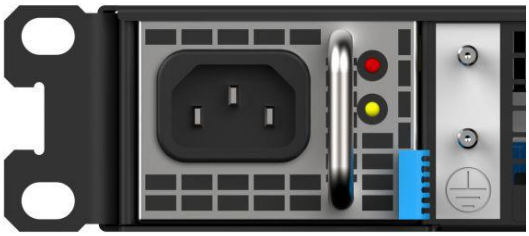
L'entrée d'alimentation CC est conçue conformément aux normes Telcordia GR-1089 et ATIS-0600315 et présente les caractéristiques suivantes :

- Entrées d’alimentation redondantes (avec diodes OR-ing actives)
- Plage de tension de fonctionnement en courant continu de -40,0 V à -56,7 V
- Fusibles internes (30 A sur RTN_A et RTN_B; 25 A sur -48V_A, -48V_B)
- Protection contre l’appel de courant transitoire et les surintensités grâce à un contrôleur d’alimentation
- Protection contre les surtensions (IEC 61000-4-5 class 2, 1 kV)

NOTICE

L'interface d'alimentation CC est protégée contre les surtensions et la longueur du câble n'est pas limitée à 6 mètres. Cette interface convient à une connexion aux systèmes locaux d'alimentation CC (GR-1089 type 8) et à une alimentation CC à l'intérieur d'un site cellulaire, avec exposition limitée à l'extérieur (type 8b).

3.5.4 Connecteur d’entrée du bloc d'alimentation CA



Connecteur homologue : IEC C13

Description :

Le connecteur d’entrée du bloc d'alimentation CA présente les caractéristiques de base suivantes (voir la documentation de Murata pour le composant D1U54P-W-650-12-HB4C pour plus de détails) :

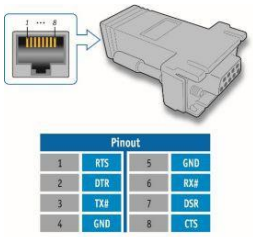
- 90 à 264 VAC, 47 à 63 Hz
- Limitation des courants d'appel transitoires (25 A crête)
- Efficacité 80Plus® Platinum
- Protection contre les surtensions (IEC 61000-4-5 class 3, 2 kV)

3.6 Matériel, information et logiciels nécessaires

3.6.1 Matériel et information nécessaires

Pour une liste des composants compatibles, voir Liste de compatibilité matérielle.

3.6.1.1 Adaptateur optionnel

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

3.6.1.2 Installation et assemblage des composants

3.6.1.2.1 Carte d'expansion PCIe

Voir Ressources de la plateforme destinées à l'application client pour des exemples de scripts à intégrer dans l'application pour gérer les capteurs de température propres au client.

Élément_1	Un tournevis Torx T10
Élément_2	(Optionnel) Une sonde thermique pour la surveillance de la température (si une surveillance physique de
Élément_3	(Optionnel) Colle pouvant résister à la température générée par la carte d'expansion PCIe et ayant des propriétés appropriées pour l'application

3.6.1.3 Câbles d'alimentation et outils

3.6.1.3.1 Pour un bloc d'alimentation CC

Élément_1	Cosses à sertir : • Deux ou quatre cosses à fourche isolées à sertir Molex pour fils de calibre 14-16 (19131-0023) **OU** • Deux ou quatre cosses à œillet isolées à sertir Panduit pour fils de calibre 10-12 (EV10-6RB-Q)
Élément_2	Fil noir toronné pour fabriquer le cordon d'alimentation en fonction de la longueur requise : • Calibre de fil approprié à l'application en fonction des spécifications du cordon et du code électrique local • Diamètre maximum de l'isolation : 4,40 mm [0,175 po] pour les cosses à sertir Molex **OU** • Diamètre maximum de l'isolation : 5,8 mm [0,23 po] pour les cosses à sertir Panduit
Élément_3	Fil rouge toronné pour fabriquer le cordon d'alimentation en fonction de la longueur requise : • Calibre de fil approprié à l'application en fonction des spécifications du cordon et du code électrique local • Diamètre maximum de l'isolation : 4,40 mm [0,175 po] pour les cosses à sertir Molex **OU** • Diamètre maximum de l'isolation : 5,8 mm [0,23 po] pour les cosses à sertir Panduit
Élément_4	Une pince à sertir manuelle : • Pince à sertir manuelle de première qualité Molex (640010100) **OU** • Pince à sertir manuelle Panduit (638130400)
Élément_5	Un câble de mise à la terre de calibre AWG nº 8 en fonction de la longueur requise
Élément_6	Une cosse de mise à la terre à angle droit, calibre AWG nº 8 (numéro de pièce Kontron 1064-4226)
Élément_7	Une pince à sertir manuelle, Panduit CT-1700
Élément_8	Clé de 7 mm ou outil équivalent

3.6.1.3.2 Pour un bloc d'alimentation CA

Élément_1	Cordon d'alimentation européen CA CEE 7/7 à C13, 10 A/250 VCA, 1,8 m de long **OU** Cordon d'alimentation CA NEMA 5-15P à C13, 10 A/125 VCA, 2 m de long

3.6.1.3.3 Matériel d'installation dans l'étagère

Élément_1	Fixations pour l'étagère (propre à chaque étagère)

3.6.1.3.4 Câbles et modules réseau

3.6.1.3.4.1 Option module d'E/S de commutation Ethernet

Élément_1	Un module optique SFP (SX, LX, SR, LR) avec câble optique compatible
Élément_2	Un câble Ethernet RJ45 pour la couche de gestion/de contrôle
Élément_3	Un câble de connexion série RJ45

3.6.1.3.4.2 Option module d'E/S de connexion directe

Le développement de cette option est envisagé. Veuillez contacter le service des ventes de Kontron.

3.6.2 Logiciels nécessaires

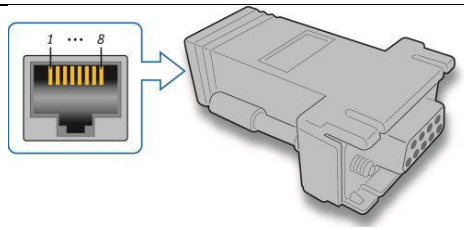
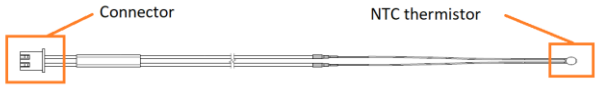
Élément_1	Un client HTTP tel que cURL ou Postman est recommandé pour utiliser l'interface Redfish de la plateforme. L'outil cURL est utilisé dans la documentation.
Élément_2	Un émulateur de terminal tel que PuTTY est installé sur un ordinateur distant.
Élément_3	Un outil de détection des périphériques tel que pciutils est installé sur le serveur local pour visualiser des
Élément_4	Une version de la communauté d'ipmitool est installée sur un ordinateur distant et sur le serveur local pour permettre la surveillance à distance – il est recommandé d'utiliser la version 1.8.18 d'ipmitool.

3.6.3 Plateforme, modules et accessoires

Section pertinente :

Installation et assemblage des composants

Cette section fournit la liste complète des pièces et composants compatibles qui peuvent être commandés auprès de Kontron.

Description	Numéro de pièce Kontron	Illustration
Adaptateur série RJ45 vers DB9	1015-9404	
Cordon d'alimentation européen CA CEE 7/7 à C13, 10 A/250 VCA, 1,8 m de long	1061-0410	
Cordon d'alimentation CA NEMA 5-15P à	1-340000-0	
Cosse de mise à la terre à angle droit, calibre	1064-4226	
Sonde thermique pour carte d'expansion PCIe	1065-9296	

3.7 Liste de compatibilité matérielle

3.7.1 Disques SSD industriels M.2 (-40 °C à 85 °C)

Type	Taille	Dimension	Fournisseur	Numéro de pièce du fournisseur	État	Numéro de pièce Kontron
NVMe	128 Go	2280	Transcend	TS128GMTE652TI	Actif	1068-6586
NVMe	512 Go	2280	Transcend	TS512GMTE652TI-KCI	Actif	1068-1170
			Western Digital	SDBPNPZ-512G-XI	Actif	
NVMe	1 To	2280	Transcend	TS1TMTE662TI-KCI	Actif	1068-1161
			Western Digital	SDBPNPZ-1T00-XI	Actif	
NVMe	2 To	2280	Transcend	TS2TMTE662TI-KCI	Actif	1068-1158
			Western Digital	SDBPNPZ-2T00-XI	Actif	

3.7.2 Modules mémoires industriels RDIMM avec ECC (-40 °C à 85 °C)

Taille	Type	Fournisseur	Numéro de pièce du fournisseur	État	Numéro de pièce Kontron
16 Go	DDR4-3200*	Micron Technology	MTA18ASF2G72PDBZ-3G2E1	Actif	1067-0181
32 Go	DDR4-3200*	Micron Technology	MTA36ASF4G72PBZ-3G2E1	Actif	1068-6284
64 Go	DDR4-3200*	Smart Modular Technology	STI8197RD440425-SA	Actif	1068-6291

* Les plateformes ME1310 prennent en charge des vitesses DDR4 allant jusqu'à 2933

3.7.3 Modules industriels SFP, SFP+ et SFP28 (-40 °C à 85 °C)

Les modules doivent être testés :

- Avec les ports du module d'E/S de commutation Ethernet configurés pour prendre en charge le niveau de vitesse du module

Type	Fournisseur	Numéro de pièce du fournisseur	Description	État	Numéro de pièce Kontron
1000BASE-SX	II-VI (Finisar)	FTLF8519P3BTL	500 m, 850 nm, -40 °C à 85 °C, émetteur-récepteur optique SFP	Actif	1064-5770
10GBASE-SR	II-VI (Finisar)	FTLX8573D3BTL	400 m, 850 nm, -40 °C à 85 °C, émetteur-récepteur optique SFP+	EOL	1064-5765
	II-VI (Finisar)	FTLX8574D3BTL	400 m, 850 nm, -40 °C à 85 °C, émetteur-récepteur optique SFP+	Actif	
	FormericaOE	TAS-A2NH1-P11	300 m, 850 nm, -40 °C à 85 °C, émetteur-récepteur optique SFP+	Actif	
25GBASE-SR	FS	SFP28-25GSR-85-I	100 m, 850 nm, -40 °C à 85 °C, émetteur-récepteur optique SFP28	Actif	1068-5031
	II-VI (Finisar)	FTLF8536W4BTV	100 m, 850 nm, -40 °C à 85 °C, émetteur-récepteur optique SFP28	Actif	
1000BASE-LX	FormericaOE	TSD-S2CA1-F11	10 km, 1310 nm, -40 °C à 85 °C, émetteur-récepteur optique SFP	Actif	1065-3758
	II-VI (Finisar)	FTLF1318P3BTL	10 km, 1310 nm, -40 °C à 85 °C, émetteur-récepteur optique SFP	Actif	
	Avago	AFCT-5715ALZ	10 km, 1310 nm, -40 °C à 85 °C, émetteur-récepteur optique SFP	Actif	
10GBASE-LR	FS	SFP-10GLR-31-I	10 km, 1310 nm, -40 °C à 85 °C, émetteur-récepteur optique SFP+	Actif	1065-6804

Type	Fournisseur	Numéro de pièce du fournisseur	Description	État	Numéro de pièce Kontron
	II-VI (Finisar)	FTLX1475D3BTL	10 km, 1310 nm, -40 °C à 85 °C, émetteur-récepteur optique SFP+	Actif	
25GBASE-LR	FS	SFP28-25GLR-31-I	10 km, 1310 nm, -40 °C à 85 °C, émetteur-récepteur optique SFP28	Actif	1068-5037

3.8 Systèmes d'exploitation validés

3.8.1 Description des états

Légende des	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
PRÉVUE	La certification est prévue.
EN COURS	La certification est en cours.

3.8.2 État de la certification selon le système d'exploitation

NOTE : Communiquez avec le soutien à la clientèle pour obtenir de l'information supplémentaire sur la certification ou la validation d'autres systèmes d'exploitation.

Système d'exploitation	État
CentOS 7.8	PRÉVUE
RHEL 7.8	PRÉVUE
RHEL 8.2	PRÉVUE
SUSE EL 15 SP2	PRÉVUE
Ubuntu 18.04	PRÉVUE
Ubuntu 20.04	PRÉVUE
VMware ESXi 6.7	PRÉVUE

3.9 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 les sous-sections de Configuration réseau.

• Le service SNMP du BMC est activé par défaut. Définir au minimum une valeur unique pour la chaîne de communauté SNMP ou désactiver le service. Voir Configurer le service SNMP du BMC

• La plateforme prend en charge la fonction de démarrage sécurisé. Voir Configuration des options UEFI/BIOS.

• La plateforme inclut un module de plateforme sécurisée (TPM). Déterminer les exigences en matière de fonctions matérielles associées à la sécurité. Voir Configurer le TPM dans la section Configuration des options UEFI/BIOS.

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

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

4.1 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.

4.2 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 ME1310 équipée de une ou deux cartes d'expansion PCIe fournies par le client et d'un disque SATA M.2 128 Go, et utilisée pour exploiter deux liaisons réseau distinctes (une pour la couche de gestion/de contrôle et l'autre pour la couche des données).

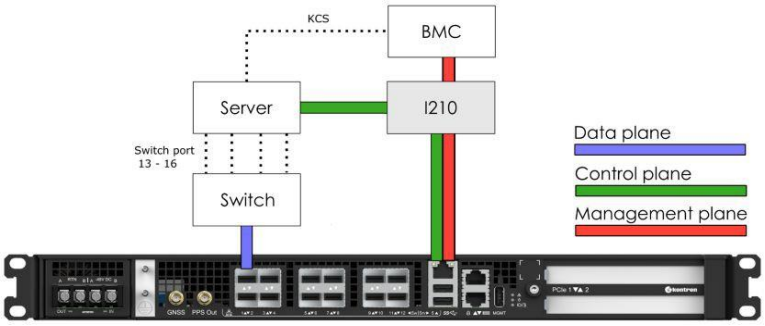
Ce cas d'utilisation est basé sur une architecture simplifiée avec une couche de gestion, une couche de contrôle et une couche des données.

Hypothèses

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

- Les connexions réseau du système sont les suivantes :
  - Une couche de gestion (ligne rouge) et une couche de contrôle (ligne verte) via le port de gestion RJ45 5 (Srv 5)
  - Une couche des données (ligne violette) via le port SFP 1 du commutateur (Sw 1)
  - Une connexion série via le port série RJ45 de la plateforme
- Le schéma d'adressage IPv4 est de type DHCP pour la couche de gestion
- La méthode privilégiée pour obtenir ou configurer l'adresse IP du BMC est d'utiliser le serveur DHCP
- La méthode privilégiée pour obtenir ou configurer l'adresse IP du NOS est d'utiliser le serveur DHCP
- La méthode d'accès privilégiée pour le BMC et le système d'exploitation est l'interface utilisateur Web
  La température de la carte ou des cartes d'expansion PCIe est surveillée à l'aide d'une sonde thermique installée dans la plateforme

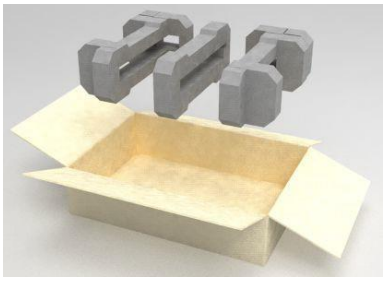
Schéma de l'intégration réseau



4.3 Déballage de la plateforme

4.3.1 Contenu de la boîte

La boîte contient une plateforme ME1310 d’informatique en périphérie multi-accès 1U.



Étape_1	Retirer soigneusement la plateforme de son emballage.
Étape_2	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

NOTE : Du matériel supplémentaire pourrait être nécessaire pour procéder à l'installation et à la configuration (voir Matériel et information nécessaires pour plus d'informations).

4.4 Planification

4.4.1 Matériel et information nécessaires

Pour une liste des composants compatibles, voir Liste de compatibilité matérielle.

Carte d'expansion PCIe

NOTE : Une sonde thermique par carte d'expansion PCIe est requise.

Élément_1	Un tournevis Torx T10
Élément_2	(Optionnel) Une sonde thermique pour la surveillance de la température (si une surveillance physique de
Élément_3	(Optionnel) Colle pouvant résister à la température générée par la carte d'expansion PCIe et ayant des propriétés appropriées pour l'application

Câbles d'alimentation et outils

Élément_1	Cosses à sertir : • Deux ou quatre cosses à fourche isolées à sertir Molex pour fils de calibre 14-16 (19131-0023) OU Deux ou quatre cosses à œillet isolées à sertir Panduit pour fils de calibre 10-12 (EV10-6RB-Q)
Élément_2	Fil noir toronné pour fabriquer le cordon d'alimentation en fonction de la longueur requise : • Calibre de fil approprié à l'application en fonction des spécifications du cordon et du code électrique local • Diamètre maximum de l'isolation : 4,40 mm [0,175 po] pour les cosses à sertir Molex **OU** • Diamètre maximum de l'isolation : 5,8 mm [0,23 po] pour les cosses à sertir Panduit
Élément_3	Fil rouge toronné pour fabriquer le cordon d'alimentation en fonction de la longueur requise : • Calibre de fil approprié à l'application en fonction des spécifications du cordon et du code électrique local • Diamètre maximum de l'isolation : 4,40 mm [0,175 po] pour les cosses à sertir Molex **OU** • Diamètre maximum de l'isolation : 5,8 mm [0,23 po] pour les cosses à sertir Panduit

Élément_4	Une pince à sertir manuelle : • Pince à sertir manuelle de première qualité Molex (640010100) **OU** • Pince à sertir manuelle Panduit (638130400)
Élément_5	Un câble de mise à la terre de calibre AWG nº 8 en fonction de la longueur requise
Élément_6	Une cosse de mise à la terre à angle droit, calibre AWG nº 8 (numéro de pièce Kontron 1064-4226)
Élément_7	Une pince à sertir manuelle, Panduit CT-1700
Élément_8	Clé de 7 mm ou outil équivalent

Matériel d'installation dans l'étagère

Élément_1	Fixations pour l'étagère (propre à chaque étagère)

Câbles et modules réseau

Élément_1	Un module optique SFP (SX, LX, SR, LR) avec câble optique compatible
Élément_2	Un câble Ethernet RJ45 pour la couche de gestion/de contrôle
Élément_3	Un câble de connexion série RJ45

Infrastructure réseau

- Les adresses IP suivantes pourraient être nécessaires :
  - L'adresse IP de la couche de gestion/de contrôle pour le BMC
  - Les adresses IP de la couche de contrôle et de la couche des données pour le serveur
  - L'adresse IP de la couche des données pour le NOS

4.4.2 Logiciels nécessaires

Section pertinente :

Installation des logiciels courants

Élément_1	Un client HTTP tel que cURL ou Postman est recommandé pour utiliser l'interface Redfish de la plateforme. L'outil cURL est utilisé dans la documentation.
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.
Élément_4	Une version de la communauté d'ipmitool est installée sur un ordinateur distant et sur le serveur local pour permettre la surveillance à distance – il est recommandé d'utiliser la version 1.8.18 d'ipmitool.

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

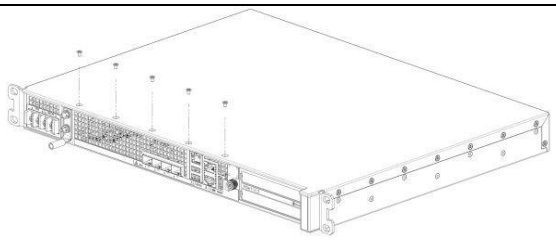
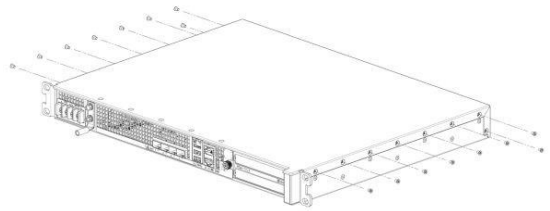
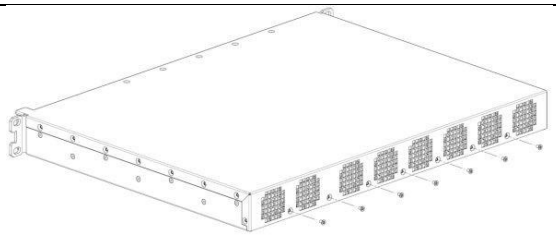
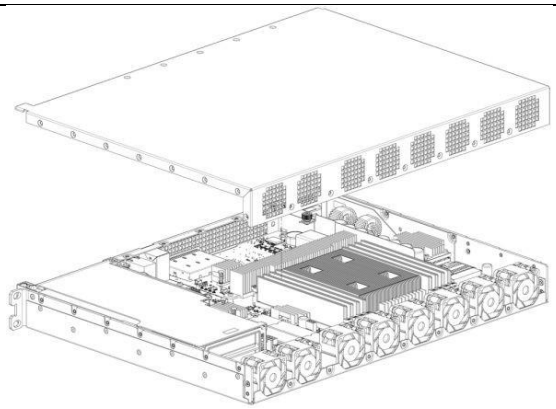
4.5 Installer une ou deux cartes d'expansion PCIe et les sondes thermiques associées dans un ME1310

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.

4.5.1 Ouvrir le châssis

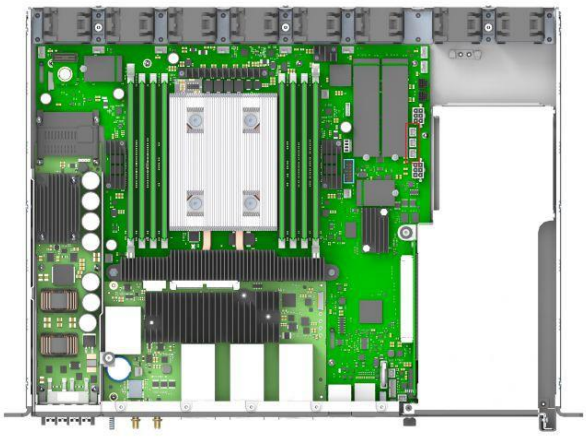
Étape_1	Retirer les 5 vis du capot supérieur avec un tournevis Torx T10.	
Étape_2	Retirer les 16 vis installées sur les côtés (8 par côté) avec un tournevis Torx T10.	
Étape_3	Retirer les 7 vis installées à l'arrière avec un tournevis Torx T10.	
Étape_4	Soulever le capot vers le haut pour le retirer du châssis.	

4.6 Installer une ou deux sondes thermiques pour la ou les cartes d'expansion PCIe

4.6.1 Localiser les connecteurs pour sondes thermiques

Le ME1310 comporte trois connecteurs pour sondes thermiques.

Emplacement	Indicateur de référence	Connecteur
Arrière	J20	Emplacement PCIe 1
Milieu	J21	Emplacement PCIe 2
Avant	J23	Châssis



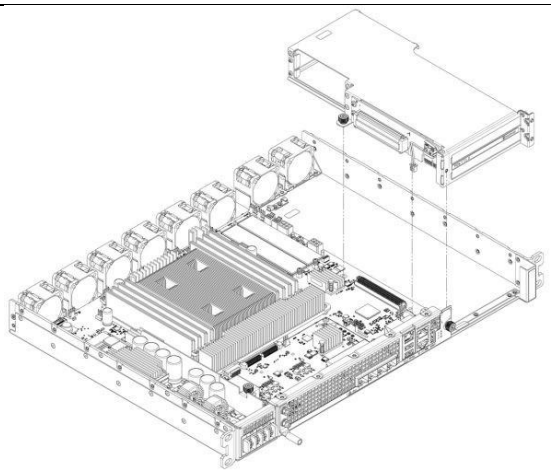
4.6.2 Installer les sondes thermiques

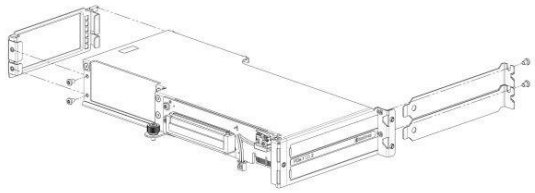
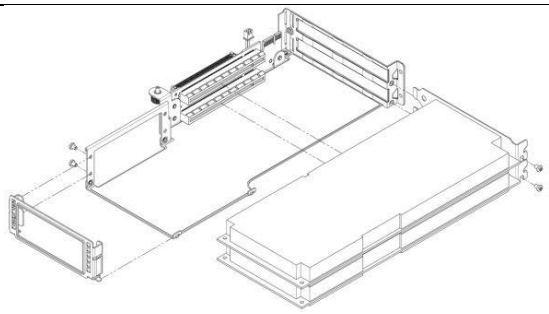
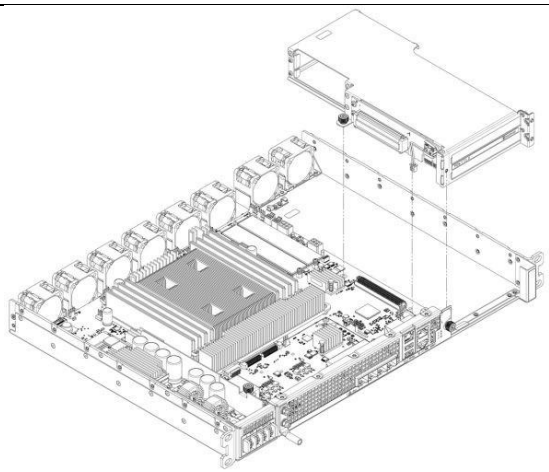
Étape_1	Installer la sonde thermique dans le connecteur comme indiqué dans les spécifications de la sonde thermique. Utiliser le connecteur approprié en fonction de l'emplacement de la carte d'expansion PCIe dans l'assemblage.
Étape_2	Fixer la thermistance à coefficient de température négatif sur la carte PCIe. Veiller à ce que la thermistance soit placée aussi près que possible des composants générateurs de chaleur afin d'obtenir une lecture pertinente de la température. Ne pas utiliser d'éléments qui ne sont pas thermoconducteurs. En général, les thermistances sont installées entre les ailettes du dissipateur thermique de la carte PCIe. Ne pas oublier d'utiliser une colle capable de résister à la température de fonctionnement et dont les propriétés sont adaptées à l'application. Voici quelques exemples de colles qui pourraient être utilisées : adhésif Loctite 444 et activateur Loctite SF 7452. **NOTE :** La configuration sera effectuée une fois que la plateforme sera opérationnelle (seuils, configurations logicielles particulières, etc.).
Étape_3	Répéter les étapes 1 et 2 si deux sondes thermiques doivent être installées.

Voir Configurer les capteurs et les paramètres thermiques pour configurer les paramètres thermiques.

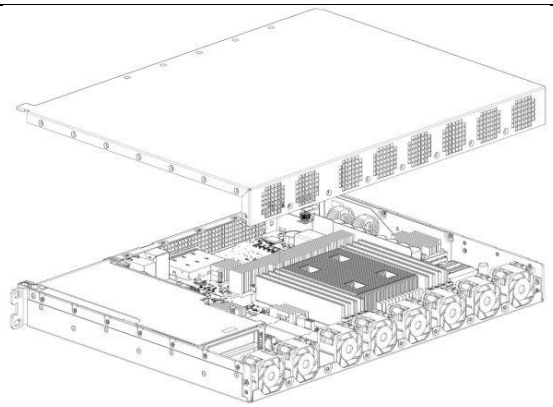
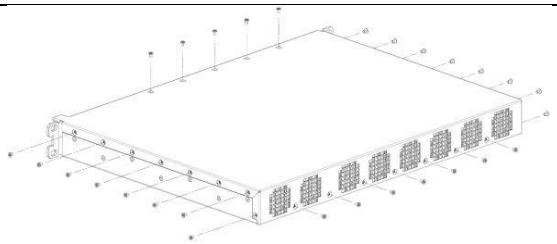
4.6.3 Installer une ou deux cartes d'expansion PCIe

Le facteur de forme maximum pour les cartes d'expansion PCIe optionnelles est pleine hauteur, trois quarts de longueur (FH3/4L).

Étape_1	Avec un tournevis Torx T10, dévisser les deux vis à serrage à main situées à l'avant du châssis et sur la carte principale. Débrancher le fil du dispositif de détection d'intrusion situé près de l'avant du châssis. Soulever la cage d'extension PCIe vers le haut pour la sortir du châssis.	

Étape_2	Avec un tournevis Torx T10, retirer une plaque en L vierge pour carte PCIe si une carte d'expansion PCIe est installée ou retirer les deux plaques en L vierges pour carte PCIe si deux cartes d'expansion PCIe sont installées. Avec le tournevis Torx T10, retirer le support arrière de la cage d'extension PCIe. **NOTE :** Si seulement une carte d'expansion PCIe est installée, elle peut être installée dans l'emplacement 1 ou 2. Le système n'a pas de préférence électrique. **NOTE :** L'emplacement PCIe 1 est l'emplacement du bas et l'emplacement PCIe 2 est l'emplacement du haut.	
Étape_3	Installer la ou les cartes d'expansion PCIe sur la carte adaptatrice de connexion PCIe. Avec un tournevis Torx T10, fixer la ou les plaques en L vierges sur la cage d'extension PCIe (couple de 6 lb-po). Fixer le support arrière de la cage d'extension PCIe sur la cage et serrer les vis M3 avec un tournevis Torx T10 (couple de 6 lb-po). **NOTE :** Si les cartes d'expansion PCIe ne sont pas conformes aux spécifications électromécaniques pour les zones d'exclusion arrière, mettre au rebut le support arrière de la cage d'extension PCIe.	
Étape_4	Insérer soigneusement la cage d'extension PCIe dans l'unité et la fixer avec les deux vis à serrage à main (couple de 6 lb-po). Brancher le fil du dispositif de détection d'intrusion situé près de l'avant du châssis.	

4.6.4 Fermer le châssis

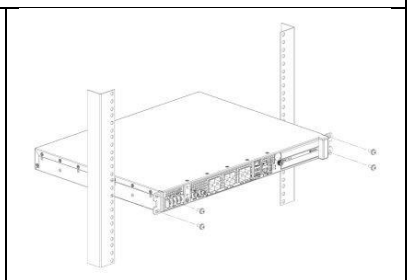
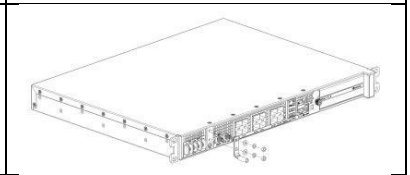
Étape_1	Placer le capot sur le châssis.	
Étape_2	Insérer et visser légèrement toutes les vis à tête plate M3 : • 5 sur le dessus • 8 par côté (16 au total) • 7 à l'arrière Avec un tournevis Torx T10, serrer toutes les vis (couple de 6 lb-po).	

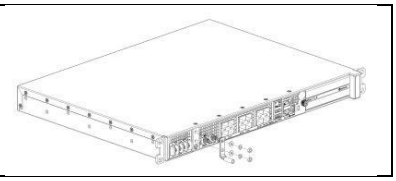
4.7 Installation de la plateforme dans une étagère

Section pertinente :

Circulation de l’air

Lors du choix de l'emplacement de la plateforme dans l’étagère (rack), veiller à ce qu'il n'y ait pas d'obstacle physique susceptible d'entraver la bonne circulation de l'air.

Étape_1	Choisir un emplacement pour la plateforme dans l’étagère.	
Étape_2	Insérer la plateforme dans l’étagère.	
Étape_3	Fixer la plateforme à l’étagère avec les fixations appropriées.	
Étape_4	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_5	Dénuder 19 mm (0,75 po) du câble de mise à la terre de calibre AWG nº 8.	
Étape_6	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).	

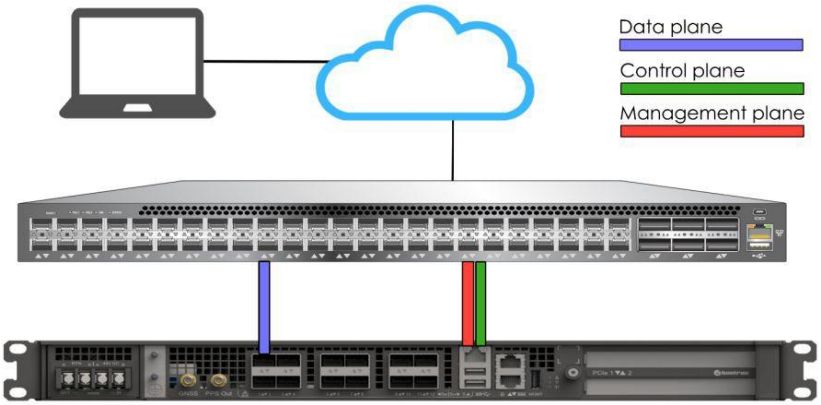
Étape_7	Installer la cosse de mise à la terre sur les goujons, en la fixant à l'aide des 2 écrous et rondelles. **NOTE :** Le filetage des deux cosses de mise à la terre du châssis est M4x0,7.	

> Vous êtes maintenant prêt à brancher les câbles réseau et d'alimentation et à amorcer la configuration de la plateforme.

4.8 Raccordement des câbles réseau

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

Étape_1	Connecter un câble RJ45 au port 5 pour les couches de gestion et de contrôle (Srv 5).
Étape_2	Connecter un câble SFP ou SFP+ au port 1 du commutateur pour la couche des données (Sw 1).



4.8.1 Fabrication et connexion des câbles du bloc d'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.

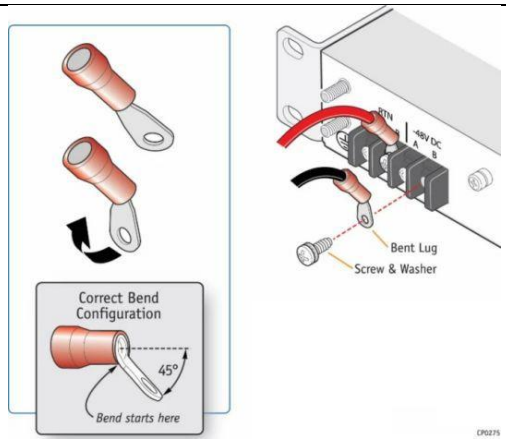
⚠WARNING

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

Des pinces peuvent être utilisées pour plier les cosses à sertir.

Procédure

Étape_1	Dénuder l'extrémité d'un fil noir toronné de calibre AWG n° 14 sur une longueur de 6 mm (0,236 po) (pour une cosse à sertir Molex 19131-0023) ou l'extrémité d'un fil noir toronné de calibre n° 12 AWG sur une longueur de 8 mm (0,315 po) (pour une cosse à sertir Panduit EV10-6RB-Q).
Étape_2	Dénuder l'extrémité d'un fil rouge toronné de calibre AWG n° 14 sur une longueur de 6 mm (0,236 po) (pour une cosse à sertir Molex 19131-0023) ou l'extrémité d'un fil rouge toronné de calibre n° 12 AWG sur une longueur de 8 mm (0,315 po) (pour une cosse à sertir Panduit EV10-6RB-Q).
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 de l'outil.
Étape_4	Plier les cosses à sertir à un angle de 45° comme illustré sur l'image.
Étape_5	Retirer la vis de l'emplacement RTN « B » de la plaque à bornes.
Étape_6	Insérer le fil rouge serti dans l'emplacement RTN « B » comme illustré sur l'image.
Étape_7	Visser la cosse à sertir en place.
Étape_8	Retirer la vis de l'emplacement -48V DC « B » de la plaque à bornes.
Étape_9	Insérer le fil noir serti dans l'emplacement -48V DC « B » comme illustré sur l'image.
Étape_10	Visser la cosse à sertir en place.
Étape_11	(Optionnel) Si une redondance est nécessaire, répéter les étapes 1 à 10 pour un deuxième jeu de câbles. Ils doivent être installés dans les emplacements -48V DC et RTN « A ».
Étape_12	Le bloc d'alimentation est protégé contre les inversions de polarité. La plateforme démarrera dès qu'une alimentation externe sera appliquée (DEL d'alimentation verte).



> Vous êtes maintenant prêt à découvrir les adresses IP.

4.9 Découvrir l'adresse IP du BMC

L'adresse IP du BMC est le minimum requis pour accéder à l'interface utilisateur Web et à l'interface de surveillance.

L'adresse IP du BMC peut être découverte en utilisant différentes méthodes : La méthode UEFI /BIOS sera utilisée dans ce Guide de démarrage.

Section pertinente :

Découvrir les adresses IP de la plateforme

4.9.1 Accéder à l'UEFI/BIOS en utilisant une console série (connexion physique)

4.9.1.1 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.

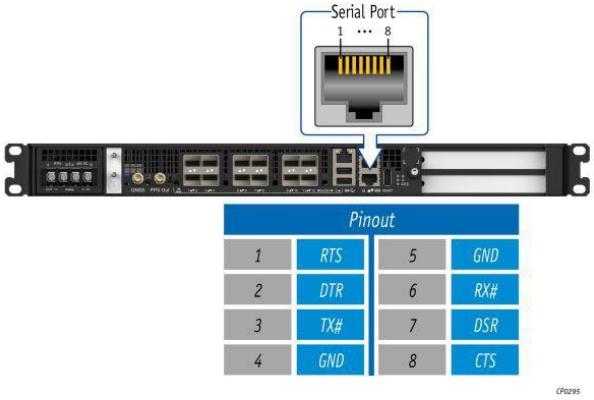
2	Un outil de console série est installé sur l'ordinateur distant. Vitesse (baud) : 115200 Bits d'information : 8 Bits d'arrêt : 1 Parité : Aucune Contrôle de flux : Aucune Mode émulation recommandé : VT100+ **NOTE** : PuTTY est recommandé.

Sections pertinentes :

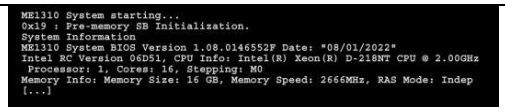
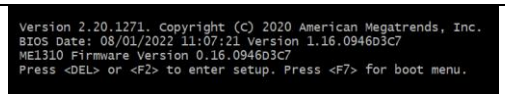
Accéder à l'UEFI/BIOS

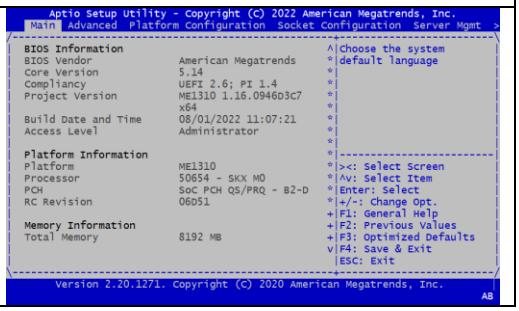
Envoi d'une commande BREAK sur une connexion série

4.9.1.2 Emplacement du port



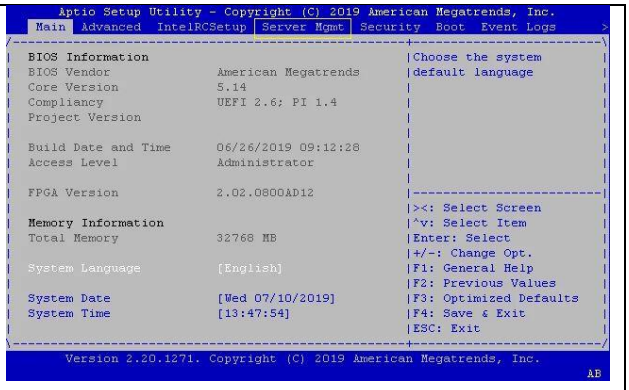
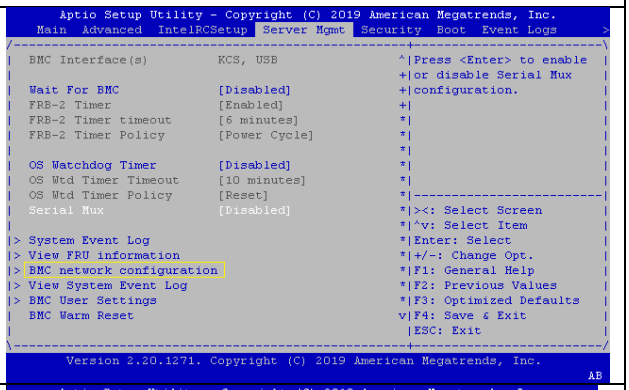
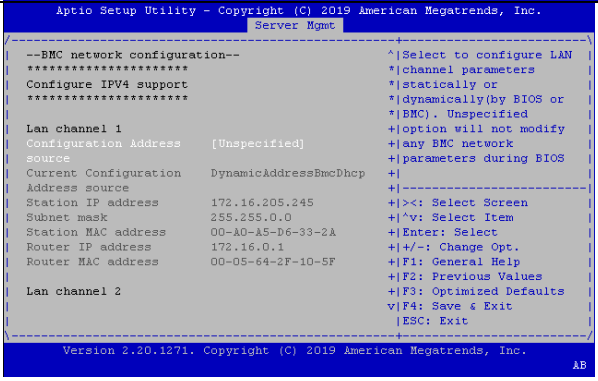
4.9.1.3 Accéder au menu de configuration de l'UEFI/BIOS

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 en utilisant l'une des options suivantes : • Si le serveur exécute actuellement un système d'exploitation installé, ouvrir une session et lancer la commande de redémarrage appropriée. • Si le serveur exécute actuellement le shell UEFI intégré, lancer la commande « reset ». • Envoyez une commande BREAK sur la connexion série en utilisant la méthode disponible dans l'émulateur de terminal. • Débrancher tous les câbles d'alimentation pendant 30 secondes, puis les rebrancher. **NOTE :** Si un système d'exploitation est installé, une méthode faisant appel à un 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 de l'UEFI/BIOS ne s'affiche.	
Étape_3	Lorsque l'écran d'accueil de l'UEFI/BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration de l'UEFI/BIOS. **NOTE :** Il peut s'écouler quelques secondes avant que l'écran d'accueil de l'UEFI/BIOS n'affiche le message de confirmation "Entering Setup…".	

Étape_4	L'écran d'accueil de l'UEFI/BIOS affiche "Entering Setup...". **NOTE :** L'affichage et l'entrée dans le menu de configuration de l'UEFI/BIOS prendront quelques secondes.	
Étape_5	Le menu de configuration de l'UEFI/BIOS s'affiche.	

4.9.1.4 Accéder au menu BMC network configuration

NOTE : Sur une plateforme ME1310, le canal LAN 1 correspond au port Srv 5, le connecteur RJ45.

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.	

4.10 Découvrir l'adresse IP du NOS

L’adresse IP du NOS est le minimum requis pour accéder à l'interface utilisateur Web du NOS et à l’interface de surveillance.

4.10.1 Découvrir l’adresse IP du NOS en utilisant le CLI de la console série du NOS

4.10.1.1 Préalables

1	L'adresse IP du BMC est connue.
2	Un outil client SSH est installé sur l'ordinateur distant. **NOTE :** PuTTY est recommandé pour les environnements Windows, et SSH est recommandé pour les environnements Linux.
3	L'ordinateur distant a accès au sous-réseau du réseau de gestion.

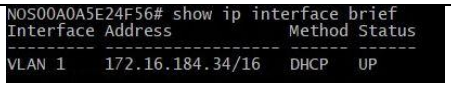
Sections pertinentes :

Noms d'utilisateur et mots de passe par défaut

Accéder au NOS

4.10.1.2 Procédure

NOTE : Lorsque série sur SSH est utilisé, appuyer sur **Entrée**, puis sur le **~** pour quitter la session.

Étape_1	À l’aide d’un outil client SSH, ouvrir une session SSH avec les paramètres suivants : • Adresse IP du BMC • Numéro de port : 2201 (une fois la session ouverte, le BMC redirigera automatiquement la communication vers la console série du NOS)	
Étape_2	Ouvrir une session sur le BMC à l'aide des données d'accès appropriées pour le BMC. Une fois la connexion établie, appuyer sur **Entrée** pour obtenir une réponse du CLI du NOS. Si une session n’est pas déjà ouverte sur la console série du NOS, une autre série de données d'accès sera demandée. Utiliser les données d'accès appropriées pour le commutateur afin d’ouvrir la session sur le NOS.	
Étape_3	Utiliser la commande suivante pour découvrir l'adresse IP du NOS. InviteCLI_NOSLocal:~# **show ip interface brief**	

> Avec les adresses IP, vous êtes maintenant prêt à commencer l'installation du système d'exploitation.

4.11 Préparation de l'installation du système d'exploitation

Étape_1	Choisir le système d'exploitation nécessaire en fonction des exigences de votre application. Il est recommandé d’en choisir un parmi les systèmes d’exploitation validés.
Étape_2	Confirmer que la version du système d'exploitation à installer comprend ou a des pilotes qui prennent en charge les composants de la plateforme inclus dans le mappage PCI.
Étape_3	Si requis, télécharger le fichier ISO du système d'exploitation à installer.

4.12 Installer un système d'exploitation en utilisant le KVM

Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut.

4.12.1 Préalables

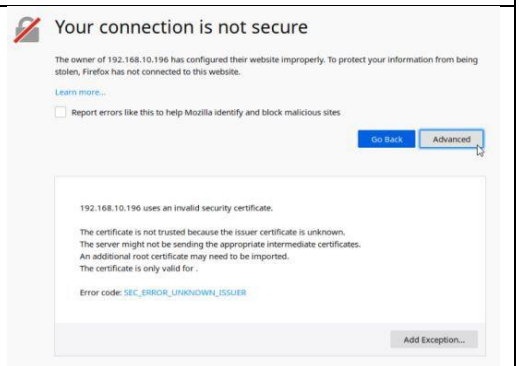
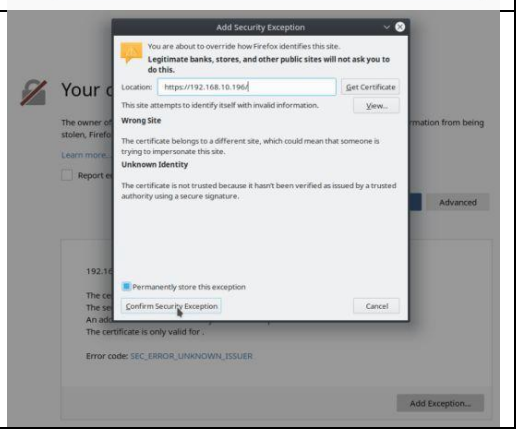
1	L'adresse IP du BMC est connue.
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.

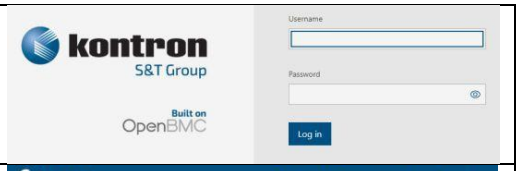
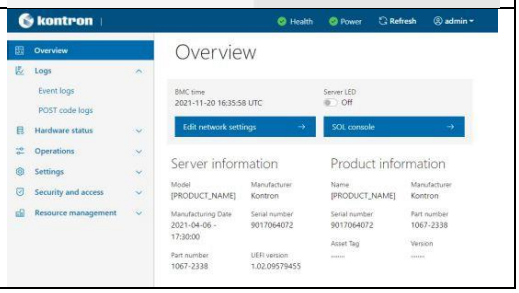
4.12.2 Considérations relatives au navigateur

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 utilisateur 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.

4.12.3 Établir la communication avec l'interface utilisateur Web du BMC

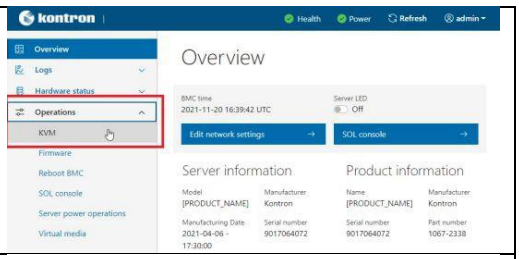
Étape_1	À partir d'un ordinateur distant ayant accès au réseau de gestion, ouvrir une fenêtre de navigateur et entrer l'adresse IP découverte pour le BMC. **NOTE : Le préfixe HTTPS est obligatoire.** *https://[IP_GESTION_BMC]*	
Étape_2	Cliquer sur **Advanced** pour lancer le processus d'acceptation du 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.	
Étape_5	Vous avez maintenant accès à l'interface utilisateur Web de gestion du BMC. Vous pouvez utiliser l'interface.	

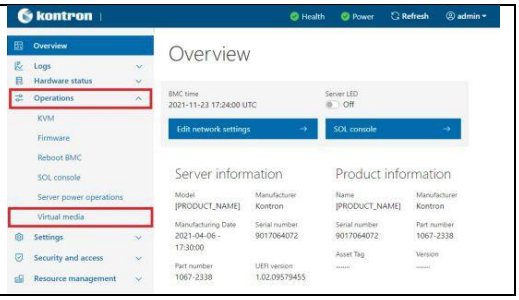
Il est recommandé de changer le mot de passe de l'administrateur immédiatement après avoir accédé à l'interface utilisateur Web.

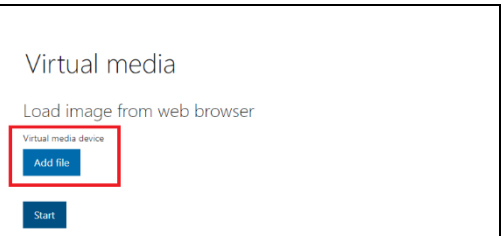
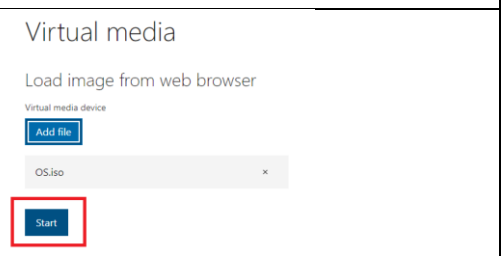
4.12.4 Lancer le KVM

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

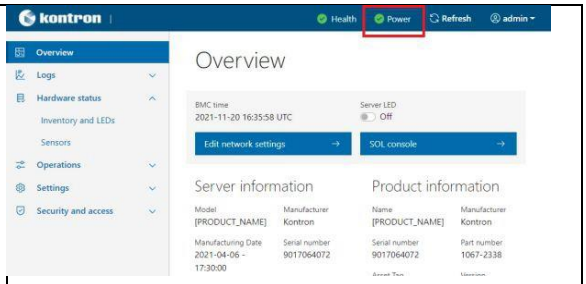
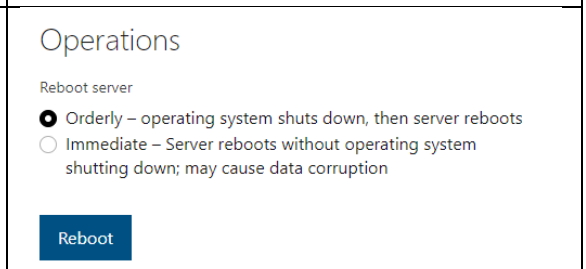
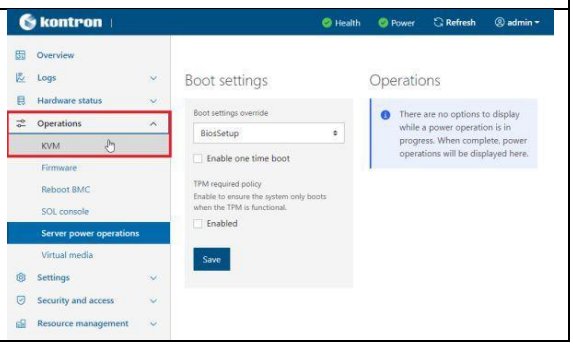
Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Operations**, puis sur **KVM**.	
Étape_2	Une nouvelle fenêtre de navigateur s'ouvre et affiche l'écran virtuel du serveur.	

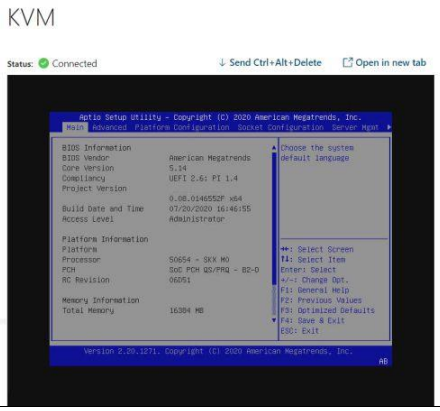
4.12.5 Monter l'image du système d'exploitation en utilisant un support virtuel

Étape_1	Dans le menu **Operations**, sélectionner **Virtual media**.	

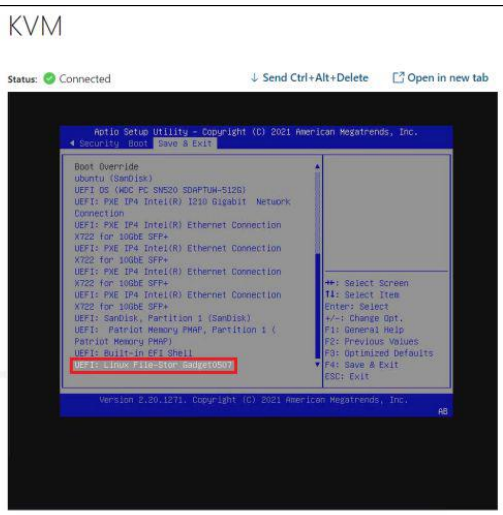
Étape_2	Cliquer sur **Add file** pour chercher le fichier ISO.	
Étape_3	Cliquer sur **Start** pour accéder au support virtuel à partir du système d'exploitation.	

4.12.6 Accéder au menu de configuration de l'UEFI/BIOS

Étape_1	Dans l'interface utilisateur Web du BMC, cliquer sur le bouton **Power**.	
Étape_2	Dans la section **Reboot server**, sélectionner **Orderly**, puis cliquer sur **Reboot**.	
Étape_3	Dans le menu **Operations**, cliquer sur **KVM**.	

Étape_4	Lorsque l'écran d'accueil de l'UEFI/BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration de l'UEFI/BIOS. **NOTE :** Lorsqu'une commande de réinitialisation du serveur est lancée, quelques secondes peuvent s'écouler avant que l'écran d'accueil de l'UEFI/BIOS ne s'affiche. **NOTE :** Il peut s'écouler quelques secondes avant que l'écran d'accueil de l'UEFI/BIOS n'affiche le message de confirmation "Entering Setup…".	
Étape_5	L'écran d'accueil de l'UEFI/BIOS affiche "Entering Setup...". **NOTE :** L'affichage et l'entrée dans le menu de configuration de l'UEFI/BIOS pourraient prendre quelques secondes.	
Étape_6	Le menu de configuration de l'UEFI/BIOS s'affiche.	

4.12.7 Choisir l'ordre de démarrage avec la fonction Boot Override

Étape_1	Dans le menu de configuration de l'UEFI/BIOS et à l'aide des flèches du clavier, sélectionner le menu **Save & Exit**. Dans la section **Boot Override**, sélectionner **UEFI: Linux File-Stor Gadgetxxxx** 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.

4.12.8 Compléter l'installation du système d'exploitation

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

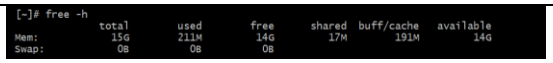
4.13 Vérifier l'installation du système d'exploitation

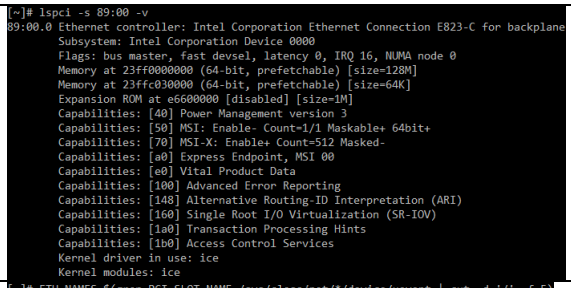
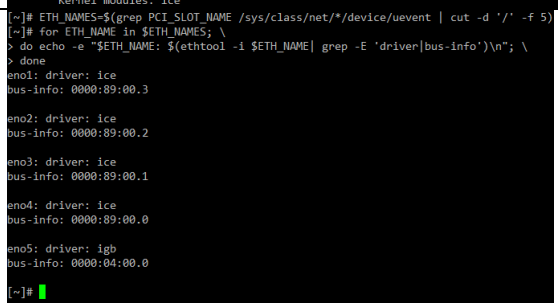
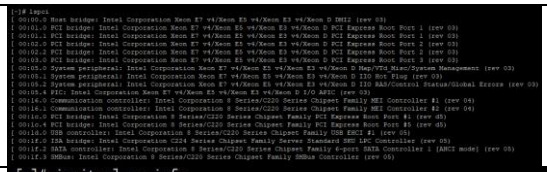
Voir l'introduction du Guide de démarrage pour passer en revue l'architecture utilisée dans cette section de démarrage.

Section pertinente :

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	Installer **ethtool**, **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 pour CentOS : InviteSE_ServeurLocal:~# **yum update** InviteSE_ServeurLocal:~# **yum install pciutils** InviteSE_ServeurLocal:~# **yum install ethtool** InviteSE_ServeurLocal:~# **yum install ipmitool** **NOTE :** La mise à jour des paquets peut prendre quelques minutes.	
Étape_3	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_4	Vérifier que les modules DIMM sont détectés. InviteSE_ServeurLocal:~# **free -h**	
Étape_5	Vérifier que toutes les unités de stockage sont détectées. InviteSE_ServeurLocal:~# **lsblk**	
Étape_6	Confirmer que les contrôleurs d'interfaces réseau de la couche de contrôle sont chargés par le pilote **igb**. InviteSE_ServeurLocal:~# **lspci -s 04:00 -v** **NOTE :** Un CIR 1GbE devrait être découvert.	

Étape_7	Confirmer que les contrôleurs d'interfaces réseau de la couche des données sont chargés par le pilote **ice**. InviteSE_ServeurLocal:~# **lspci -s 89:00 -v** **NOTE :** Jusqu'à quatre CIR 25GbE devraient être découverts.	
Étape_8	Confirmer que toutes les interfaces réseau sont détectées et obtenir la liste des noms de périphériques. Le script suivant nécessite l'utilisation du shell Bash. Saisir le bloc de commandes suivant. InviteSE_ServeurLocal:~# **ETH_NAMES=$(grep PCI _SLOT_NAME /sys/class/net/*/device/uevent | cut -d '/' -f 5)** **for ETH_NAME in $ETH_NAMES; ** **do echo -e "$ETH_NAME: $(ethtool -i $ETH_NAME| grep -E 'driver|bus- info')\n"; ** **done** **NOTE :** Jusqu'à quatre CIR 25GbE et un CIR 1GbE devraient être découverts.	
Étape_9	Configurer les contrôleurs d'interfaces réseau en fonction de vos exigences et de la topologie de réseau. **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_10	(Optionnel) Si une ou deux cartes d'expansion PCIe sont installées, vérifier qu'elles sont détectées. InviteSE_ServeurLocal:~# **lspci**	
Étape_11	Vérifier la communication entre le système d'exploitation et le BMC. InviteSE_ServeurLocal:~# **ipmitool mc info**	

4.14 Conduite de tests de performance sur une application

Installer l'application et procéder aux tests de performance.

4.15 Surveillance des capteurs de la plateforme

Les capteurs de la plateforme peuvent être surveillés à l'aide de différentes méthodes, entre autres en utilisant l'interface utilisateur Web du BMC. Les principaux capteurs à considérer sont les suivants :

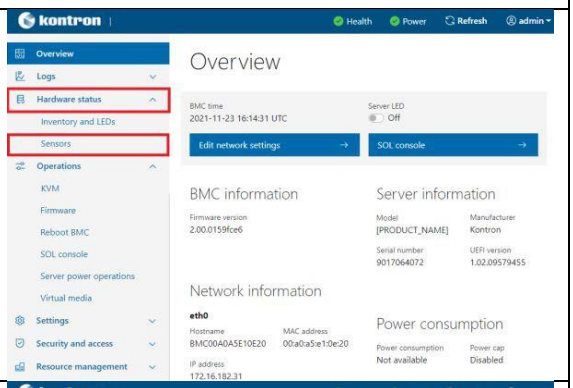
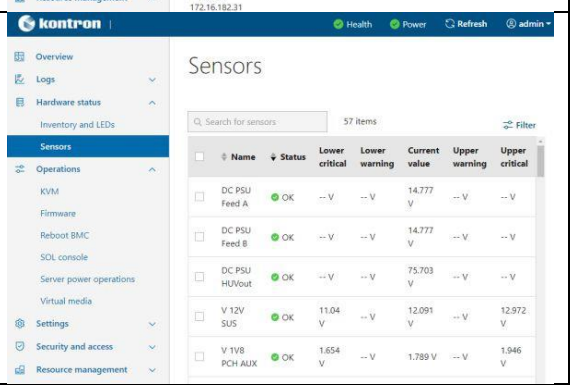
- Capteurs de température
- Capteurs d'alimentation

Sections pertinentes :

Accéder au BMC

Surveillance des capteurs

4.15.1 Surveiller les capteurs de la plateforme en utilisant l'interface utilisateur Web

Étape_1	Accéder à l'interface utilisateur Web du BMC.	
Étape_2	Dans le menu de gauche, cliquer sur **Hardware status**, puis sur **Sensors**.	
Étape_3	La liste des capteurs s'affiche. Faire défiler vers le bas pour voir la liste des capteurs ou utiliser la barre de recherche dédiée pour filtrer les capteurs.	

5/ Installation mécanique et précautions

5.1 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.

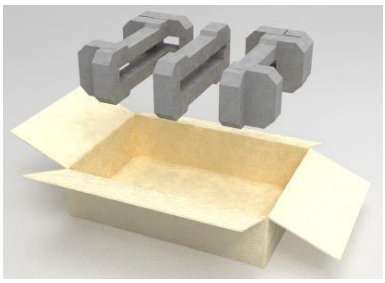
Nous vous recommandons d'effectuer toutes les procédures d'installation décrites dans la documentation sur un poste de travail ESD. Si cela n'est pas possible, utiliser des mesures de protection contre les décharges électrostatiques telles que les suivantes :

- 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.

5.2 Déballage

5.2.1 Contenu de la boîte

La boîte contient une plateforme ME1310 d’informatique en périphérie multi-accès 1U.



Étape_1	Retirer soigneusement la plateforme de son emballage.
Étape_2	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.**

5.3 Installation et assemblage des composants

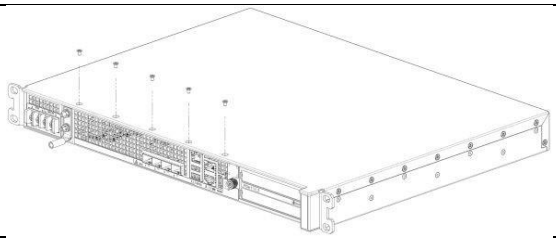
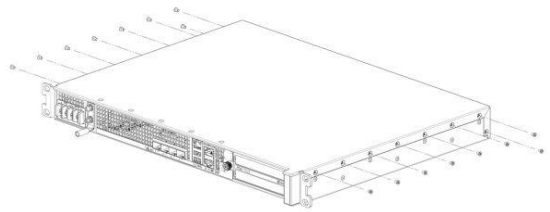
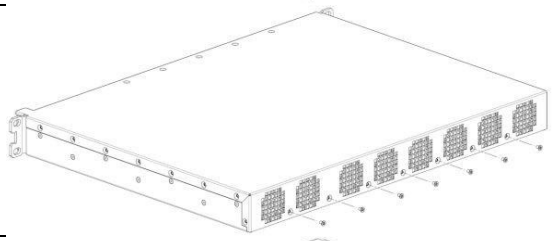
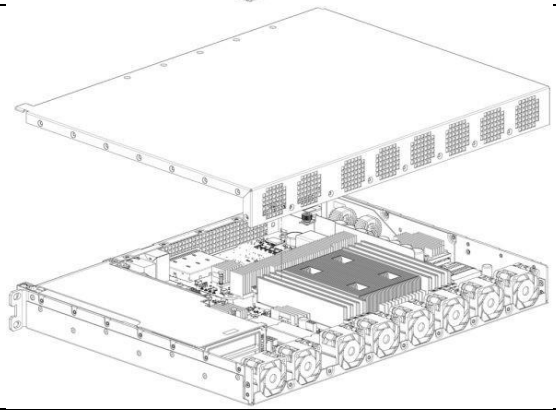
Appareil sensible aux ESD!

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.

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

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.

5.3.1 Ouvrir le châssis

Étape_1	Retirer les 5 vis du capot supérieur avec un tournevis Torx T10.	
Étape_2	Retirer les 16 vis installées sur les côtés (8 par côté) avec un tournevis Torx T10.	
Étape_3	Retirer les 7 vis installées à l'arrière avec un tournevis Torx T10.	
Étape_4	Soulever le capot vers le haut pour le retirer du châssis.	

5.3.2 Installer une ou deux cartes d'expansion PCIe

Le facteur de forme maximum pour les cartes d'expansion PCIe optionnelles est pleine hauteur, trois quarts de longueur (FH3/4L).

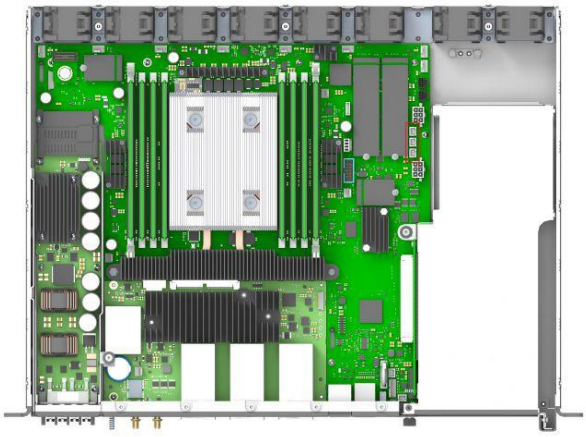
5.3.2.1 (Optionnel) Installer une sonde thermique pour la carte d'expansion PCIe

Pour connaître le numéro de pièce de la sonde thermique, voir Plateforme, modules et accessoires.

5.3.2.1.1 (Optionnel) Localiser le connecteur de la sonde thermique

Le ME1310 comporte trois connecteurs pour sondes thermiques.

Emplacement	Indicateur de référence	Connecteur
Arrière	J20	Emplacement PCIe 1
Milieu	J21	Emplacement PCIe 2
Avant	J23	Châssis



5.3.2.1.2 (Optionnel) Fabriquer une sonde thermique

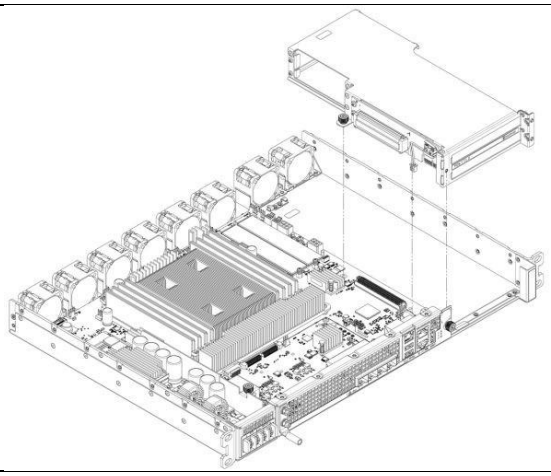
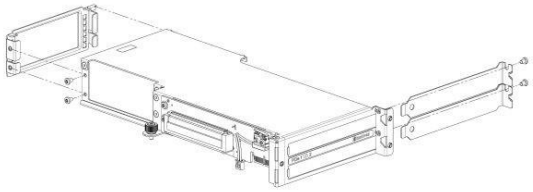
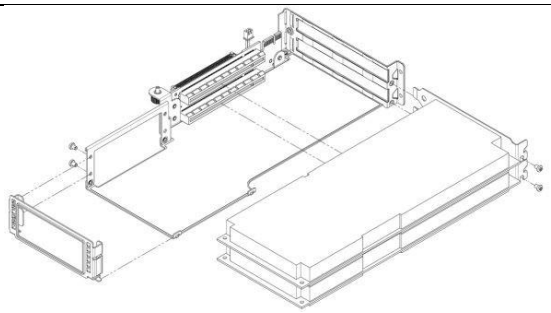
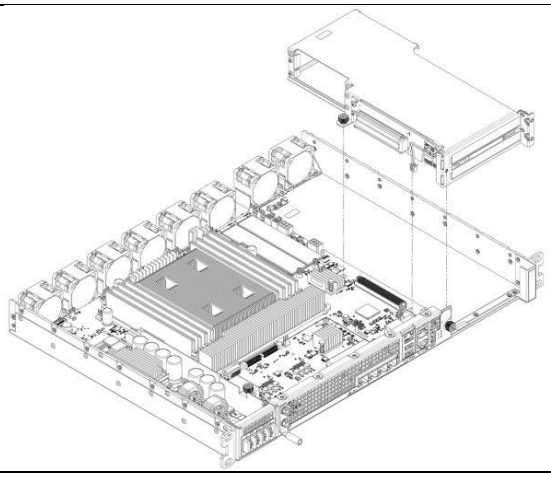
Composant	**Numéro de pièce**	**Description**
Thermistance à coefficient de température négatif	GA10K3A1IA	Thermistance à coefficient de température négatif (NTC), 10 kΩ (perle), 3976 K
Connecteur	XHP-2	Boîtier de connecteur 2,5 mm, 2 positions
Broches	SXH-001-P0.6	Contact de réceptacle, de calibre AWG nº 22-28, avec embout serti

Étape_1	Avec les composants décrits dans le tableau ci-dessus, fabriquer une sonde thermique.

5.3.2.1.3 (Optionnel) Installer la sonde thermique

Étape_1	Installer la sonde thermique dans le connecteur comme indiqué dans les spécifications de la sonde thermique. Utiliser le connecteur approprié en fonction de l'emplacement de la carte d'expansion PCIe dans l'assemblage.
Étape_2	Fixer la thermistance à coefficient de température négatif sur la carte PCIe. Veiller à ce que la thermistance soit placée aussi près que possible des composants générateurs de chaleur afin d'obtenir une lecture pertinente de la température. Ne pas utiliser d'éléments qui ne sont pas thermoconducteurs. En général, les thermistances sont installées entre les ailettes du dissipateur thermique de la carte PCIe. Ne pas oublier d'utiliser une colle capable de résister à la température de fonctionnement et dont les propriétés sont adaptées à l'application. Voici quelques exemples de colles qui pourraient être utilisées : adhésif Loctite 444 et activateur Loctite SF 7452. **NOTE :** La configuration sera effectuée une fois que la plateforme sera opérationnelle (seuils, configurations logicielles particulières, etc.).
Étape_3	Répéter les étapes 1 et 2 si deux sondes thermiques doivent être installées.

5.3.2.2 Installer une carte d'expansion PCIe

Étape_1	Avec un tournevis Torx T10, dévisser les deux vis à serrage à main situées à l'avant du châssis et sur la carte principale. Débrancher le fil du dispositif de détection d'intrusion situé près de l'avant du châssis. Soulever la cage d'extension PCIe vers le haut pour la sortir du châssis.	
Étape_2	Avec un tournevis Torx T10, retirer une plaque en L vierge pour carte PCIe si une carte d'expansion PCIe est installée ou retirer les deux plaques en L vierges pour carte PCIe si deux cartes d'expansion PCIe sont installées. Avec le tournevis Torx T10, retirer le support arrière de la cage d'extension PCIe. **NOTE :** Si seulement une carte d'expansion PCIe est installée, elle peut être installée dans l'emplacement 1 ou 2. Le système n'a pas de préférence électrique. **NOTE :** L'emplacement PCIe 1 est l'emplacement du bas et l'emplacement PCIe 2 est l'emplacement du haut.	
Étape_3	Installer la ou les cartes d'expansion PCIe sur la carte adaptatrice de connexion PCIe. Avec un tournevis Torx T10, fixer la ou les plaques en L vierges sur la cage d'extension PCIe (couple de 6 lb-po). Fixer le support arrière de la cage d'extension PCIe sur la cage et serrer les vis M3 avec un tournevis Torx T10 (couple de 6 lb-po). **NOTE :** Si les cartes d'expansion PCIe ne sont pas conformes aux spécifications électromécaniques pour les zones d'exclusion arrière, mettre au rebut le support arrière de la cage d'extension PCIe.	
Étape_4	Insérer soigneusement la cage d'extension PCIe dans l'unité et la fixer avec les deux vis à serrage à main (couple de 6 lb-po). Brancher le fil du dispositif de détection d'intrusion situé près de l'avant du châssis.	

5.3.2.3 (Optionnel) Instructions d'installation des éléments logiciels

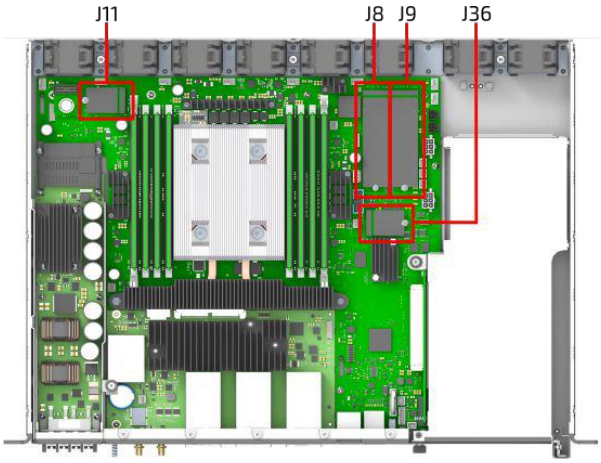
Voir Liste de compatibilité matérielle pour connaître les instructions d'installation des éléments logiciels pour les cartes d'expansion PCIe prise en charge.

5.3.3 Installer un disque de stockage M.2

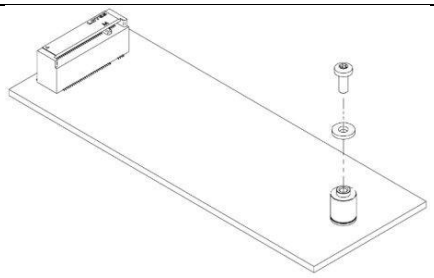
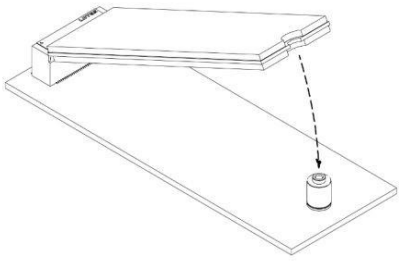
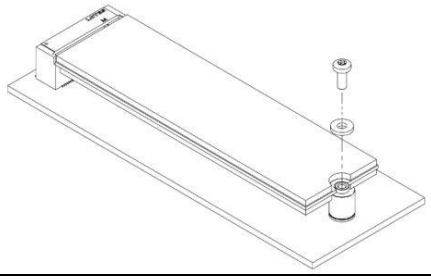
Jusqu'à quatre disques de stockage M.2 peuvent être installés dans un ME1310.

Pour la liste des disques de stockage M.2 testés, voir Liste de compatibilité matérielle.

5.3.3.1 Localiser les disques de stockage M.2



5.3.3.2 Installer un disque de stockage M.2

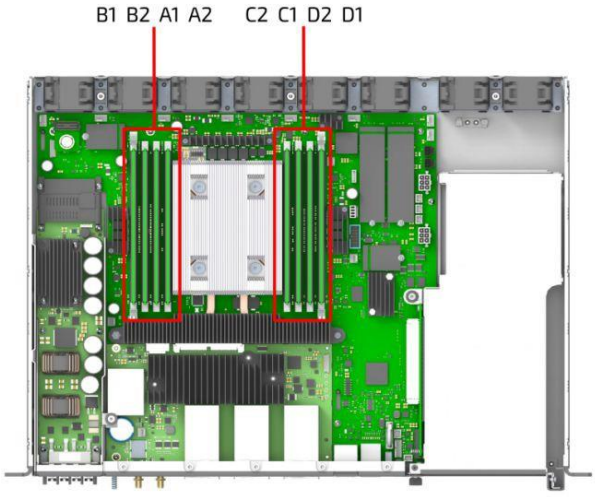
Étape_1	Retirer la vis et la rondelle du montant à l'aide d'un tournevis Torx T6.	
Étape_2	Insérer le disque de stockage M.2 dans le connecteur comme le prévoient les spécifications M.2.	
Étape_3	Remettre la vis et la rondelle en place et serrer (couple de 2 lb-po).	

5.3.4 Installer des modules DIMM

Jusqu'à huit modules DIMM peuvent être installés dans un ME1310.

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

5.3.4.1 Localiser les modules DIMM



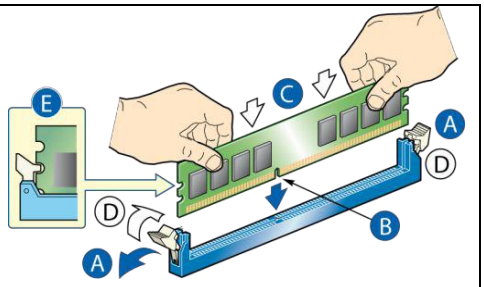
5.3.4.2 Directives d’installation des modules DIMM pour une performance optimale

Il y a 8 emplacements DIMM, mais seulement 4 canaux – B1 et B2 sont sur le même canal, A1 et A2 sont sur le même canal, C1 et C2 sont sur le même canal et D1 et D2 sont sur le même canal.

Par conséquent, ne pas remplir les emplacements A2, B2, C2 et D2 à moins d’avoir rempli tous les autres emplacements DIMM. Installer les modules DIMM conformément aux directives suivantes pour une performance optimale.

- Pour les configurations avec 1 module DIMM – remplir l’emplacement C1.
- Pour les configurations avec 2 modules DIMM – remplir les emplacements A1 et C1.
- Pour les configurations avec 4 modules DIMM – remplir les emplacements A1, B1, C1 et D1.
- Pour les configurations avec 8 modules DIMM – remplir tous les emplacements DIMM.
- Les autres configurations ne sont pas recommandées, car elles pourraient être déséquilibrées et produiront une performance moins optimale.

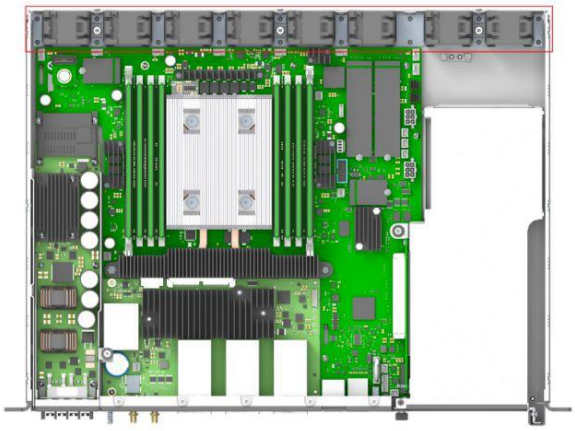
5.3.4.3 Installer un module DIMM

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 du 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)	

5.3.5 Remplacer des ventilateurs

Il y a huit ventilateurs dans cette plateforme.

5.3.5.1 Localiser les ventilateurs



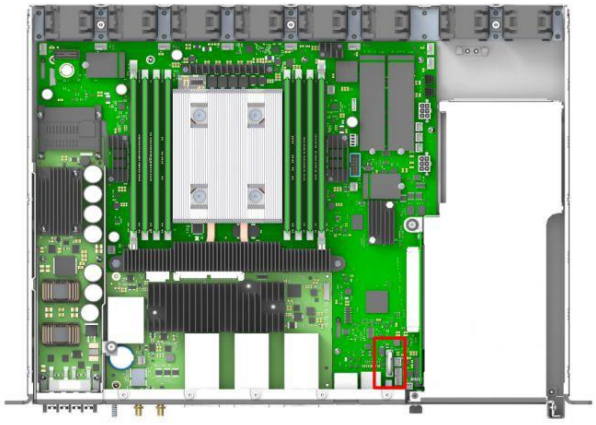
5.3.5.2 Remplacer un ventilateur

Étape_1	Débrancher le connecteur du ventilateur.
Étape_2	Soulever le ventilateur vers le haut pour le sortir de la plateforme.
Étape_3	Insérer un nouveau ventilateur et brancher le connecteur du ventilateur.

5.3.6 Remplacer la pile de l’horloge temps réel (RTC)

⚠CAUTION Risque d'explosion si la pile est remplacée par un type inadéquat. Se débarrasser des piles usées selon les instructions.

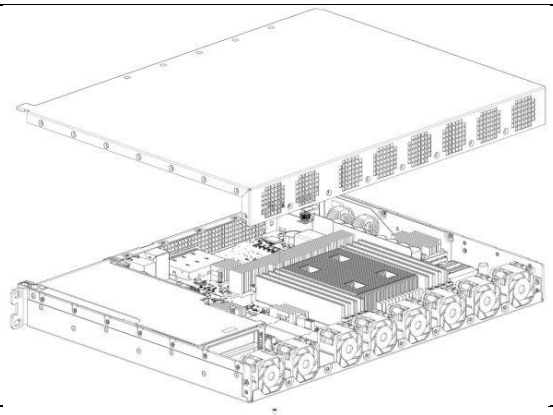
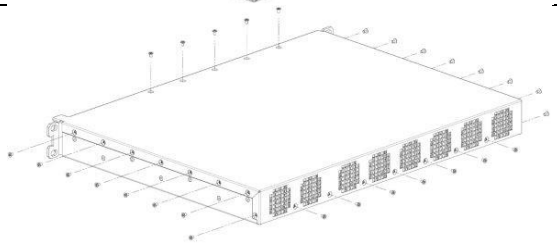
5.3.6.1 Localiser la pile de l’horloge temps réel



5.3.6.2 Remplacer la pile

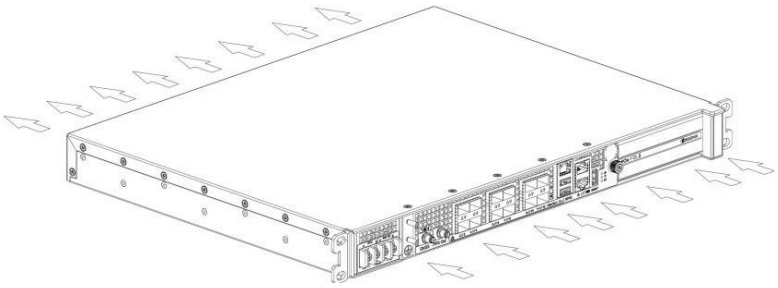
Étape_1	Une goupille de verrouillage permet de fixer la pile en place. D'une main, pousser doucement la goupille pour libérer la pile. Tout en maintenant la goupille, utiliser l'autre main pour retirer la pile.
Étape_2	Recycler la pile de façon sécuritaire.
Étape_3	D'une main, pousser doucement la goupille et, de l'autre, insérer une nouvelle pile. Respecter l'orientation et la polarité appropriées.

5.3.7 Fermer le châssis

Étape_1	Placer le capot sur le châssis.	
Étape_2	Insérer et visser légèrement toutes les vis à tête plate M3 : • 5 sur le dessus • 8 par côté (16 au total) • 7 à l'arrière Avec un tournevis Torx T10, serrer toutes les vis (couple de 6 lb-po).	

5.4 Circulation de l’air

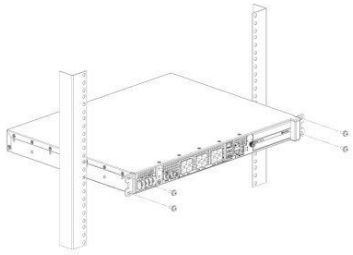
La plateforme ME1310 est dotée d'un système de circulation de l'air allant de l’avant à l’arrière. Pour optimiser le transfert de chaleur, voir Spécifications pour connaître les dégagements idéaux.

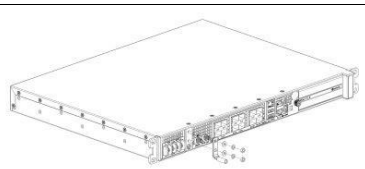
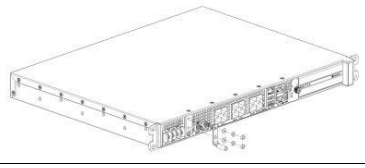


5.5 Installation dans une étagère

5.5.1 Installer une plateforme ME1310 dans une étagère de 19 pouces

Lors du choix de l'emplacement de la plateforme dans l’étagère (rack), veiller à ce qu'il n'y ait pas d'obstacle physique susceptible d'entraver la bonne circulation de l'air.

Étape_1	Choisir un emplacement pour la plateforme dans l’étagère.	
Étape_2	Insérer la plateforme dans l’étagère.	
Étape_3	Fixer la plateforme à l’étagère avec les fixations appropriées.	

Étape_4	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_5	Dénuder 19 mm (0,75 po) du câble de mise à la terre de calibre AWG nº 8.	
Étape_6	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_7	Installer la cosse de mise à la terre sur les goujons, en la fixant à l'aide des 2 écrous et rondelles. **NOTE :** Le filetage des deux cosses de mise à la terre du châssis est M4x0,7.	

5.6 Câblage

5.6.1 Entrée du bloc d'alimentation CC

Description	**Courant d'entrée maximum**	**Modèle de la prise du bloc d'alimentation**
Connecteur d'entrée du bloc d'alimentation CC 600 W	17 A	Amphenol (Anytek) YK6050423000G

5.6.2 Fabriquer les câbles du bloc d'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.

⚠WARNING

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

Des pinces peuvent être utilisées pour plier les cosses à sertir.

5.6.2.1 Matériel nécessaire

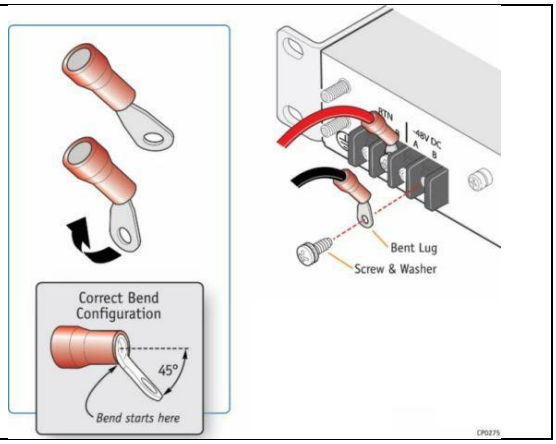
Kontron suggère d'utiliser des cosses à sertir (cosses à sertir à œillet ou à fourche, droites, isolées, UL94V-0) pour les câbles d'alimentation. Connecter le câble approprié à la polarité appropriée.

Utiliser un calibre de fil approprié pour les emplacements -48V DC et RTN en fonction des spécifications du cordon et du code électrique local.

Description	**Quantité**	**Numéro de pièce du fabricant**	**Lien**
Cosses à sertir : • Cosses à fourche isolées à sertir Molex pour fils de calibre 14-16 • Cosses à œillet isolées à sertir Panduit pour fils de calibre 10-12	2 (ou 4 pour la redondance)	19131-0023 ou équivalent	Catalogue des produits Molex Détails de la pièce
		EV10-6RB-Q ou équivalent	Catalogue des produits Panduit Dessin de la pièce
Fil noir toronné pour fabriquer le cordon d'alimentation en fonction de la longueur requise : • Diamètre maximum de l'isolation : 4,40 mm [0,175 po] pour les cosses à sertir Molex • Diamètre maximum de l'isolation : 5,8 mm [0,23 po] pour les cosses à sertir Panduit	Longueur requise		
Fil rouge toronné pour fabriquer le cordon d'alimentation en fonction de la longueur requise : • Diamètre maximum de l'isolation : 4,40 mm [0,175 po] pour les cosses à sertir Molex • Diamètre maximum de l'isolation : 5,8 mm [0,23 po] pour les cosses à sertir Panduit	Longueur requise		
Pince à sertir manuelle : • Pince à sertir manuelle de première qualité Molex • Pince à sertir manuelle Panduit	1	640010100 ou équivalent	Catalogue des produits Molex Spécifications
		CT-460 ou équivalent	Catalogue des produits Panduit Spécifications

5.6.2.2 Procédure

Étape_1	Dénuder l'extrémité d'un fil noir toronné de calibre AWG n° 14 sur une longueur de 6 mm (0,236 po) (pour une cosse à sertir Molex 19131-0023) ou l'extrémité d'un fil noir toronné de calibre n° 12 AWG sur une longueur de 8 mm (0,315 po) (pour une cosse à sertir Panduit EV10-6RB-Q).	
Étape_2	Dénuder l'extrémité d'un fil rouge toronné de calibre AWG n° 14 sur une longueur de 6 mm (0,236 po) (pour une cosse à sertir Molex 19131-0023) ou l'extrémité d'un fil rouge toronné de calibre n° 12 AWG sur une longueur de 8 mm (0,315 po) (pour une cosse à sertir Panduit EV10-6RB-Q).	
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 de l'outil.	
Étape_4	Plier les cosses à sertir à un angle de 45° comme illustré sur l'image.	
Étape_5	Retirer la vis de l'emplacement RTN « B » de la plaque à bornes.	
Étape_6	Insérer le fil rouge serti dans l'emplacement RTN « B » comme illustré sur l'image.	
Étape_7	Visser la cosse à sertir en place.	
Étape_8	Retirer la vis de l'emplacement -48V DC « B » de la plaque à bornes.	
Étape_9	Insérer le fil noir serti dans l'emplacement -48V DC « B » comme illustré sur l'image.	

Étape_10	Visser la cosse à sertir en place.	
Étape_11	(Optionnel) Si une redondance est nécessaire, répéter les étapes 1 à 10 pour un deuxième jeu de câbles. Ils doivent être installés dans les emplacements -48V DC et RTN « A ».	
Étape_12	Le bloc d'alimentation est protégé contre les inversions de polarité. La plateforme démarrera dès qu'une alimentation externe sera appliquée (DEL d'alimentation verte).	

5.6.3 Entrée du bloc d'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.

5.6.3.1 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.

5.6.3.2 Brancher le bloc d'alimentation CA

Étape_1	Brancher un cordon avec une classification appropriée d'une source d'alimentation externe dans le bloc d'alimentation situé à l'avant de la plateforme.	
Étape_2	La plateforme démarrera dès qu'une alimentation externe sera appliquée (DEL d'alimentation verte).	

Pour de l'information sur la mise à la terre, voir Installation de la plateforme dans une étagère.

Pour de l'information sur le comportement des DEL, voir Composants de la plateforme.

5.6.4 Entrée GNSS

5.6.4.1 Connexion à un répartiteur RF

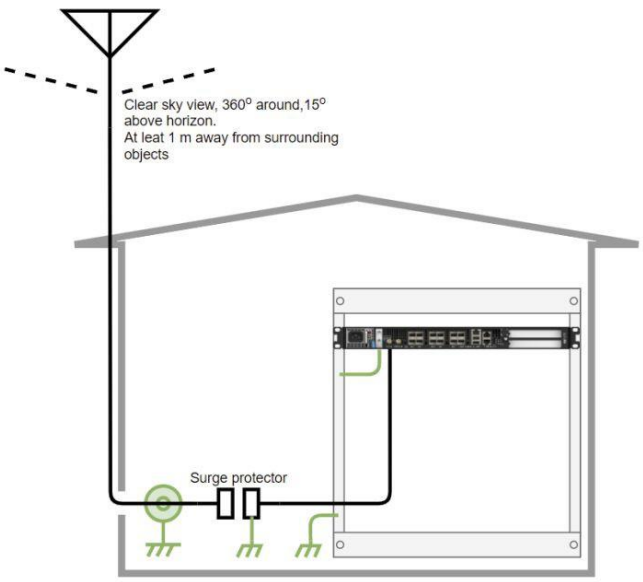
Étape_1	Brancher un câble coaxial de 50 ohms entre le répartiteur et la plateforme. **NOTE :** La plateforme nécessite que le câble soit terminé par un connecteur SMA femelle. Le type de câble n'est pas très important pourvu qu'il reste court entre le répartiteur et la plateforme et qu'une bonne antenne avec un amplificateur à faible bruit soit utilisée.
Étape_2	Suivre les instructions de la documentation du répartiteur RF pour connecter l'antenne.

5.6.4.2 Connexion à une antenne externe

⚠WARNING

Lors de la connexion d'une antenne externe, une mise à la terre appropriée est nécessaire et une protection supplémentaire contre les surtensions pourrait être requise. Toujours se référer au code électrique local.

Il s'agit d'une directive d'installation générale et les utilisateurs sont encouragés à lire les meilleures pratiques d'installation des antennes GNSS des fournisseurs d'antennes.



Étape_1	Choisir une antenne de haute qualité comprenant un amplificateur à faible bruit avec un gain de 15 à 35 dB (en fonction de la distance entre l'antenne et le récepteur).
Étape_2	Installer l'antenne dans un endroit où il y a une vue dégagée du ciel, idéalement plus haut que les objets, bâtiments ou arbres environnants. Utiliser un support solide pour minimiser les mouvements dus aux vents forts.
Étape_3	Utiliser un câble coaxial de 50 ohms de haute qualité, tel que le LMR-400, pour connecter l'antenne au bloc de mise à la terre ou au parasurtenseur. La terminaison de type N est un bon choix pour l'antenne, le câble et le bloc de mise à la terre ou le parasurtenseur.
Étape_4	Installer un bloc de mise à la terre et/ou un parasurtenseur à proximité de l'entrée du câble coaxial dans le bâtiment et le connecter à la mise à la terre du bâtiment. Toujours se référer au code électrique local. La plateforme comprend une protection contre les surtensions allant jusqu'à 1 kV.
Étape_5	Utiliser un câble coaxial de 50 ohms de haute qualité, tel que le LMR-400, entre le bloc de mise à la terre et le parasurtenseur et la plateforme. Ce câble nécessite une connexion SMA du côté de la plateforme.

6/ Accès aux composants de la plateforme

6.1 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 Redfish
- En utilisant IPMI sur LAN (IOL)
- En utilisant IPMI via KCS

Voir Description des méthodes d'accès au système pour plus d'information sur les différentes méthodes d'accès.

6.1.1 Accéder au BMC en utilisant l'interface utilisateur Web

6.1.1.1 Préalables

1	L'adresse IP du BMC est connue.
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.

Sections pertinentes :

Découvrir les adresses IP de la plateforme

Configuration réseau du BMC

6.1.1.2 Considérations relatives au navigateur

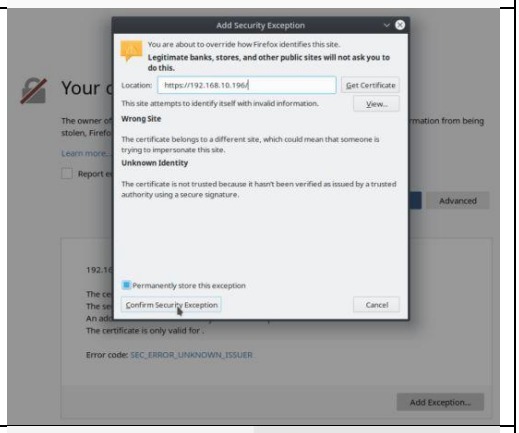
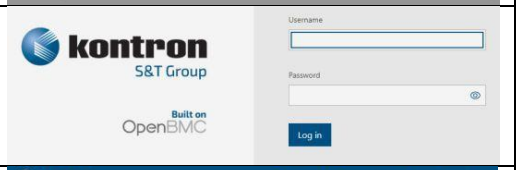
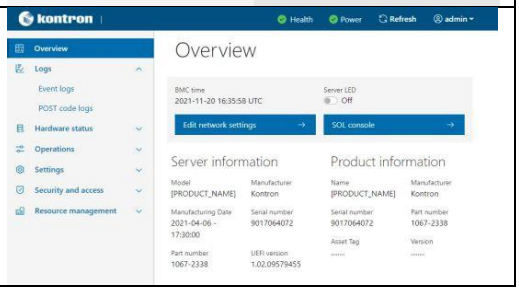
HTML5	Pour établir une communication avec l'interface utilisateur Web, un navigateur Web prenant en charge HTML5 est nécessaire.
Certificat auto-signé HTTPS	Lors de l'établissement d'une connexion à l'interface utilisateur Web, il est obligatoire d'accepter le certificat auto-signé HTTPS. Pour plus d'information 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.

6.1.1.3 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.	
Étape_5	Vous avez maintenant accès à l'interface utilisateur Web de gestion du BMC. Vous pouvez utiliser l'interface.	

6.1.2 Accéder au BMC en utilisant Redfish

Il existe deux méthodes pour accéder au BMC :

- Via une connexion réseau externe
- Via l'interface hôte Redfish interne

6.1.2.1 Accéder au BMC en utilisant Redfish via une connexion réseau externe

6.1.2.1.1 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 :

Découvrir les adresses IP de la plateforme

Configuration et gestion des utilisateurs (si un mot de passe doit être modifié)

6.1.2.1.2 Créer l'URL racine Redfish

Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut.

Étape_1	Commencer l'URL par le préfixe https.	**https://**
Étape_2	Ajouter le nom d'utilisateur et le mot de passe pour le BMC, séparés par le deux-points.	**https:// [NOM D'UTILISATEUR BMC] : [MOT DE PASSE BMC]**
Étape_3	Ajouter @ à l'URL, puis l'adresse IP du BMC.	**https:// [NOM D'UTILISATEUR BMC] : [MOT DE PASSE BMC] @ [IP_GESTION_BMC]** Dans la documentation, cette URL sera remplacée par [URL_RACINE] dans toutes les commandes Redfish.
Étape_4	Accéder à l'API à l'aide d'un client HTTP et vérifier que l'URL est valide.	InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE]/redfish/v1/ | jq**

6.1.2.1.3 Procédure d'accès

Étape_1	Accéder à Redfish. InviteSE_OrdinateurDistant:~# **curl -k -s – request GET --url [URL_RACINE] /redfish/v1/ | jq**	

6.1.2.2 Accéder au BMC via l'interface hôte Redfish interne

Les ressources de BMC Redfish sont accessibles localement via le serveur intégré à l'aide de l'interface hôte Redfish interne et privée. Dans le ME1310, cette fonction est disponible grâce à l'interface USB vers LAN. La plupart des systèmes d'exploitation Linux modernes devraient intégrer la prise en charge de ce périphérique USB vers LAN.

6.1.2.2.1 Préalables

1	L'adresse IP de l'interface hôte Redfish est configurée.
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 :

Configurer l'interface hôte Redfish

Configuration et gestion des utilisateurs (si un mot de passe doit être modifié)

6.1.2.2.2 Créer l'URL racine Redfish afin de l'utiliser avec l'interface hôte Redfish

Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut.

Étape_1	Commencer l'URL par le préfixe https.	**https://**
Étape_2	Ajouter le nom d'utilisateur et le mot de passe pour le BMC, séparés par le deux-points.	**https:// [NOM D'UTILISATEUR BMC] : [MOT DE PASSE BMC]**
Étape_3	Ajouter @ à l'URL, puis l'adresse IP configurée pour l'interface hôte Redfish.	**https:// [NOM D'UTILISATEUR BMC] : [MOT DE PASSE BMC] @ 169.254.0.17** Dans la documentation, cette URL sera remplacée par [URL_RACINE] dans toutes les commandes Redfish.
Étape_4	Accéder à l'API à l'aide d'un client HTTP et vérifier que l'URL est valide.	InviteSE_OrdinateurDistant:~# **curl -k -s [URL_RACINE] /redfish/v1/ | jq**

6.1.2.2.3 Procédure d'accès

Étape_1	Accéder à Redfish. InviteSE_OrdinateurDistant:~# **curl -k -s -- request GET --url [URL_RACINE] /redfish/v1/ | jq**	

6.1.3 Accéder au BMC en utilisant IPMI sur LAN (IOL)

6.1.3.1 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 :

Découvrir les adresses IP de la plateforme

Configuration réseau du BMC

6.1.3.2 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.

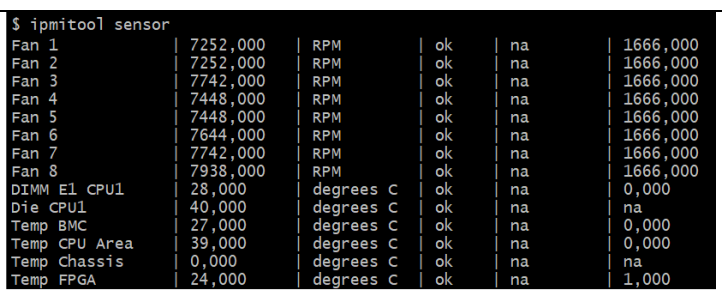
Étape_1	À partir d'un ordinateur distant ayant accès au sous-réseau du réseau de gestion, saisir la commande souhaitée. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] -C 17 [COMMANDE_IPMI]**	

6.1.4 Accéder au BMC en utilisant IPMI via KCS

6.1.4.1 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.

6.1.4.2 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]**	

6.2 Accéder au système d'exploitation d'un serveur

Un système d'exploitation est accessible par différentes méthodes :

- En utilisant le KVM – il s'agit de la méthode recommandée pour la configuration initiale d'un système sorti de son emballage
- En utilisant la console série sur LAN de l'interface utilisateur Web
- En utilisant série sur LAN via SSH
  En utilisant série sur LAN via IPMI
- En utilisant les protocoles SSH, RDP et des applications clients
- En utilisant une console série (connexion physique)

Voir Description des méthodes d'accès au système pour plus d'information sur les différentes méthodes d'accès.

NOTE : Cette plateforme ne comporte pas de port d'affichage physique.

6.2.1 Accéder à un système d'exploitation en utilisant le KVM

NOTE : Le KVM n'est pas adapté à la surveillance ou à la configuration du chargeur d'amorçage (bootloader) du système d'exploitation en raison du délai de rafraîchissement du KVM au démarrage. Le KVM peut cependant être utilisé pour la configuration du système d'exploitation. La fenêtre du KVM sera redimensionnée après l'affichage de l'UEFI/BIOS, ce qui peut rendre l'affichage du chargeur d'amorçage indisponible. Le rafraîchissement complet de la page du navigateur Web pourrait rendre possible la surveillance du chargeur d'amorçage du système d'exploitation (utiliser le bouton de rafraîchissement du navigateur ou la touche F5, qui fonctionne dans la plupart des navigateurs). Une autre méthode consiste à configurer le chargeur d'amorçage pour rediriger la sortie vers le port série. Voir la documentation du système d'exploitation pour configurer la sortie du chargeur d'amorçage.

6.2.1.1 Préalables

1	Un système d'exploitation est installé.
2	L'adresse IP du BMC est connue.
3	L'ordinateur distant a accès au sous-réseau du réseau de gestion.

Sections pertinentes :

Accéder au BMC

Découvrir les adresses IP de la plateforme

Gestion de l'alimentation de la plateforme

6.2.1.2 Considérations relatives au navigateur

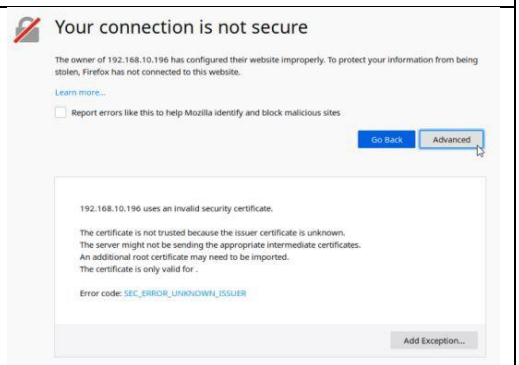
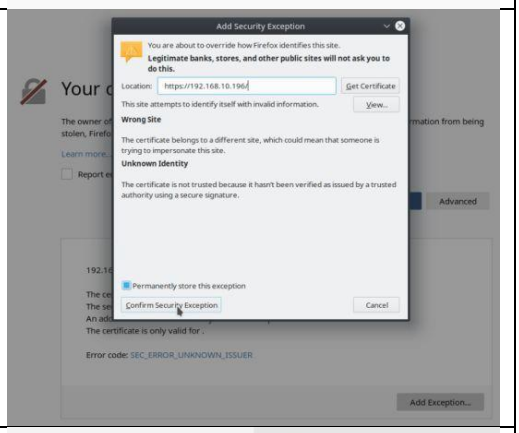
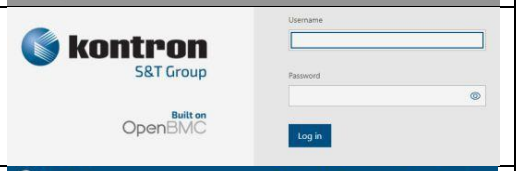
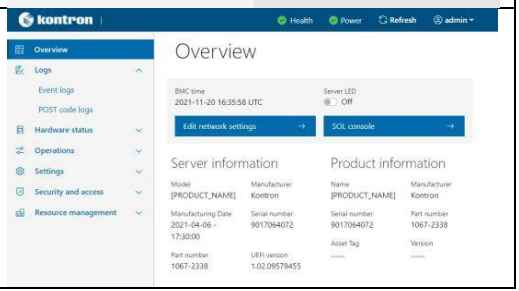
HTML5	Pour établir une communication avec l'interface utilisateur Web, un navigateur Web prenant en charge HTML5 est nécessaire.
Certificat auto-signé HTTPS	Lors de l'établissement d'une connexion à l'interface utilisateur Web, il est obligatoire d'accepter le certificat auto-signé HTTPS. Pour plus d'information 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.

6.2.1.3 Procédure d'accès

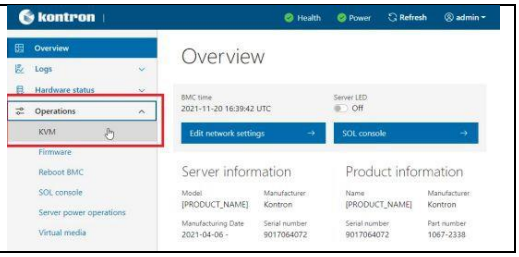
6.2.1.3.1 Accéder au BMC du serveur pour lequel vous souhaitez accéder au système d'exploitation

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.	
Étape_5	Vous avez maintenant accès à l'interface utilisateur Web de gestion du BMC. Vous pouvez utiliser l'interface.	

6.2.1.3.2 Lancer le KVM

NOTE : Le KVM perd parfois la connexion. Il suffit de rafraîchir la page du navigateur Web pour établir la connexion.

Étape_1	Dans l'interface utilisateur Web du BMC, cliquer sur le menu **Operations**, puis sur le bouton **KVM**.	

Étape_2	L'écran du système d'exploitation devrait s'afficher.	

NOTE : Si le système d'exploitation n'est pas affiché, réinitialiser le serveur. Voir la section Gestion de l'alimentation de la plateforme.

6.2.2 Accéder à un système d'exploitation en utilisant la console série sur LAN de l'interface utilisateur Web

6.2.2.1 Préalables

1	Un système d'exploitation est installé.
2	L'adresse IP du BMC est connue.
3	L'ordinateur distant a accès au sous-réseau du réseau de gestion.
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.

Sections pertinentes :

Accéder au BMC

Découvrir les adresses IP de la plateforme

Gestion de l'alimentation de la plateforme

6.2.2.2 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 utilisateur 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.

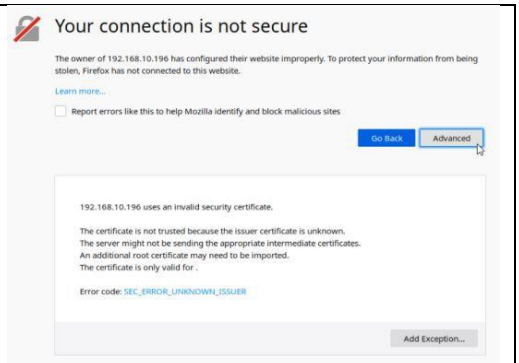
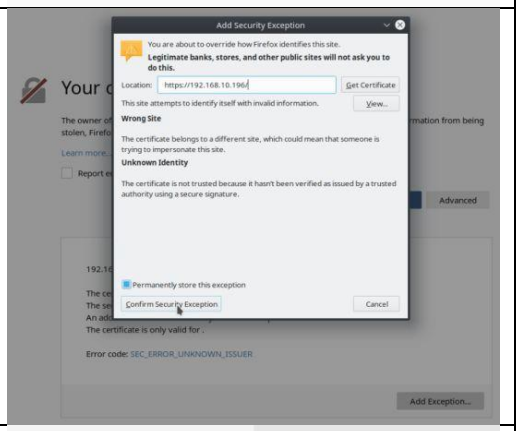
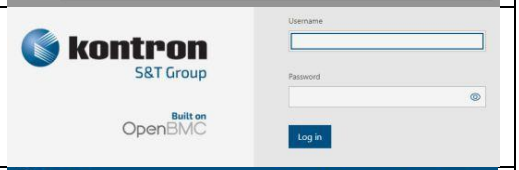
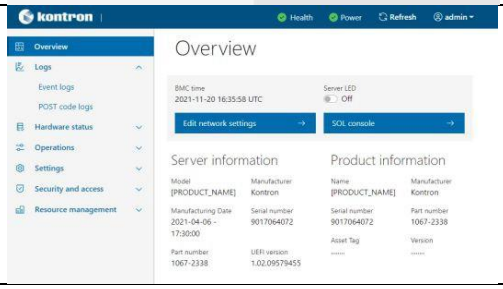
NOTE : La procédure peut varier selon le navigateur utilisé. Les exemples fournis utilisent Firefox.

6.2.2.3 Procédure d'accès

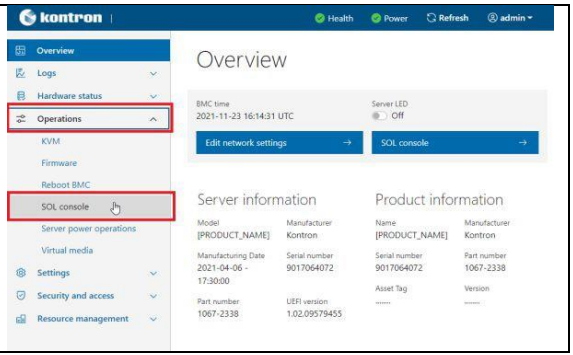
6.2.2.3.1 Accéder au BMC du serveur pour lequel vous souhaitez accéder au système d'exploitation

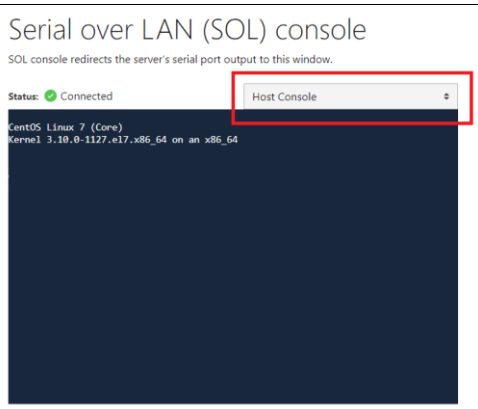
Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut.

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.	
Étape_5	Vous avez maintenant accès à l'interface utilisateur Web de gestion du BMC. Vous pouvez utiliser l'interface.	

6.2.2.3.2 Lancer la console SOL de l'interface utilisateur Web

Étape_1	Dans l'interface utilisateur Web du BMC, cliquer sur le menu **Operations**, puis sur le bouton **SOL console**.	

Étape_2	L'écran du système d'exploitation devrait s'afficher. **NOTE :** Si l'écran ne s'affiche pas, s'assurer que le menu déroulant est réglé sur **Host Console**.	

NOTE : Si le système d'exploitation n'est pas affiché, réinitialiser le serveur. Voir la section Gestion de l'alimentation de la plateforme.

6.2.3 Accéder à un système d'exploitation en utilisant série sur SSH

6.2.3.1 Préalables

1	Un système d'exploitation est installé.
2	L'adresse IP du BMC est connue.
3	L'ordinateur distant a accès au sous-réseau du réseau de gestion.
4	Un outil client SSH est installé sur l'ordinateur distant. **NOTE :** PuTTY est recommandé pour les environnements Windows, et SSH est recommandé pour les environnements Linux.
5	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.

Sections pertinentes :

Découvrir les adresses IP de la plateforme

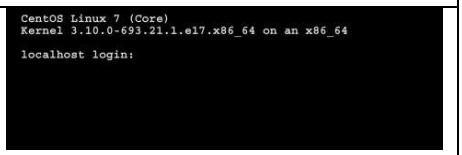
Installation des logiciels courants

Accéder au BMC

6.2.3.2 Procédure d'accès

NOTE : Lorsque série sur SSH est utilisé, appuyer sur **Entrée**, puis sur le **~** pour quitter la session.

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 l'aide d'un outil client SSH, ouvrir une session SSH avec les paramètres suivants : Adresse IP du BMC Numéro de port du serveur : 2200	
Étape_2	Ouvrir une session sur le BMC à l'aide des données d'accès appropriées. Une fois la connexion établie, appuyer sur **Entrée** pour obtenir une réponse de la console série du système d'exploitation.	

6.2.4 Accéder à un système d'exploitation en utilisant série sur LAN via IPMI

6.2.4.1 Préalables

1	Un système d'exploitation est installé.
2	L'adresse IP du BMC est connue.
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 :

Découvrir les adresses IP de la plateforme

Gestion de l'alimentation de la plateforme

6.2.4.2 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 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] -C 17 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] -C 17 sol activate**	
Étape_3	L'écran de démarrage du système d'exploitation s'affiche.	

NOTE : Si le système d'exploitation n'est pas affiché, réinitialiser le serveur. Voir la section Gestion de l'alimentation de la plateforme.

6.2.5 Accéder à un système d'exploitation en utilisant le protocole SSH, RDP ou des applications clients

6.2.5.1 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.

Section pertinente :

Gestion de l'alimentation de la plateforme

6.2.5.2 Procédure d'accès

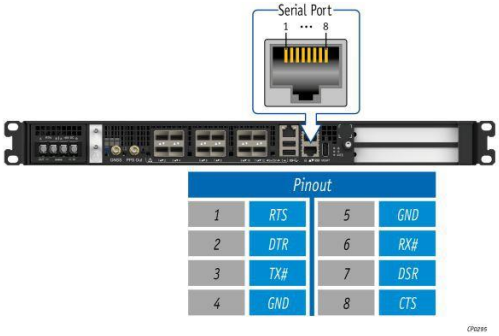
Étape_1	En utilisant l'adresse IP du système d'exploitation, utiliser la méthode d'accès à distance de votre choix.

6.2.6 Accéder au système d’exploitation en utilisant une console série (connexion physique)

6.2.6.1 Préalables

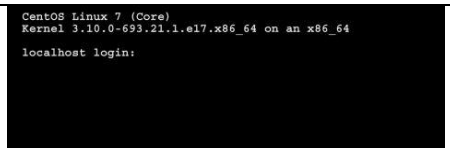
1	Un système d'exploitation est installé.
2	Une connexion physique à l'appareil est requise. **NOTE :** Le port de console série est compatible avec le câble 72-3383-01 de Cisco.
3	Un outil de console série est installé sur l'ordinateur distant. • Vitesse (baud) : 115200 • Bits d'information : 8 • Bits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

6.2.6.2 Emplacement du port



6.2.6.3 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	Connecter physiquement un ordinateur au port série de la plateforme.	
Étape_2	À l'aide d'un outil de console série, établir la communication en utilisant les paramètres fournis. Appuyer sur **Entrée**.	
Étape_3	L'écran de démarrage du système d'exploitation s'affiche.	

NOTE : Si le système d'exploitation n'est pas affiché, réinitialiser le serveur. Voir la section Gestion de l'alimentation de la plateforme.

6.3 Accéder à l’UEFI/BIOS

L’UEFI/BIOS est accessible par différentes méthodes :

- Série sur LAN (SOL) via l’interface utilisateur Web – il s’agit de la méthode recommandée pour la configuration initiale d'un système sorti de son emballage
- KVM
- Série sur SSH
- Série sur LAN (SOL) via IPMI
- Console série (connexion physique)

Voir Description des méthodes d'accès au système pour plus d'information sur les différentes méthodes d'accès.

6.3.1 Accéder à l'UEFI/BIOS en utilisant série sur LAN via l'interface utilisateur Web

6.3.1.1 Préalables

1	L'adresse IP du BMC est connue.
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.

Section pertinente :

Découvrir les adresses IP de la plateforme

6.3.1.2 Considérations relatives au navigateur

HTML5	Pour établir une communication avec l'interface utilisateur Web, un navigateur Web
Certificat auto-signé HTTPS	Lors de l'établissement d'une connexion à l'interface utilisateur 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	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
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.

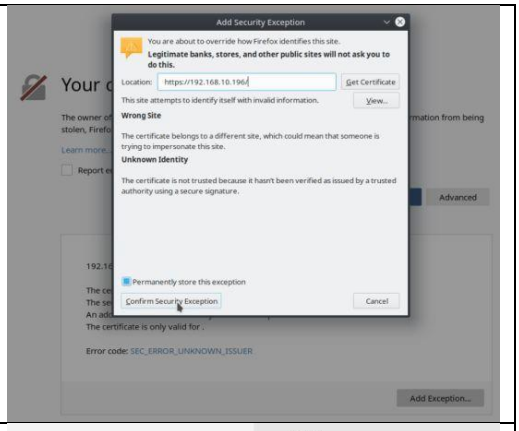
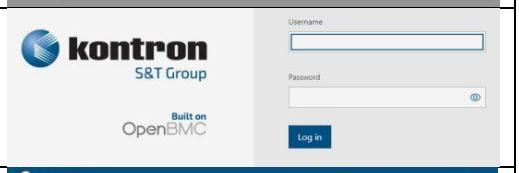
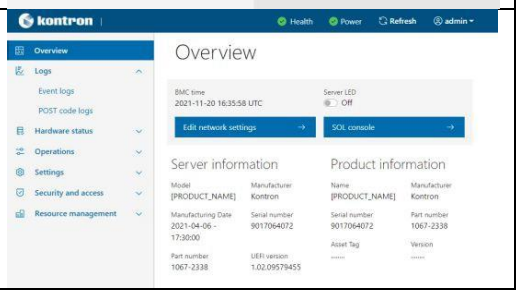
NOTE : La procédure peut varier selon le navigateur utilisé. Les exemples fournis utilisent Firefox.

6.3.1.3 Procédure d'accès

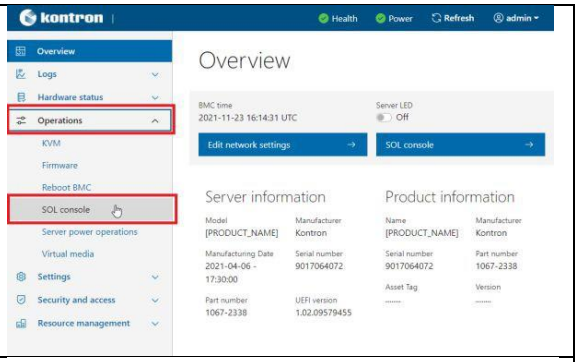
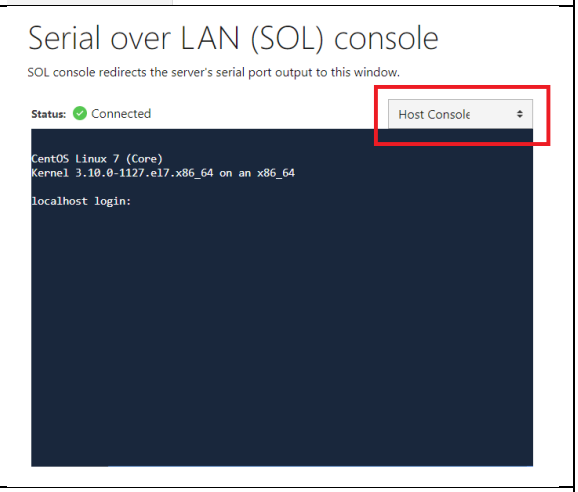
Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut.

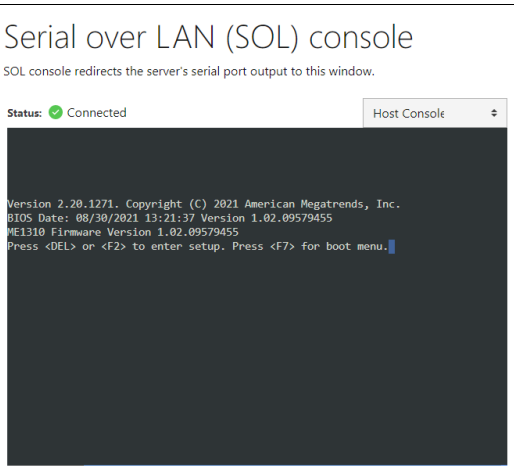
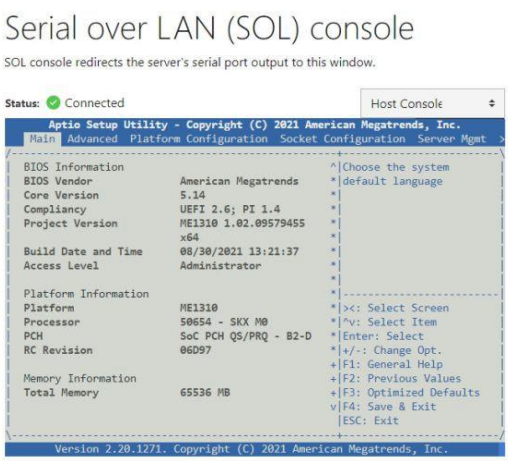
6.3.1.4 Accéder à l'interface utilisateur Web du BMC

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.	
Étape_5	Vous avez maintenant accès à l'interface utilisateur Web de gestion du BMC. Vous pouvez utiliser l'interface.	

6.3.1.5 Accéder au menu de configuration de l'UEFI/BIOS via SOL en utilisant l'interface utilisateur Web

Étape_1	Dans l'interface utilisateur Web du BMC, cliquer sur le menu **Operations**, puis sur le bouton **SOL console**.	
Étape_2	Appuyer sur une flèche du clavier pour rafraîchir la console. L'écran du système d'exploitation devrait s'afficher. **NOTE :** Si l'écran ne s'affiche pas, s'assurer que le menu déroulant est réglé sur **Host Console**.	
Étape_3	Si le système est déjà démarré, réinitialiser le serveur. Sinon, démarrer le serveur.	

Étape_4	Lorsque l'écran d'accueil de l'UEFI/BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration de l'UEFI/BIOS. **NOTE :** Lorsqu'une commande de réinitialisation du serveur est lancée, quelques secondes peuvent s'écouler avant que l'écran d'accueil de l'UEFI/BIOS ne s'affiche. **NOTE :** Il peut s'écouler quelques secondes avant que l'écran d'accueil de l'UEFI/BIOS n'affiche le message de confirmation "Entering Setup…".	
Étape_5	L'écran d'accueil de l'UEFI/BIOS affiche "Entering Setup...". **NOTE :** L'affichage et l'entrée dans le menu de configuration de l'UEFI/BIOS pourraient prendre quelques secondes.	
Étape_6	Le menu de configuration de l'UEFI/BIOS s'affiche.	

6.3.2 Accéder à l'UEFI/BIOS en utilisant le KVM

NOTE : Le KVM n'est pas adapté à la configuration de l'UEFI/BIOS en raison du délai de rafraîchissement du KVM au démarrage de l'UEFI/BIOS. Le KVM peut cependant être utilisé pour la configuration de l'UEFI/BIOS mais, lorsque l'UEFI/BIOS démarre, la fenêtre du KVM sera redimensionnée et inutilisable jusqu'à ce qu'un rafraîchissement complet de la page du navigateur Web soit effectué (utiliser le bouton d'actualisation du navigateur ou la touche F5, qui fonctionne dans la plupart des navigateurs). Après le rafraîchissement, le KVM devrait être stable et fonctionnel jusqu'au prochain redémarrage de l'UEFI/BIOS.

6.3.2.1 Préalables

1	L'adresse IP du BMC est connue.
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.

Section pertinente :

Découvrir les adresses IP de la plateforme

6.3.2.2 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 utilisateur 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.

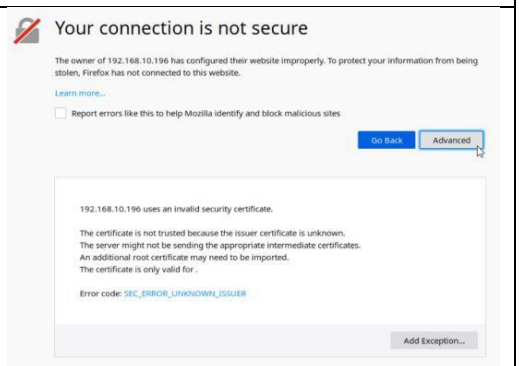
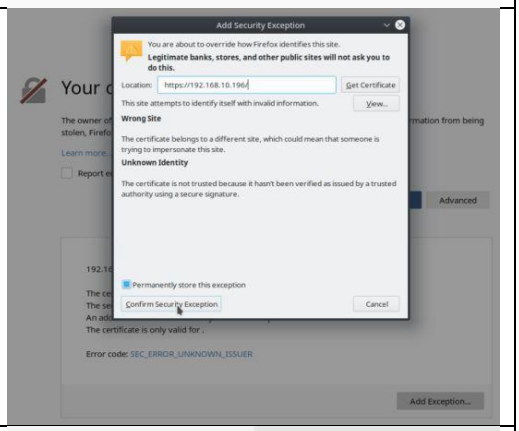
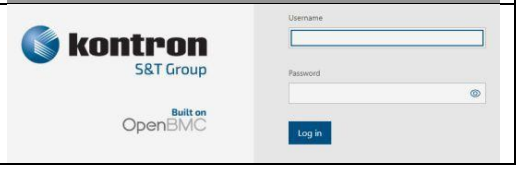
NOTE : La procédure peut varier selon le navigateur utilisé. Les exemples fournis utilisent Firefox.

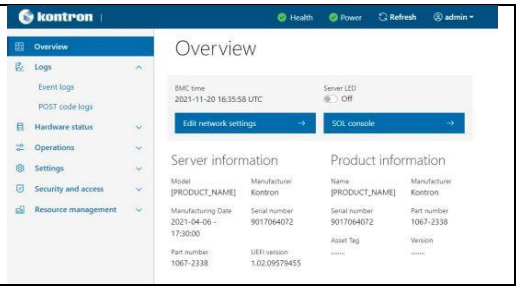
6.3.2.3 Procédure d'accès

Pour les noms d'utilisateur et les mots de passe par défaut, voir Noms d'utilisateur et mots de passe par défaut.

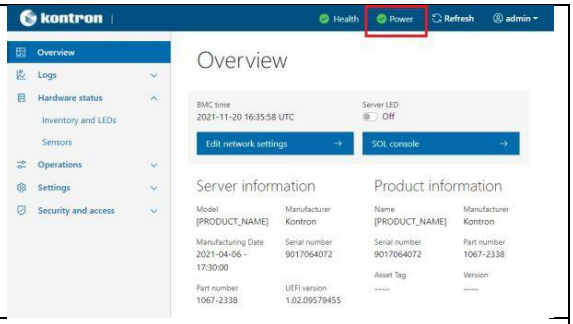
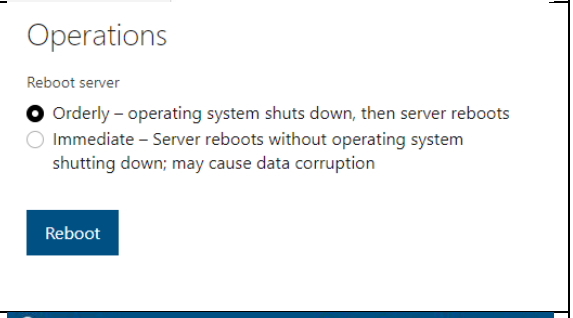
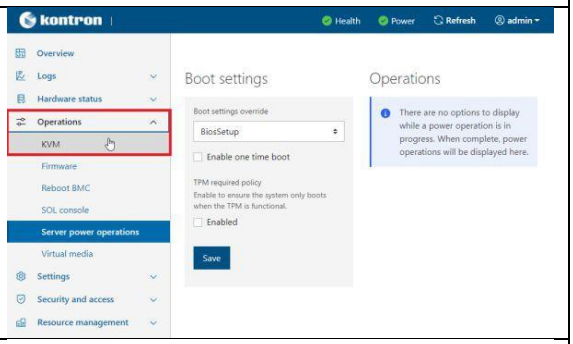
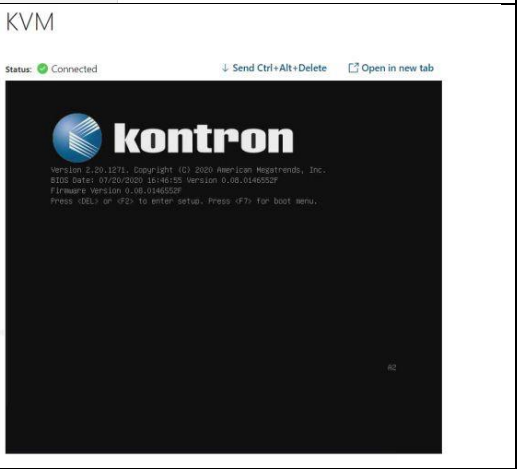
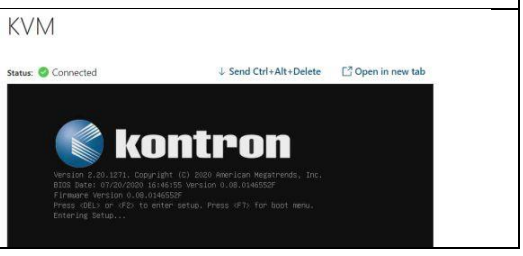
NOTE : Le KVM perd parfois la connexion. Il suffit de rafraîchir la page du navigateur Web pour établir la connexion.

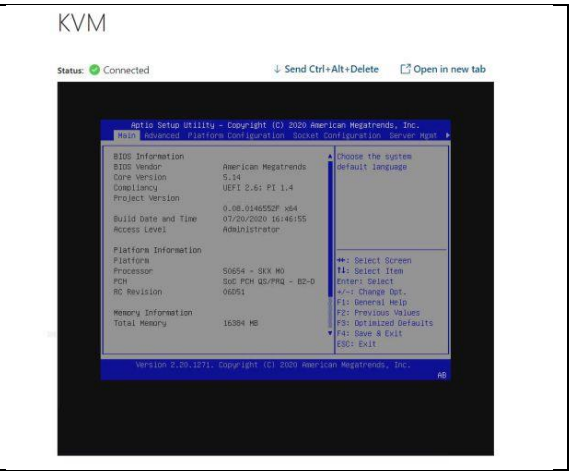
6.3.2.4 Accéder à l'interface utilisateur Web du BMC

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.	

Étape_5	Vous avez maintenant accès à l'interface utilisateur Web de gestion du BMC. Vous pouvez utiliser l'interface.	

6.3.2.5 Accéder au menu de configuration de l'UEFI/BIOS en utilisant le KVM

Étape_1	Dans l'interface utilisateur Web du BMC, cliquer sur le bouton **Power**.	
Étape_2	Dans la section **Reboot server**, sélectionner **Orderly**, puis cliquer sur **Reboot**.	
Étape_3	Dans le menu **Operations**, cliquer sur **KVM**.	
Étape_4	Lorsque l'écran d'accueil de l'UEFI/BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration de l'UEFI/BIOS. **NOTE :** Lorsqu'une commande de réinitialisation du serveur est lancée, quelques secondes peuvent s'écouler avant que l'écran d'accueil de l'UEFI/BIOS ne s'affiche. **NOTE :** Il peut s'écouler quelques secondes avant que l'écran d'accueil de l'UEFI/BIOS n'affiche le message de confirmation "Entering Setup…".	
Étape_5	L'écran d'accueil de l'UEFI/BIOS affiche "Entering Setup...". **NOTE :** L'affichage et l'entrée dans le menu de configuration de l'UEFI/BIOS pourraient prendre quelques secondes.	

Étape_6	Le menu de configuration de l'UEFI/BIOS s'affiche.	

6.3.3 Accéder à l'UEFI/BIOS en utilisant série sur SSH

6.3.3.1 Préalables

1	L'adresse IP du BMC est connue.
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.
3	Un outil client SSH est installé sur l'ordinateur distant. **NOTE :** PuTTY est recommandé pour les environnements Windows, et SSH est recommandé pour les environnements Linux.

Sections pertinentes :

Découvrir les adresses IP de la plateforme

Installation des logiciels courants

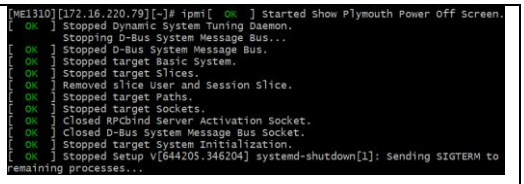
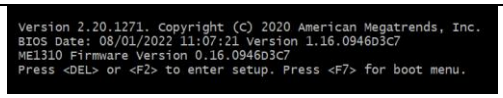
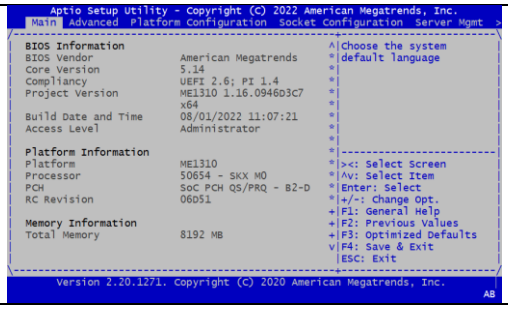
Accéder au BMC

Noms d'utilisateur et mots de passe par défaut

6.3.3.2 Procédure d'accès

NOTE : Lorsque série sur SSH est utilisé, appuyer sur **Entrée**, puis sur le **~** pour quitter la session.

Étape_1	À l'aide d'un outil client SSH, ouvrir une session SSH avec les paramètres suivants : • Adresse IP du BMC • Nom d'utilisateur et mot de passe pour le BMC • Numéro de port du serveur : 2200 Une fois le mot de passe saisi, appuyer sur la touche **Entrée** pour générer une réponse du logiciel en cours d'exécution sur le serveur.	

Étape_2	Redémarrer le serveur en utilisant votre méthode privilégiée. Voici quelques exemples : • Ouvrir une session dans l'interface utilisateur Web du BMC et procéder au redémarrage. • Si le serveur exécute actuellement un système d'exploitation installé, ouvrir une session et lancer la commande de redémarrage appropriée. • Si le serveur exécute actuellement le shell UEFI intégré, lancer la commande « reset ». **NOTE :** Lorsqu'une commande de réinitialisation du serveur est lancée, quelques secondes peuvent s'écouler avant que l'écran d'accueil de l'UEFI/BIOS ne s'affiche.	
Étape_3	L'écran d'accueil de l'UEFI/BIOS devrait afficher "Entering Setup...". Appuyer sur la touche spécifiée pour accéder au menu de configuration de l'UEFI/BIOS. **NOTE :** L'affichage et l'entrée dans le menu de configuration de l'UEFI/BIOS prendront quelques secondes.	
Étape_4	Le menu de configuration de l'UEFI/BIOS devrait s'afficher.	

6.3.4 Accéder à l'UEFI/BIOS en utilisant série sur LAN via IPMI

6.3.4.1 Préalables

1	Un système d'exploitation est installé.
2	L'adresse IP du BMC est connue.
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.

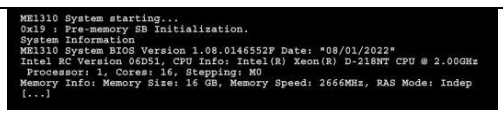
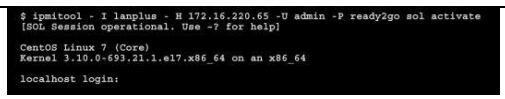
Sections pertinentes :

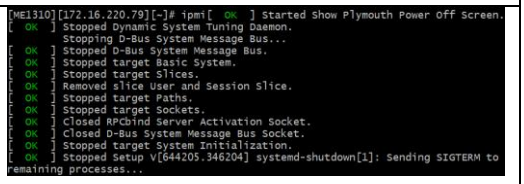
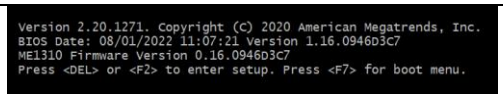
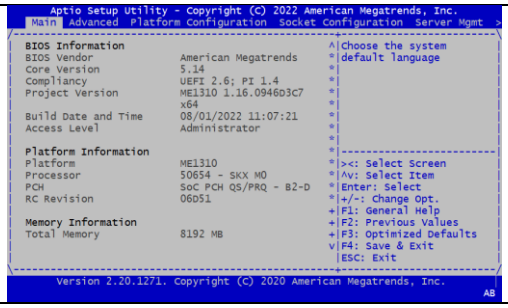
Découvrir les adresses IP de la plateforme

Installation des logiciels courants

6.3.4.2 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 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] -C 17 sol deactivate**	
Étape_2	Activer une session SOL. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] -C 17 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	À partir d'une autre fenêtre de ligne de commande, faire en sorte que la plateforme entre dans l'UEFI/BIOS automatiquement au prochain redémarrage à l'aide de la commande suivante. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] -C 17 chassis bootdev bios**	
Étape_4	À partir de la même fenêtre de ligne de commande, réinitialiser le serveur. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] -C 17 chassis power reset** **NOTE :** Lorsqu'une commande de réinitialisation du serveur est lancée, quelques secondes peuvent s'écouler avant que l'écran d'accueil de l'UEFI/BIOS ne s'affiche.	
Étape_5	L'écran d'accueil de l'UEFI/BIOS devrait afficher "Entering Setup...". **NOTE :** L'affichage et l'entrée dans le menu de configuration de l'UEFI/BIOS prendront quelques secondes.	
Étape_6	Le menu de configuration de l'UEFI/BIOS devrait s'afficher.	

6.3.5 Accéder à l'UEFI/BIOS en utilisant une console série à partir d'une connexion physique

6.3.5.1 Préalables

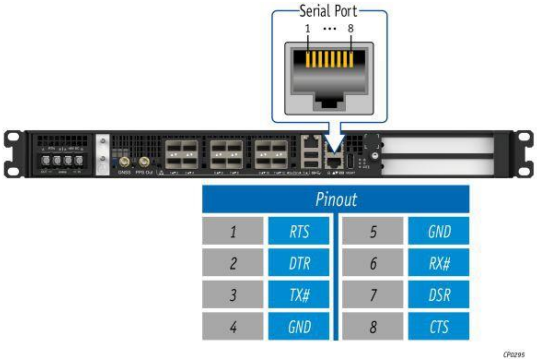
1	Une connexion physique à l'appareil est requise. **NOTE :** Le port de console série est compatible avec le câble 72-3383-01 de Cisco.
2	Un outil de console série est installé sur l'ordinateur distant. • Vitesse (baud) : 115200 • Bits d'information : 8 • Bits d'arrêt : 1 • Parité : Aucune • Contrôle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

Sections pertinentes :

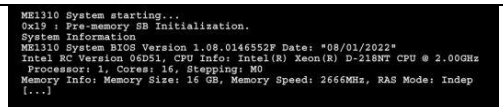
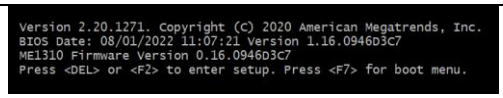
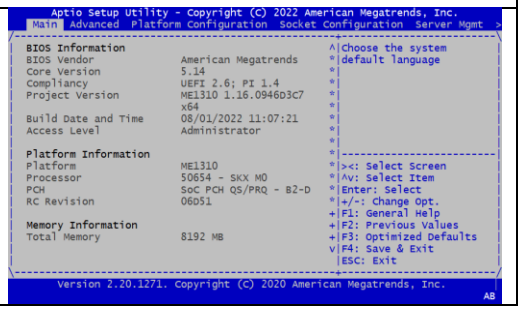
Installation des logiciels courants

Envoi d'une commande BREAK sur une connexion série

6.3.5.2 Emplacement du port



6.3.5.3 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 en utilisant l'une des options suivantes : • Si le serveur exécute actuellement un système d'exploitation installé, ouvrir une session et lancer la commande de redémarrage appropriée. • Si le serveur exécute actuellement le shell UEFI intégré, lancer la commande « reset ». • Envoyez une commande BREAK sur la connexion série en utilisant la méthode disponible dans l'émulateur de terminal. • Débrancher tous les câbles d'alimentation pendant 30 secondes, puis les rebrancher. **NOTE :** Si un système d'exploitation est installé, une méthode faisant appel à un 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 de l'UEFI/BIOS ne s'affiche.	
Étape_3	Lorsque l'écran d'accueil de l'UEFI/BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration de l'UEFI/BIOS. **NOTE :** Il peut s'écouler quelques secondes avant que l'écran d'accueil de l'UEFI/BIOS n'affiche le message de confirmation "Entering Setup…".	
Étape_4	L'écran d'accueil de l'UEFI/BIOS affiche "Entering Setup…". **NOTE :** L'affichage et l'entrée dans le menu de configuration de l'UEFI/BIOS prendront quelques secondes.	
Étape_5	Le menu de configuration de l'UEFI/BIOS s'affiche.	

6.4 Accéder au NOS

L’information présentée dans cette section ne concerne que les plateformes équipées du module d'E/S de commutation Ethernet.

Le NOS est accessible par différentes méthodes :

- En utilisant l’interface utilisateur Web du NOS
- En utilisant la console SOL de l’interface utilisateur Web du BMC
- En utilisant série sur SSH à partir d'un ordinateur distant
- En utilisant SSH à partir d'un ordinateur distant
- En utilisant SSH à partir du serveur intégré

Voir Description des méthodes d'accès au système pour plus d'information sur les différentes méthodes d'accès.

6.4.1 Accéder au NOS en utilisant l’interface utilisateur Web

6.4.1.1 Préalables

1	L'une des adresses IP du NOS est connue.
2	L'ordinateur distant est dans le même sous-réseau que le commutateur.

Section pertinente :

Découvrir les adresses IP de la plateforme

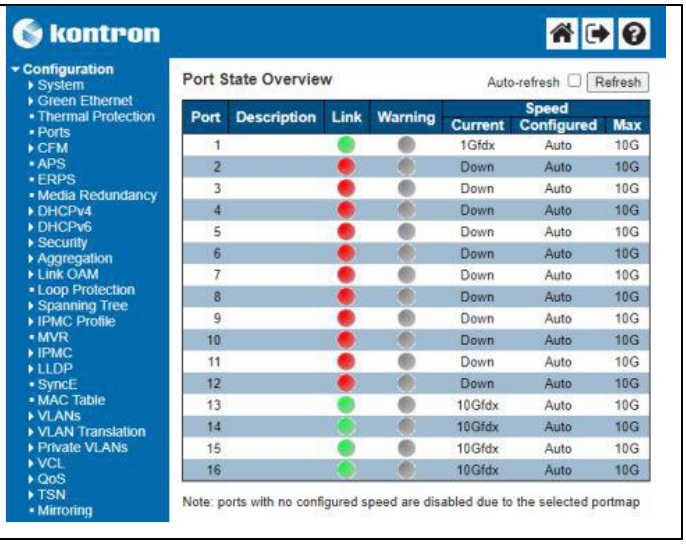
6.4.1.2 Considérations relatives au navigateur

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 utilisateur 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.

6.4.1.3 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 même sous-réseau que le commutateur, ouvrir une fenêtre de navigateur et entrer l'adresse IP découverte pour le commutateur. *http://[IP_NOS]*	

6.4.2 Accéder au CLI du NOS en utilisant la console série sur LAN de l'interface utilisateur Web du BMC

6.4.2.1 Préalables

1	L'adresse IP du BMC est connue.
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.

Sections pertinentes :

Accéder au BMC

Découvrir les adresses IP de la plateforme

Gestion de l'alimentation de la plateforme

6.4.2.2 Considérations relatives au navigateur

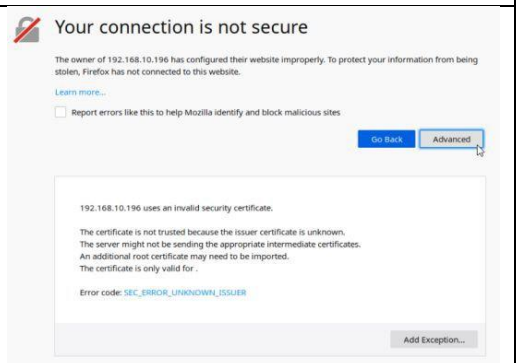
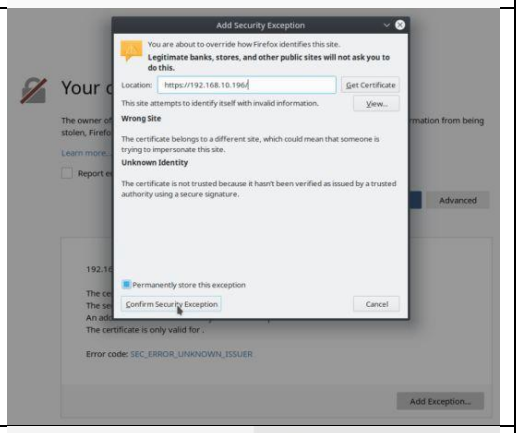
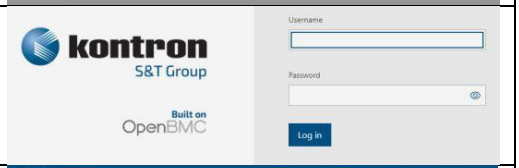
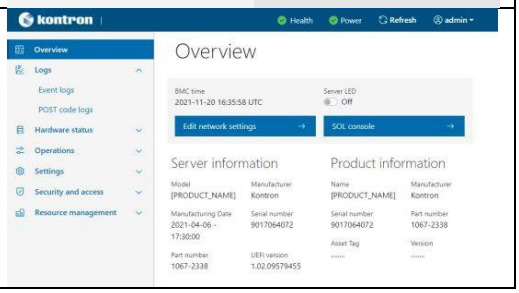
HTML5	Pour établir une communication avec l'interface utilisateur Web, un navigateur Web prenant en charge HTML5 est nécessaire.
Certificat auto-signé HTTPS	Lors de l'établissement d'une connexion à l'interface utilisateur Web, il est obligatoire d'accepter le certificat auto-signé HTTPS. Pour plus d'information 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.

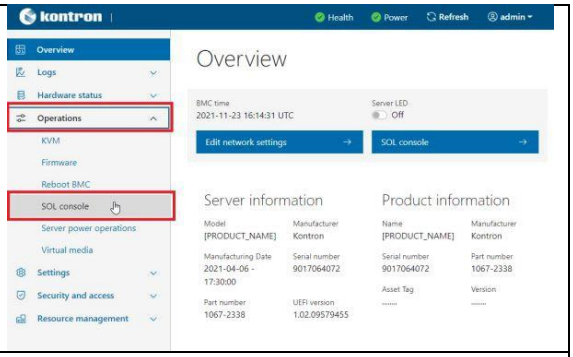
6.4.2.3 Procédure d'accès

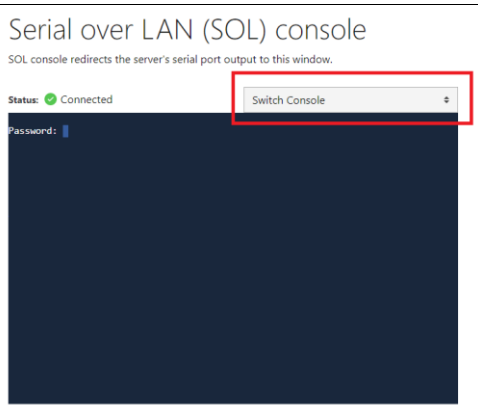
6.4.2.3.1 Accéder au BMC du serveur pour lequel vous souhaitez accéder au NOS

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.	
Étape_5	Vous avez maintenant accès à l'interface utilisateur Web de gestion du BMC. Vous pouvez utiliser l'interface.	

6.4.2.3.2 Lancer la console SOL de l'interface utilisateur Web

Étape_1	Dans l'interface utilisateur Web du BMC, cliquer sur le menu **Operations**, puis sur le bouton **SOL console**.	
Étape_2	Changer la valeur du menu déroulant pour **Switch Console**.	

Étape_3	L'écran du NOS devrait s'afficher.	

NOTE : Si le système d'exploitation n'est pas affiché, réinitialiser le serveur. Voir la section Gestion de l'alimentation de la plateforme.

6.4.3 Accéder au CLI du NOS en utilisant série sur SSH à partir d'un ordinateur distant

6.4.3.1 Préalables

1	L'adresse IP du BMC est connue.
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.
3	Un outil client SSH est installé sur l'ordinateur distant. **NOTE :** PuTTY est recommandé pour les environnements Windows, et SSH est recommandé pour les environnements Linux.

Section pertinente :

Découvrir les adresses IP de la plateforme

6.4.3.2 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. **NOTE :** Lorsque série sur SSH est utilisé, appuyer sur **Entrée**, puis sur le **~** pour quitter la session.

Étape_1	À l'aide d'un outil client SSH, ouvrir une session SSH avec les paramètres suivants : • Adresse IP du BMC • Numéro de port : 2201 (une fois la session ouverte, le BMC redirigera automatiquement la communication vers la console série du NOS)	
Étape_2	Ouvrir une session sur le BMC à l'aide des données d'accès appropriées. Une fois la connexion établie, appuyer sur **Entrée** pour obtenir une réponse du CLI du NOS. Si une session n'est pas déjà ouverte sur la console série du NOS, une autre série de données d'accès sera demandée. Utiliser les données d'accès appropriées afin d'ouvrir la session sur le NOS.	

6.4.4 Accéder au CLI du NOS en utilisant SSH à partir d'un ordinateur distant

6.4.4.1 Préalables

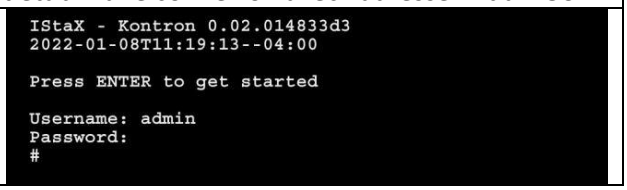
1	L'adresse IP réseau du commutateur est connue.
2	L'ordinateur distant est dans le même sous-réseau que le commutateur.
3	Un outil client SSH est installé sur l'ordinateur distant. **NOTE :** PuTTY est recommandé pour les environnements Windows, et SSH est recommandé pour les environnements Linux.

Section pertinente :

Découvrir les adresses IP de la plateforme

6.4.4.2 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, ouvrir un outil client SSH et établir une connexion avec l'adresse IP du NOS.	
Étape_2	Ouvrir une session dans le CLI du NOS à l'aide des données d'accès appropriées.	

6.4.5 Accéder au CLI du NOS en utilisant SSH à partir du serveur intégré

6.4.5.1 Préalables

1	Un système d'exploitation est installé sur le serveur intégré.
2	L'ordinateur distant a accès au système d'exploitation du serveur intégré.
3	L'une des adresses IP du NOS est connue.
4	Le serveur intégré est dans le même sous-réseau que le commutateur.
5	Un outil client SSH est installé sur l'ordinateur distant. **NOTE :** PuTTY est recommandé pour les environnements Windows, et SSH est recommandé pour les environnements Linux.

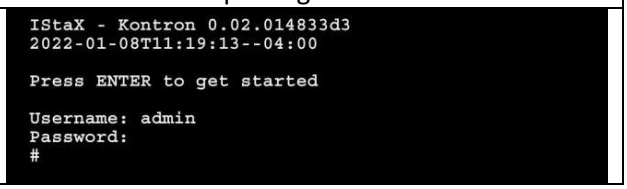
Sections pertinentes :

Découvrir les adresses IP de la plateforme

Accéder au système d'exploitation d'un serveur

6.4.5.2 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	Accéder au système d'exploitation du serveur intégré en utilisant la méthode privilégiée.	
Étape_2	À l'aide d'un outil client SSH, ouvrir une session SSH avec les paramètres suivants : Adresse IP du NOS Ouvrir une session dans le CLI du NOS à l'aide des données d'accès appropriées.	

7/ Découvrir les adresses IP de la plateforme

7.1 Découvrir l'adresse IP du BMC

L'adresse IP du BMC est le minimum requis pour accéder à l'interface utilisateur Web du BMC de la plateforme. Elle est également utilisée pour accéder à l'interface de surveillance et au KVM/VM pour installer un système d'exploitation.

L'adresse IP du BMC peut être découverte :

- En utilisant la mise à jour DNS dynamique par DHCP
- En utilisant l'UEFI/BIOS via la console série (connexion physique) – plateforme sans système d'exploitation installé et sans adresse IP connue
- En utilisant les journaux du serveur DHCP

7.1.1 Découvrir l'adresse IP du BMC de la plateforme en utilisant la mise à jour DNS dynamique par DHCP

7.1.1.1 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	La première adresse MAC attribuée du BMC est connue.

Section pertinente :

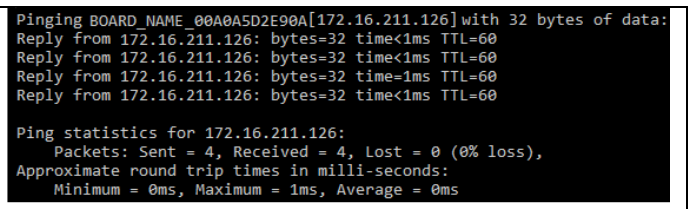
Adresses MAC (pour trouver la première adresse MAC attribuée du BMC)

7.1.1.2 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 du préfixe BMC et de la première adresse MAC du BMC. Voir la section Adresses MAC pour déterminer celles qui sont propres à une plateforme.

Par exemple, si nous utilisons la première adresse MAC du BMC (00:a0:a5:d2:e9:0a), le nom d'hôte sera : BMC 00A0A5D2E90A. Noter qu'il s'agit de la configuration par défaut, mais que le paramètre est configurable par l'utilisateur. La méthode décrite ici ne fonctionne que si le nom d'hôte par défaut est toujours en vigueur.

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 BMC00A0A5D2E90A**	

7.1.2 Découvrir l'adresse IP du BMC de la plateforme en utilisant l'UEFI/BIOS

7.1.2.1 Accéder à l'UEFI/BIOS en utilisant une console série (connexion physique)

7.1.2.1.1 Préalables

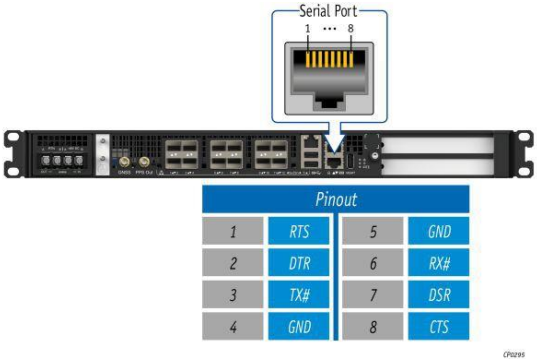
1	Une connexion physique à l'appareil est requise. **NOTE :** Le port de console série est compatible avec le câble 72-3383-01 de Cisco.

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 : Aucune • Mode émulation recommandé : VT100+ **NOTE :** PuTTY est recommandé.

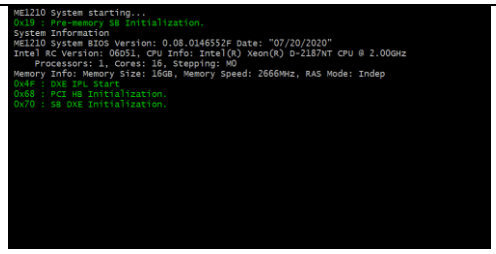
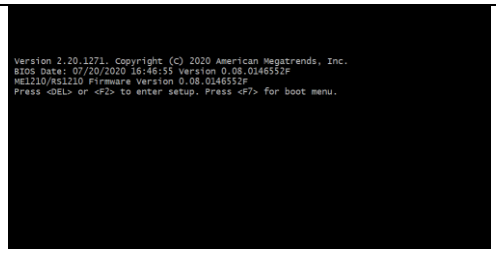
Section pertinente :

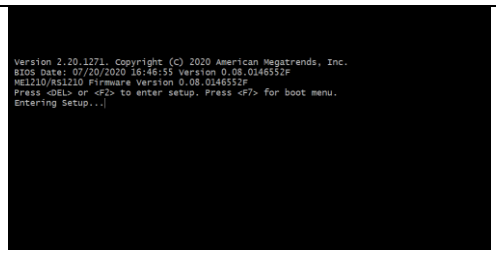
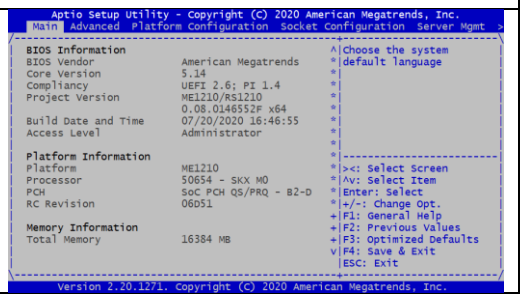
Envoi d'une commande BREAK sur une connexion série

7.1.2.1.2 Emplacement du port



7.1.2.1.3 Accéder au menu de configuration de l'UEFI/BIOS

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 en utilisant l'une des options suivantes : • Si le serveur exécute actuellement un système d'exploitation installé, ouvrir une session et lancer la commande de redémarrage appropriée. • Si le serveur exécute actuellement le shell UEFI intégré, lancer la commande « reset ». • Envoyez une commande BREAK sur la connexion série en utilisant la méthode disponible dans l'émulateur de terminal. • Débrancher tous les câbles d'alimentation pendant 30 secondes, puis les rebrancher. **NOTE :** Si un système d'exploitation est installé, une méthode faisant appel à un 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 de l'UEFI/BIOS ne s'affiche.	
Étape_3	Lorsque l'écran d'accueil de l'UEFI/BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration de l'UEFI/BIOS. **NOTE :** Il peut s'écouler quelques secondes avant que l'écran d'accueil de l'UEFI/BIOS n'affiche le message de confirmation "Entering Setup…".	

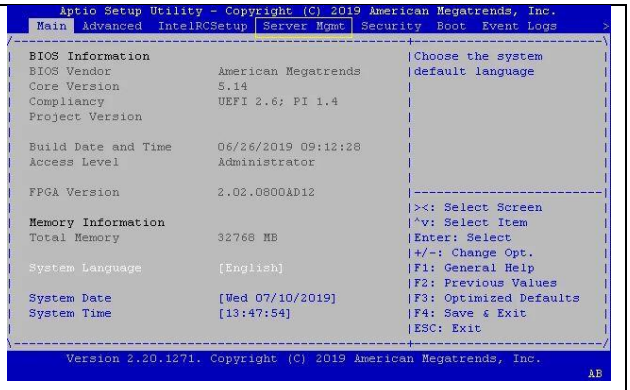
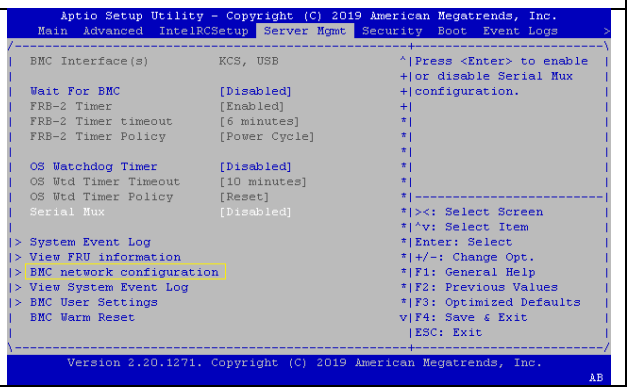
Étape_4	L'écran d'accueil de l'UEFI/BIOS affiche "Entering Setup...". **NOTE :** L'affichage et l'entrée dans le menu de configuration de l'UEFI/BIOS prendront quelques secondes.	
Étape_5	Le menu de configuration de l'UEFI/BIOS s'affiche.	

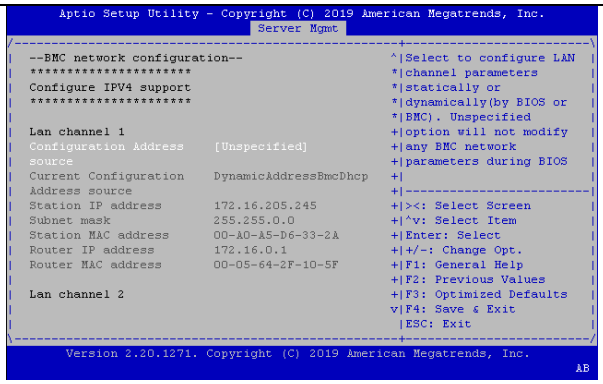
7.1.2.2 Accéder au menu BMC network configuration

Dans une plateforme équipée d'un module d'E/S de commutation Ethernet, le BMC est accessible via deux connexions réseau. Selon l'interface de configuration utilisée, les noms des connexions réseau changent.

IPMI et UEFI /BIOS	**Redfish et interface utilisateur Web**	**Connectivité de réseau**
Canal LAN 1 (LAN channel 1)	eth0	Panneau avant Srv 5
Canal LAN 2 (LAN channel 1)	eth1	Port interne du serveur 4 → port 16 du commutateur*

* Le BMC peut alors communiquer via les ports SFP Sw1 à Sw12, selon la configuration du commutateur.

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.	

7.1.3 Découvrir l'adresse IP du BMC de la plateforme en utilisant les journaux du serveur DHCP

7.1.3.1 Préalables

1	L'accès aux journaux du serveur DHCP est nécessaire.
2	L'adresse MAC est connue pour l'interface du BMC connectée au réseau pour lequel l'adresse IP est requise.

Section pertinente :

Adresses MAC (pour trouver la première adresse MAC attribuée du BMC)

7.1.3.2 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, commutateur du système d'exploitation de réseau [SER], 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).

```
Serveur_DHCP:~$ 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

7.2 Découvrir l'adresse IP du NOS

L'adresse IP du NOS peut être découverte :

- En utilisant la mise à jour DNS dynamique par DHCP
- En utilisant le CLI de la console série du NOS
- En utilisant les journaux du serveur DHCP

7.2.1 Découvrir l’adresse IP du NOS en utilisant la mise à jour DNS dynamique par DHCP

7.2.1.1 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'ordinateur distant est dans le même sous-réseau que le commutateur.
4	La première adresse MAC attribuée au NOS est connue.

Section pertinente :

Adresses MAC (pour trouver la première adresse MAC attribuée au NOS)

7.2.1.2 Procédure

Lorsqu'un bail DHCP est demandé, le NOS 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 du préfixe NOS et de la première adresse MAC du NOS. Voir la section Adresses MAC pour déterminer celles qui sont propres à une plateforme.

Par exemple, si nous utilisons la première adresse MAC du NOS (**00:a0:a5:d2:e9:0a**), le nom d'hôte sera : NOS **00A0A5D2E90A**. Noter qu'il s'agit de la configuration par défaut, mais que le paramètre est configurable par l'utilisateur. La méthode décrite ici ne fonctionne que si le nom d'hôte par défaut est toujours en vigueur.

L'exemple suivant illustre la méthode qui utilise l'enregistrement DNS automatique avec un ordinateur distant.

Étape_1	Sonder le nom de l'hôte par PING. InviteSE_OrdinateurDistant:~$ **ping NOS00A0A5D2E90A**	Pinging BOARD_NAME_00A0A5D2E90A[172.16.211.126] with 32 bytes of data: Reply from 172.16.211.126: bytes=32 time<1ms TTL=60 Reply from 172.16.211.126: bytes=32 time<1ms TTL=60 Reply from 172.16.211.126: bytes=32 time=1ms TTL=60 Reply from 172.16.211.126: bytes=32 time<1ms TTL=60 Ping statistics for 172.16.211.126: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms

7.2.2 Découvrir l’adresse IP du NOS en utilisant le CLI de la console série du NOS

7.2.2.1 Préalables

1	L'adresse IP du BMC est connue.
2	L'ordinateur distant a accès au sous-réseau du réseau de gestion.
3	Un outil client SSH est installé sur l'ordinateur distant. **NOTE :** PuTTY est recommandé pour les environnements Windows, et SSH est recommandé pour les environnements Linux.

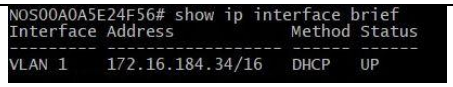
Sections pertinentes :

Noms d'utilisateur et mots de passe par défaut

Accéder au NOS

7.2.2.2 Procédure

NOTE : Lorsque série sur SSH est utilisé, appuyer sur **Entrée**, puis sur le **~** pour quitter la session.

Étape_1	À l'aide d'un outil client SSH, ouvrir une session SSH avec les paramètres suivants : • Adresse IP du BMC • Numéro de port : 2201 (une fois la session ouverte, le BMC redirigera automatiquement la communication vers la console série du NOS)	
Étape_2	Ouvrir une session sur le BMC à l'aide des données d'accès appropriées pour le BMC. Une fois la connexion établie, appuyer sur **Entrée** pour obtenir une réponse du CLI du NOS. Si une session n'est pas déjà ouverte sur la console série du NOS, une autre série de données d'accès sera demandée. Utiliser les données d'accès appropriées pour le commutateur afin d'ouvrir la session sur le NOS.	
Étape_3	Utiliser la commande suivante pour découvrir l'adresse IP du NOS. InviteCLI_NOSLocal:~# **show ip interface brief**	

7.2.3 Découvrir l'adresse IP du NOS en utilisant les journaux du serveur DHCP

7.2.3.1 Préalables

1	L'accès aux journaux du serveur DHCP est nécessaire.
2	La première adresse MAC attribuée au NOS est connue.

Section pertinente :

Adresses MAC (pour trouver la première adresse MAC attribuée au NOS)

7.2.3.2 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, commutateur du système d'exploitation de réseau [SER], 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).

```
Serveur_DHCP:~$ 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

8/ Noms d'utilisateur et mots de passe par défaut

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.

8.1 Interface de gestion (BMC)

Le BMC est accessible via les interfaces suivantes :

- Interface utilisateur Web
- Redfish
- IPMI

Toutes les méthodes d'accès partagent les mêmes utilisateurs.

Nom d'utilisateur	Mot de passe
admin	ready2go

8.2 Système d'exploitation réseau (NOS) du commutateur

Nom d'utilisateur	Mot de passe
admin	ready2go

8.3 Système d'exploitation

Le nom d'utilisateur et le mot de passe sont propres à l'application.

Cependant, si Kontron a fourni un système d'exploitation, les données d'accès seront les suivantes :

Nom d'utilisateur	Mot de passe
root	kontron

8.4 UEFI/BIOS

Aucun mot de passe par défaut n'est défini.

9/ Installation et déploiement de logiciels

9.1 Préparation de l'installation du système d'exploitation

Étape_1	Choisir le système d'exploitation nécessaire en fonction des exigences de votre application. Il est recommandé d'en choisir un parmi les systèmes d'exploitation validés.
Étape_2	Confirmer que la version du système d'exploitation à installer comprend ou a des pilotes qui prennent en charge les composants de la plateforme inclus dans le mappage PCI.
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 Installation d'un système d'exploitation sur un serveur

Le système d'exploitation peut être installé :

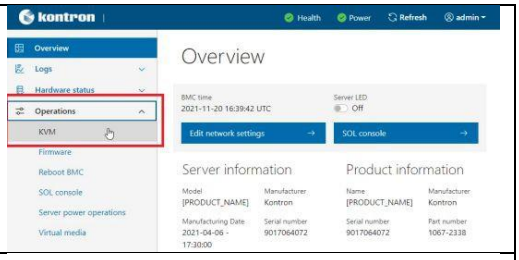
- En utilisant le KVM
- En utilisant PXE (Boot from LAN)
- En utilisant une unité de stockage USB

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

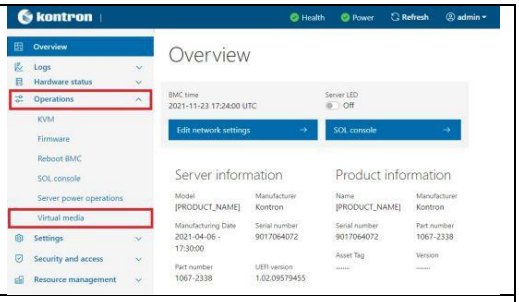
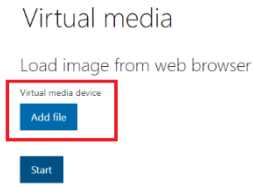
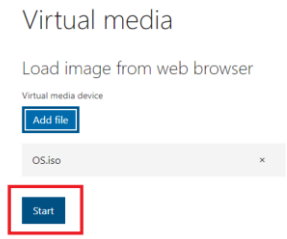
Section pertinente :

Accéder au BMC en utilisant l'interface utilisateur Web

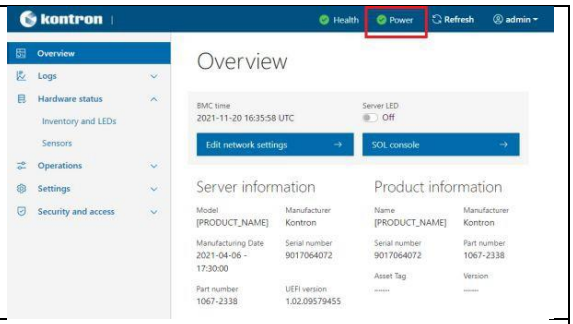
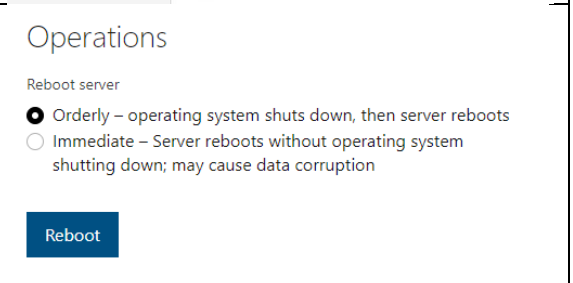
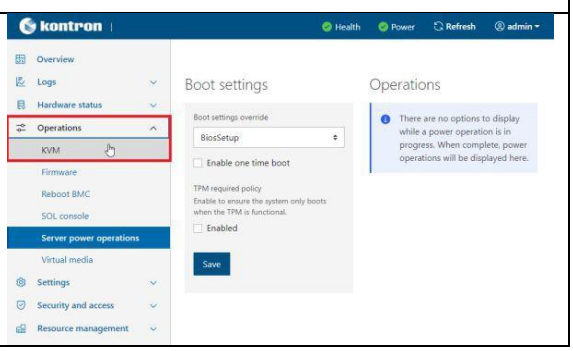
9.2.1.1 Lancer le KVM

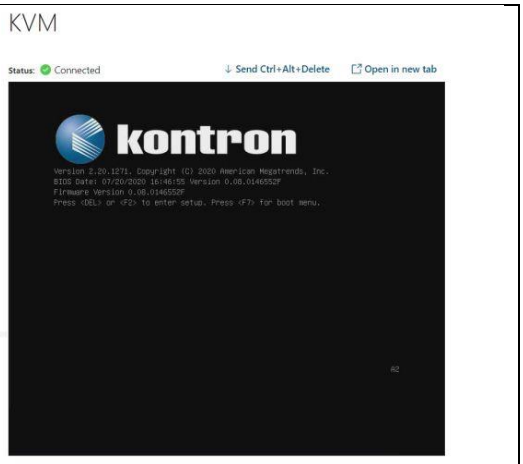
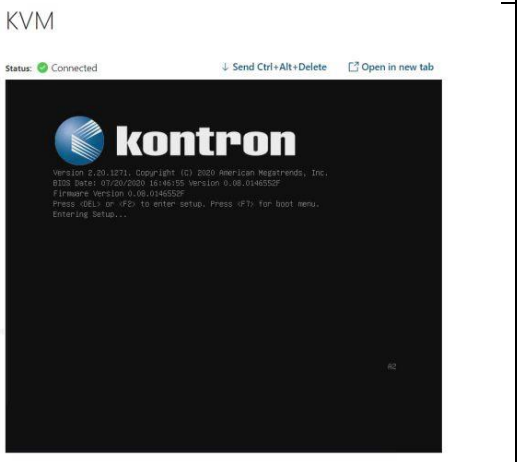
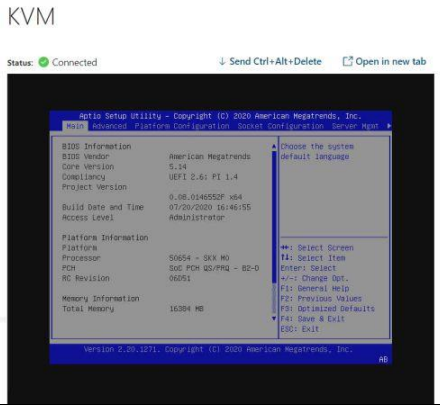
Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Operations**, puis sur **KVM**.	
Étape_2	Une nouvelle fenêtre de navigateur s'ouvre et affiche l'écran virtuel du serveur.	

9.2.1.2 Monter l'image du système d'exploitation en utilisant un support virtuel

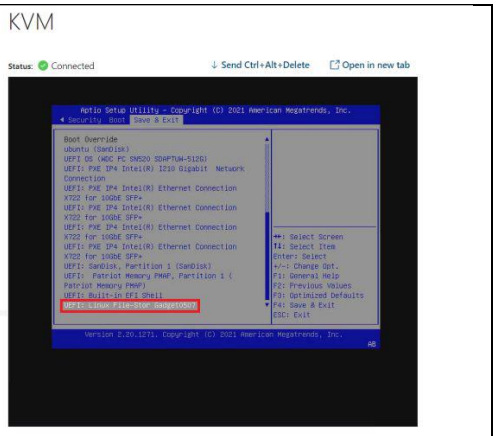
Étape_1	Dans le menu **Operations**, sélectionner **Virtual media**.	
Étape_2	Cliquer sur **Add file** pour chercher le fichier ISO.	
Étape_3	Cliquer sur **Start** pour accéder au support virtuel à partir du système d'exploitation.	

9.2.1.3 Accéder au menu de configuration de l'UEFI/BIOS

Étape_1	Dans l'interface utilisateur Web du BMC, cliquer sur le bouton **Power**.	
Étape_2	Dans la section **Reboot server**, sélectionner **Orderly**, puis cliquer sur **Reboot**.	
Étape_3	Dans le menu **Operations**, cliquer sur **KVM**.	

Étape_4	Lorsque l'écran d'accueil de l'UEFI/BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration de l'UEFI/BIOS. **NOTE :** Lorsqu'une commande de réinitialisation du serveur est lancée, quelques secondes peuvent s'écouler avant que l'écran d'accueil de l'UEFI/BIOS ne s'affiche. **NOTE :** Il peut s'écouler quelques secondes avant que l'écran d'accueil de l'UEFI/BIOS n'affiche le message de confirmation "Entering Setup…".	
Étape_5	L'écran d'accueil de l'UEFI/BIOS affiche "Entering Setup...". **NOTE :** L'affichage et l'entrée dans le menu de configuration de l'UEFI/BIOS pourraient prendre quelques secondes.	
Étape_6	Le menu de configuration de l'UEFI/BIOS s'affiche.	

9.2.1.4 Choisir l'ordre de démarrage avec la fonction Boot Override

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

9.2.1.5 Compléter l'installation du système d'exploitation

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

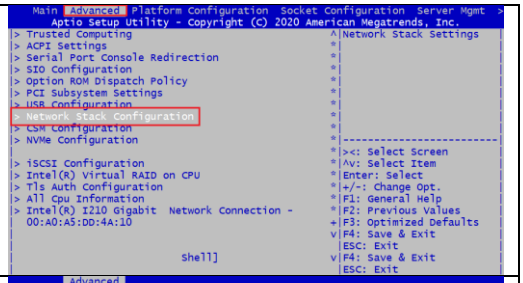
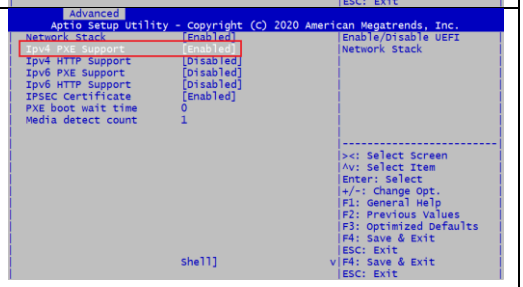
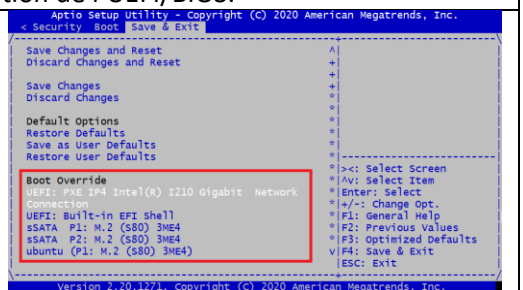
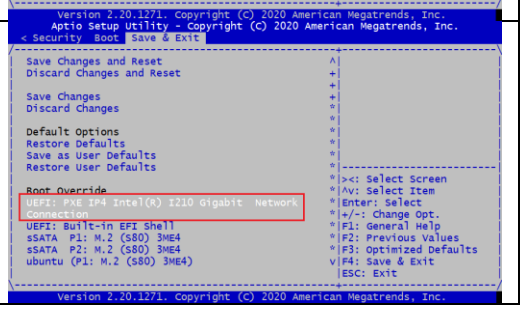
9.2.2 Installer un système d'exploitation sur un serveur en utilisant PXE (Boot from LAN)

Sections pertinentes :

Accéder à l'UEFI/BIOS

Gestion de l'alimentation de la plateforme

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

Étape_1	Dans le menu de configuration de l'UEFI/BIOS, sélectionner l'onglet **Advanced**, puis le sous-menu **Network Stack Configuration**.	
Étape_2	Mettre **Network Stack** à **Enabled**. Selon l'application, mettre **IPv4 PXE Support** ou **IPv6 PXE Support** à **Enabled**.	
Étape_3	Redémarrer le système et accéder à nouveau au menu de configuration de l'UEFI/BIOS.	
Étape_4	Naviguer jusqu'au menu **Save & Exit** et ensuite jusqu'à la section **Boot Override**.	
Étape_5	Choisir l'option PXE souhaitée.	

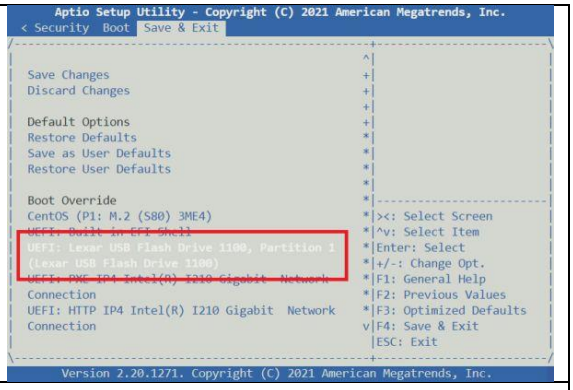
9.2.3 Installer un système d'exploitation sur un serveur en utilisant une unité de stockage USB

Sections pertinentes :

Accéder à l'UEFI/BIOS

Gestion de l'alimentation de la plateforme

Étape_1	Créer une clé USB amorçable avec le logiciel approprié. **NOTE :** RUFUS est recommandé.
Étape_2	Insérer la clé USB dans l'un des ports USB du panneau avant.
Étape_3	Démarrer la plateforme et accéder au menu de configuration de l'UEFI/BIOS.

Étape_4	Naviguer jusqu'au menu **Save & Exit** et ensuite jusqu'à la section **Boot Override**.	
Étape_5	Choisir l'option USB souhaitée.	

9.3 Vérifier l'installation du système d'exploitation

Sections pertinentes :

Architecture du produit

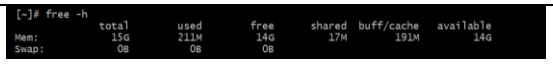
Mappage PCI

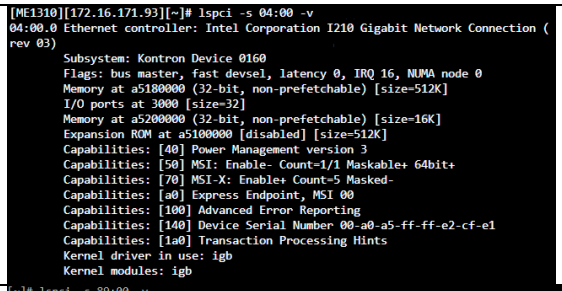
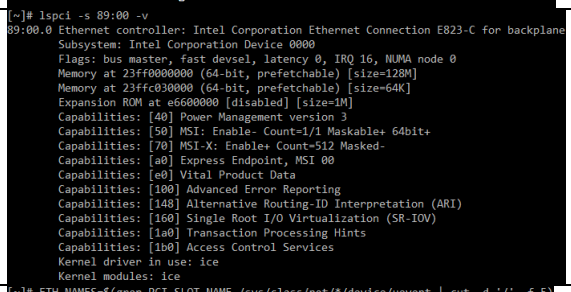
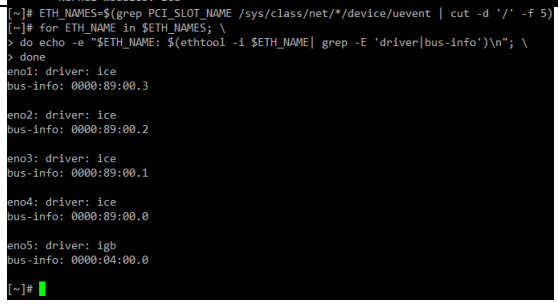
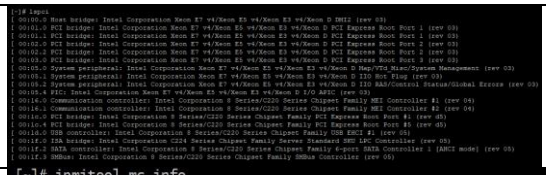
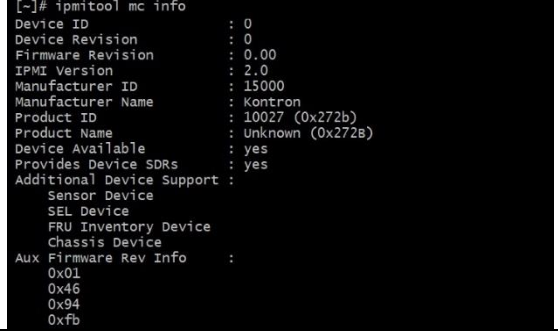
Accéder au système d'exploitation d'un serveur

Installation des logiciels courants

9.3.1 Vérifier la prise en charge des périphériques

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	Installer **ethtool**, **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 pour CentOS : InviteSE_ServeurLocal:~# **yum update** InviteSE_ServeurLocal:~# **yum install pciutils** InviteSE_ServeurLocal:~# **yum install ethtool** InviteSE_ServeurLocal:~# **yum install ipmitool** **NOTE :** La mise à jour des paquets peut prendre quelques minutes.	
Étape_3	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_4	Vérifier que les modules DIMM sont détectés. InviteSE_ServeurLocal:~# **free -h**	
Étape_5	Vérifier que toutes les unités de stockage sont détectées. InviteSE_ServeurLocal:~# **lsblk**	

Étape_6	Confirmer que les contrôleurs d'interfaces réseau de la couche de contrôle sont chargés par le pilote **igb**. InviteSE_ServeurLocal:~# **lspci -s 04:00 -v** **NOTE :** Un CIR 1GbE devrait être découvert.	
Étape_7	Confirmer que les contrôleurs d'interfaces réseau de la couche des données sont chargés par le pilote **ice**. InviteSE_ServeurLocal:~# **lspci -s 89:00 -v** **NOTE :** Jusqu'à quatre CIR 25GbE devraient être découverts.	
Étape_8	Confirmer que toutes les interfaces réseau sont détectées et obtenir la liste des noms de périphériques. Le script suivant nécessite l'utilisation du shell Bash. Saisir le bloc de commandes suivant. InviteSE_ServeurLocal:~# **ETH_NAMES=$(grep PCI _SLOT_NAME /sys/class/net/*/device/uevent | cut -d '/' -f 5)** **for ETH_NAME in $ETH_NAMES; ** **do echo -e "$ETH_NAME: $(ethtool -i $ETH_NAME| grep -E 'driver|bus- info')\n"; ** **done** **NOTE :** Jusqu'à quatre CIR 25GbE et un CIR 1GbE devraient être découverts.	
Étape_9	Configurer les contrôleurs d'interfaces réseau en fonction de vos exigences et de la topologie de réseau. **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_10	(Optionnel) Si une ou deux cartes d'expansion PCIe sont installées, vérifier qu'elles sont détectées. InviteSE_ServeurLocal:~# **lspci**	
Étape_11	Vérifier la communication entre le système d'exploitation et le BMC. InviteSE_ServeurLocal:~# **ipmitool mc info**	

9.3.2 États de gestion de l'alimentation du système d'exploitation

La plateforme ME1310 ne prend pas en charge les états de gestion de l'alimentation. Pour plus d'information, voir Désactiver les états de veille sous Linux.

9.4 Ressources de la plateforme destinées à l'application client

Cette section décrit les ressources de la plateforme qui doivent être codées dans l'application client pour bénéficier de toutes les fonctionnalités de la plateforme.

9.4.1 Indication que l'application est prête via la DEL d'alimentation

La DEL d'alimentation verte peut être configurée de façon à indiquer que l'application est prête.

NOTES :

- L'action devra être faite à chaque démarrage.
- La DEL ne peut pas revenir à l'état clignotant. Un cycle d'alimentation sera nécessaire.
- L'action est inoffensive si elle est effectuée plusieurs fois.

9.4.1.1 Préalables

1	Un système d'exploitation est installé.
2	L'accès au système d'exploitation est nécessaire.
3	L'option **OS App**. **Ready Led Control** de l'UEFI/BIOS doit être mise à **Disabled**.

Sections pertinentes :

Accéder au système d'exploitation d'un serveur

Configuration des options UEFI/BIOS

9.4.1.2 Exemple de script

L'exemple de script fourni est en C.

La valeur 0x01 doit être écrite dans le registre d'E/S 0xA20 (sur un octet).

```
#include <sys/io.h>
int main(void)
{
iopl(3);
outb(0x01, 0xa0f);
iopl(0);
return 0;
}
```

9.4.2 Capteurs de température propres aux clients

Certains capteurs de température peuvent être définis manuellement à partir du système d'exploitation du serveur. Lorsqu'une valeur est définie, elle doit être envoyée périodiquement dans les 5 secondes afin que l'algorithme de ventilation n'augmente pas les ventilateurs au maximum. Cela permet de s’assurer que si le système d'exploitation ne répond plus, les ventilateurs continueront à refroidir le système de manière adéquate.

La plage de température valide est comprise entre -127 °C et 127 °C. Si la valeur n'est pas mise à jour dans les 5 secondes, le capteur sera réglé sur la valeur maximale de 128, ce qui déclenchera un événement de type critique supérieur avec une vitesse maximale des ventilateurs.

Les capteurs qui peuvent être mis à jour de cette manière sont les suivants :

- Temp PCIe 1 mbox
- Temp PCIe 2 mbox

En modifiant les scripts fournis ci-dessous, les capteurs peuvent être renommés.

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.

9.4.2.1 Préalables

1	Un système d'exploitation est installé.
2	L'accès au système d'exploitation est nécessaire.

Sections pertinentes :

Accéder au système d'exploitation d'un serveur

Configurer les capteurs et les paramètres thermiques

Liste des capteurs

9.4.2.2 Exemple de script

L'exemple suivant utilise 2 scripts.

Le premier script (daemon.sh) est un démon qui surveille un fichier à la recherche de nouvelles valeurs de capteurs. Il convertit les informations du capteur lisibles en clair et les écrit sur le port approprié. Ce script doit être lancé au démarrage.

Pour lancer le script, taper "./daemon.sh start"

daemon.sh

```
#!/usr/bin/env bash

sensor_daemon_pipe=/tmp/sensor_daemon_pipe sensor_names=("Temp PCIe 1 mbox" "Temp PCIe 2 mbox" "" "" "" "" "" "")

get_sensor_index() {
name=$1
for i in "${!sensor_names[@]}"; do
if [[ "${sensor_names[$i]}" = "${name}" ]]; then echo "${i}";
fi done
}

start() {
trap "rm $sensor_daemon_pipe" EXIT

if [[ ! -p $sensor_daemon_pipe ]]; then mkfifo $sensor_daemon_pipe
fi

echo "Daemon started"

while read data < $sensor_daemon_pipe; do sensor_name=$(echo $data | cut -f1 -d=) sensor_value=$(echo $data | cut -f2 -d=) index=$(get_sensor_index "$sensor_name") let TEMP_PORT=0xa28+$index hexa=$(printf '%02x\n' $sensor_value)
printf "\\x$hexa" | dd of=/dev/port bs=1 count=1 seek=$(($TEMP_PORT)) status=none done
}

case "$1" in
```

```
'start')
start
;;
*)
echo
echo "Usage: $0 { start }" echo
exit 1
;;
esac
```

L'autre script envoie les nouvelles valeurs des capteurs au fichier surveillé en utilisant la syntaxe suivante :

<Sensor Name>=<Sensor Value>

client.sh

```
#!/usr/bin/env bash

sensor_daemon_pipe=/tmp/sensor_daemon_pipe

echo "Client Started"
while true; do
  echo "Temp PCIe 2 mbox=50" > $sensor_daemon_pipe sleep 2
  echo "Temp PCIe 2 mbox=30" > $sensor_daemon_pipe sleep 2
  echo "Temp PCIe 2 mbox=60" > $sensor_daemon_pipe sleep 2
done
```

NOTE : Les scripts ont été testés avec Ubuntu 20.04. Ils devraient fonctionner sur n'importe quel système Linux supportant la version 4.x+ de Bash.

9.4.2.3 Informations complémentaires de bas niveau

L'information contenue dans cette section n'est nécessaire que si vous écrivez directement dans le port mémoire associé aux capteurs.

9.4.2.3.1 Décalage de l'adresse du port

Le décalage de l'adresse permet d'accéder au registre du capteur souhaité.

Capteur	Décalage de l'adresse
Temp PCIe 1 mbox	0xa28
Temp PCIe 2 mbox	0xa29

9.4.2.4 Convertir une température en hexadécimal

Les valeurs positives sont représentées par des nombres hexadécimaux compris entre 0x00 et 0x7F.

- 0 °C est la plus petite valeur positive disponible et correspond à 0x00.
- 127 °C est la plus grande valeur positive et correspond à 0x7F.

Les valeurs négatives sont représentées par des nombres hexadécimaux compris entre 0x81 et 0xFF.

- -1 °C est la plus petite valeur négative disponible et correspond à 0xFF.
- -127 °C est la plus grande valeur négative et correspond à 0x81.

La valeur 0x80 est associée à n/a, ce qui signifie qu'il n'y a pas de lecture.

9.4.3 Configurer le FRU virtuel pour une carte d'expansion PCIe

Pour que leurs températures soient automatiquement transmises au BMC, certaines cartes d'expansion PCIe doivent être enregistrées dans le FRU virtuel du BMC.

Sections pertinentes :

Liste de compatibilité matérielle

Liste des capteurs

Accéder au BMC

Configurer les capteurs et les paramètres thermiques

9.4.3.1 Lister les FRU disponibles

Étape_1	Pour vérifier si une carte d'expansion PCIe particulière peut être enregistrée dans le FRU virtuel, utiliser la commande suivante. InviteSE_OrdinateurDistant:~# **cur l -k -s --request GET --url [URL_RACINE] /redfish/v1/Managers/bmc | jq .Oem.Kontron.VirtualPcieFru**

	`curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc | jq .Oem.Kontron.VirtualPcieFru`
	`{`
	`  "AvailableFrus": [`
	`  "P3iMB"`
	`  ],`
	`  "PCIe1": "P3iMB",`
	`  "PCIe2": ""`
	`}`

9.4.3.2 Ajouter un FRU virtuel

Étape_1	Ajouter une carte PCIe au FRU virtuel avec la commande suivante. La variable EMPLACEMENT_PCIE peut être PCIe1 ou PCIe2. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/Managers/bmc --header "'Content-Type: application/json'" --data '{"Oem": {"Kontron": {"VirtualPcieFru": {"[EMPLACEMENT_PCIE]": " [FRU] "} } } } ' | jq**

	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc --header "'Content-Type: application/json'" --data '{"Oem": {"Kontron": {"VirtualPcieFru": {"PCIe1": "P3iMB"}}}}' | jq`
	`{`
	`  "Oem": {`
	`  "Kontron": {`
	`  "VirtualPcieFru": {`
	`  "PCIe1": "P3iMB"`
	`  }`
	`  }`
	`  }`
	`}`

Étape_2	Redémarrer le BMC pour appliquer les changements. InviteSE_OrdinateurDistant:~$ **curl -k -s --request POST --url [URL_RACINE] /redfish/v1/ Managers /bmc/Actions/Manager.Reset -- header "Content-Type: application/json" –data '{"ResetType":"GracefulRestart"}' | jq**

	`$ curl -k -s --request POST --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/Actions/Manager.Reset --header 'Content-Type: application/json' -data '"{"ResetType":"GracefulRestart"}"' | jq`
	`{`
	`  "@Message.ExtendedInfo": [`
	`  {`
	`  "@odata.type": "#Message.v1_1_1.Message",`
	`  "Message": "Successfully Completed Request",`
	`  "MessageArgs": [],`
	`  "MessageId": "Base.1.8.1.Success",`
	`  "MessageSeverity": "OK",`
	`  "Resolution": "None"`
	`  }`
	`  ]`
	`}`

9.4.3.3 Supprimer un FRU virtuel

<table>
<tr><td>Étape_1</td><td>Pour désenregistrer une carte d'expansion PCIe du FRU virtuel, utiliser la commande suivante. La variable EMPLACEMENT_PCIE peut être PCIe1 ou PCIe2.
InviteSE_OrdinateurDistant:~# curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/Managers/bmc --header "'Content-Type: application/json'" --data '{"Oem": {"Kontron": {"VirtualPcieFru": {"[EMPLACEMENT_PCIE]": ""} } } } ' | jq</td></tr>
<tr><td></td><td><pre>$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc --header "'Content-Type: application/json'" --data '{"Oem": {"Kontron": {"VirtualPcieFru": {"PCIe1": ""}}}}' | jq
{
 "Oem": {
  "Kontron": {
   "VirtualPcieFru": {
    "PCIe1": ""
   }
  }
 }
}</pre></td></tr>
<tr><td>Étape_2</td><td>Redémarrer le BMC pour appliquer les changements.
InviteSE_OrdinateurDistant:~$ curl -k -s --request POST --url [URL_RACINE] /redfish/v1/ Managers /bmc/Actions/Manager.Reset -- header "Content-Type: application/json" --data '{"ResetType":"GracefulRestart"}' | jq</td></tr>
<tr><td></td><td><pre>$ curl -k -s --request POST --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/Actions/Manager.Reset --header 'Content-Type: application/json' -data '"{"ResetType":"GracefulRestart"}"' | jq
{
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "Message": "Successfully Completed Request",
      "MessageArgs": [],
      "MessageId": "Base.1.8.1.Success",
      "MessageSeverity": "OK",
      "Resolution": "None"
    }
  ]
}</pre></td></tr>
</table>

9.5 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.

9.5.1 Outils logiciels requis

Outil	Description
ipmitool	Utilitaire IPMI pour contrôler et surveiller des périphériques via les interfaces IPMI de la plateforme.
ethtool	Outil de pilotes réseau utilisé dans la documentation.
pciutils	Outil utilisé pour gérer les cartes d'expansion PCIe connectées à la plateforme
hdparm	Programme de ligne de commande pour Linux
nvme-cli	Outils en espace utilisateur (userspace) pour contrôler les disques NVMe

9.5.2 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

10/ Configuration

10.1 Configuration et gestion des utilisateurs

10.1.1 Configurer et gérer les utilisateurs du BMC

Il est recommandé de changer le mot de passe de l'administrateur immédiatement après avoir accédé à l'interface utilisateur Web.

10.1.1.1 Niveaux de privilèges

Cette section décrit les autorisations associées aux différents niveaux de privilèges dans l'interface utilisateur Web du BMC et Redfish.

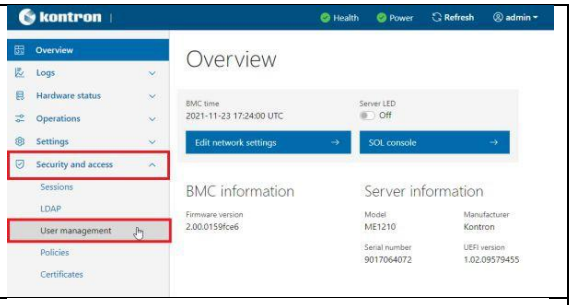
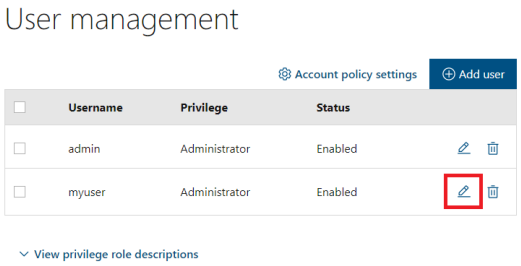
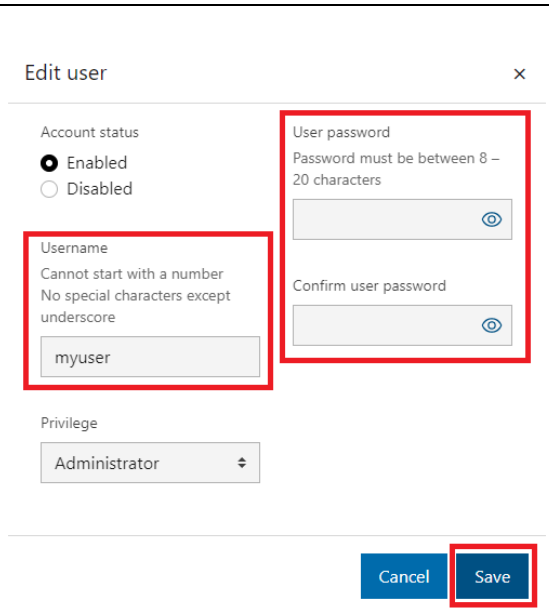
Rôles		**Description**
Interface utilisateur Web du BMC et Redfish	**IPMI**	
Admin (administrateur)	0x4 - Administrator	Les utilisateurs sont autorisés à configurer tout ce qui concerne le BMC (y compris la gestion des utilisateurs et la configuration du réseau). Les utilisateurs auront un accès administratif complet.
Operator (opérateur)	0x3 - Operator	Les utilisateurs sont autorisés à visualiser et à contrôler des opérations de base. Cela inclut le redémarrage de l'hôte. Les utilisateurs ne sont pas autorisés à modifier quoi que ce soit concernant la gestion des utilisateurs et la configuration du réseau. Les utilisateurs peuvent modifier leur propre mot de passe.
User (utilisateur)	0x1 - Callback	Les utilisateurs n'ont qu'un accès en lecture et ne peuvent pas modifier le comportement du système. Les utilisateurs peuvent modifier leur propre mot de passe.
No-Access (aucun accès)	0xF - No Access	Les utilisateurs ayant ce niveau de privilège n'auront pas accès au BMC.

10.1.1.2 Configurer les noms d'utilisateur et les mots 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.

10.1.1.2.1 En utilisant l’interface utilisateur Web

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

Étape_1	Dans le menu de gauche, cliquer sur **Security and access**, puis sur **User Management**.	
Étape_2	Sélectionner l'utilisateur à gérer dans la section **User management**.	
Étape_3	Modifier le nom d'utilisateur et/ou le mot de passe et confirmer les modifications en cliquant sur **Save**. **NOTE :** Le mot de passe doit être mis à jour pour actualiser tout autre paramètre.	

10.1.1.2.2 En utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Lister les utilisateurs disponibles. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET –url [URL_RACINE]/redfish/v1/AccountService/Accounts | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/AccountSe
rvice/Accounts | jq
{
  "@odata.id": "/redfish/v1/AccountService/Accounts",
  "@odata.type": "#ManagerAccountCollection.ManagerAccountCollection",
  "Description": "BMC User Accounts",
  "Members": [
    {
      "@odata.id": "/redfish/v1/AccountService/Accounts/myuser"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Accounts/admin"
    }
  ],
  "Members@odata.count": 3,
  "Name": "Accounts Collection"
}
```

Étape_2	Modifier le mot de passe. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE] /redfish/v1/ AccountService/Accounts/ [NOM_UTILISATEUR] -- header 'Content-type: application/json' --data '"{"Password":" [NOUVEAU_MOT_DE_PASSE] ", "UserName":" [NOUVEAU_NOM_D'UTILISATEUR] "}"'. | jq** `$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/AccountService/Accounts/myuser --header 'Content-Type: application/json' --data '"{"Password": "Password7890!","UserName": "myuser2"}"' | jq`

10.1.1.2.3 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] -C 17**.

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 du BMC.
	InviteSE_ServeurLocal:~# **ipmitool user list [CANAL_LAN]**
		`[root@localhost ~]# ipmitool user list 1`
		`ID Name Callin Link Auth IPMI Msg Channel Priv Limit`
		`1 false false true ADMINISTRATOR`
		`2 admin false false true ADMINISTRATOR`
		`3 user true true true ADMINISTRATOR`
		`4 true false false NO ACCESS`
		`5 true false false NO ACCESS`
		`6 true false false NO ACCESS`
		`7 true false false NO ACCESS`
		`8 true false false NO ACCESS`
		`9 true false false NO ACCESS`
		`10 true false false NO ACCESS`

Étape_2	Identifier le numéro d'identification de l'utilisateur à modifier.	`[root@localhost ~]# ipmitool user list 1`
		`ID Name Callin Link Auth IPMI Msg Channel Priv Limit`
		`1 false false true ADMINISTRATOR`
		`2 admin false false true ADMINISTRATOR`
		`3 user true true true ADMINISTRATOR`
		`4 true false false NO ACCESS`
		`5 true false false NO ACCESS`
		`6 true false false NO ACCESS`
		`7 true false false NO ACCESS`
		`8 true false false NO ACCESS`
		`9 true false false NO ACCESS`
		`10 true false false NO ACCESS`

Étape_3	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.	

Étape_4	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]**
		`[root@localhost ~]# ipmitool user list 1`
		`ID Name Callin Link Auth IPMI Msg Channel Priv Limit`
		`1 false false true ADMINISTRATOR`
		`2 admin false false true ADMINISTRATOR`
		`3 operator true true true ADMINISTRATOR`
		`4 true false false NO ACCESS`
		`5 true false false NO ACCESS`
		`6 true false false NO ACCESS`
		`7 true false false NO ACCESS`
		`8 true false false NO ACCESS`
		`9 true false false NO ACCESS`
		`10 true false false NO ACCESS`

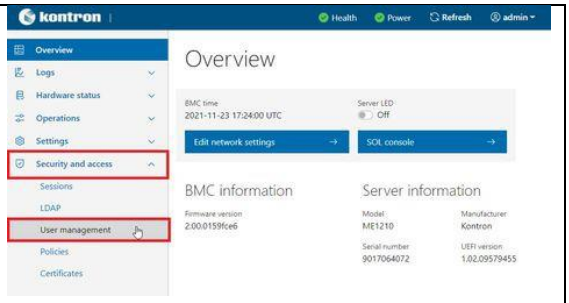
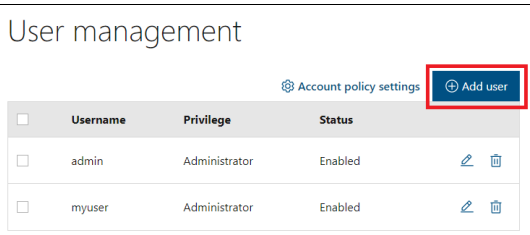
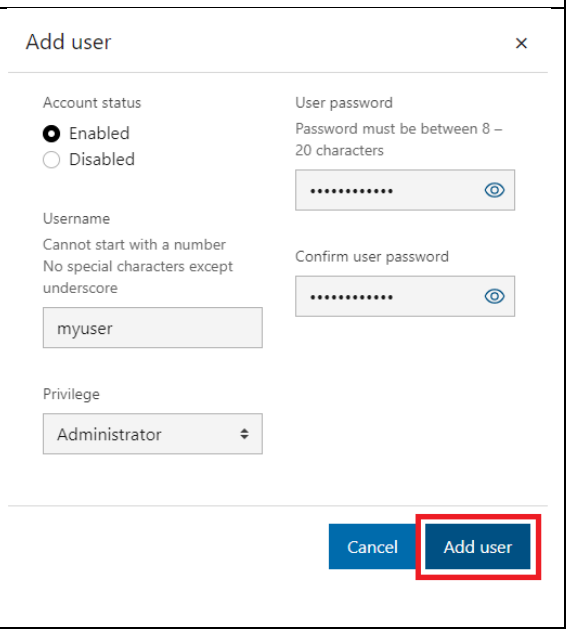
Étape_5	Modifier le mot de passe. InviteSE_ServeurLocal: ~# **ipmitool user set password [ID_UTILISATEUR_IPMI] [NOUVEAU_MOT_DE_PASSE_IPMI]**	`[root@localhost ~]# ipmitool user set password 3 newpassword` `Set User Password command successful (user 3)`
Étape_6	Vérifier que les données d'accès ont été 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.	

10.1.1.3 Ajouter un utilisateur

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.

10.1.1.3.1 En utilisant l'interface utilisateur Web

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

Étape_1	Dans le menu de gauche, cliquer sur **Security and access**, puis sur **User Management**.	
Étape_2	Cliquer sur **Add user**.	
Étape_3	Remplir les champs obligatoires et cliquer sur **Add user**.	

10.1.1.3.2 En utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur.

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

Étape_1	Lister les niveaux de privilèges disponibles. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/AccountService/Roles | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/AccountSe
rvice/Roles | jq
{
  "@odata.id": "/redfish/v1/AccountService/Roles",
  "@odata.type": "#RoleCollection.RoleCollection",
  "Description": "BMC User Roles",
  "Members": [
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/Administrator"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/Operator"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/ReadOnly"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/NoAccess"
    }
  ],
  "Members@odata.count": 4,
  "Name": "Roles Collection"
}
```

Étape_2	Créer l'utilisateur en utilisant un autre utilisateur disposant des privilèges d'administrateur. InviteSE_OrdinateurDistant:~# **curl -k -s --request POST --url [URL_RACINE]/redfish/v1/AccountService/Accounts --header 'Content- Type: application/json' --data '"{"Password":" [MOT_DE_PASSE] ","RoleI d":" [ID_ROLE] ","UserName":" [NOM_UTILISATEUR] "}"'. | jq**

```
$ curl -k -s --request POST --url https://admin:ready2go@172.16.182.31/redfish/v1/AccountS
ervice/Accounts --header 'Content-Type: application/json' --data '"{"Password": "Password1
234!","RoleId": "Operator","UserName": "myuser"}"' | jq
{
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "Message": "The resource has been created successfully",
      "MessageArgs": [],
      "MessageId": "Base.1.8.1.Created",
      "MessageSeverity": "OK",
      "Resolution": "None"
    }
  ]
}
```

Étape_3	Vérifier que l'utilisateur a été créé correctement en établissant une connexion à Redfish à l'aide des données d'accès de cet utilisateur.

10.1.1.3.3 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] -C 17**.

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]**	

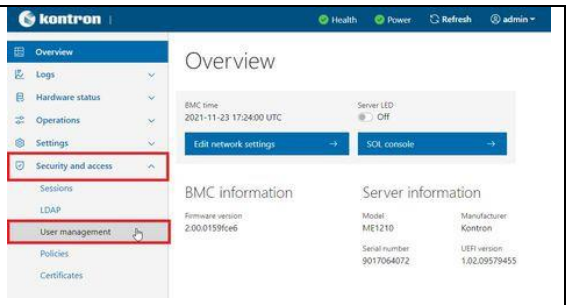
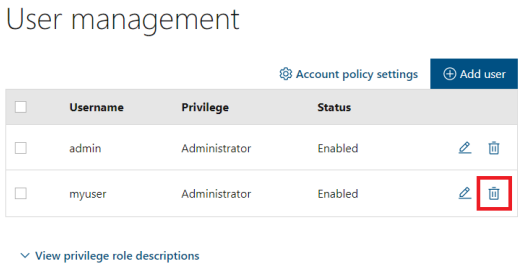
```
[root@localhost ~]# ipmitool user list 1
ID  Name             Callin  Link Auth  IPMI Msg   Channel Priv Limit
1                    false   false      true       ADMINISTRATOR
2   admin            false   false      true       ADMINISTRATOR
3                    true    false      false      NO ACCESS
4                    true    false      false      NO ACCESS
5                    true    false      false      NO ACCESS
6                    true    false      false      NO ACCESS
7                    true    false      false      NO ACCESS
8                    true    false      false      NO ACCESS
9                    true    false      false      NO ACCESS
10                   true    false      false      NO ACCESS
```

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]**

10.1.1.4 Supprimer un utilisateur

10.1.1.4.1 En utilisant l'interface utilisateur Web

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

Étape_1	Dans le menu de gauche, cliquer sur **Security and access**, puis sur **User Management**.	
Étape_2	Sélectionner l'utilisateur à supprimer dans la section **User management**.	

10.1.1.4.2 En utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Lister les niveaux de privilèges disponibles. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/AccountService/Roles | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/AccountSe
rvice/Roles | jq
{
  "@odata.id": "/redfish/v1/AccountService/Roles",
  "@odata.type": "#RoleCollection.RoleCollection",
  "Description": "BMC User Roles",
  "Members": [
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/Administrator"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/Operator"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/ReadOnly"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/NoAccess"
    }
  ],
  "Members@odata.count": 4,
  "Name": "Roles Collection"
}
```

Étape_2	Changer le niveau de privilège. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/AccountService/Accounts/ [ID_UTILISATEUR] -- header 'Content-type: application/json' - -data '"{"RoleI d":" [ROLE] "}"' | jq**

```
$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Account
Service/Accounts/myuser --header 'Content-Type: application/json' --data '"{"RoleId": "Adm
inistrator"}"' | jq
{
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "Message": "Successfully Completed Request",
      "MessageArgs": [],
      "MessageId": "Base.1.8.1.Success",
      "MessageSeverity": "OK",
      "Resolution": "None"
    }
  ]
}
```

10.1.1.4.3 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] -C 17**.

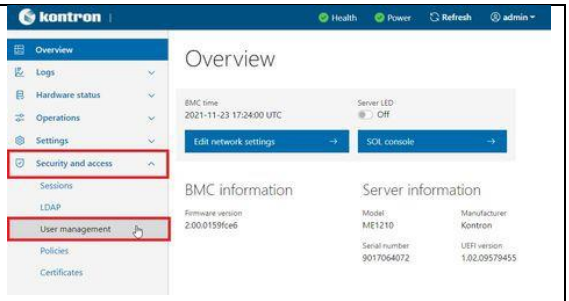
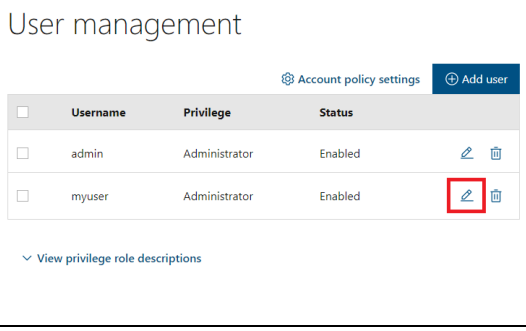
Les utilisateurs ne peuvent pas être supprimés avec ipmitool. Cependant, ils peuvent être désactivés.

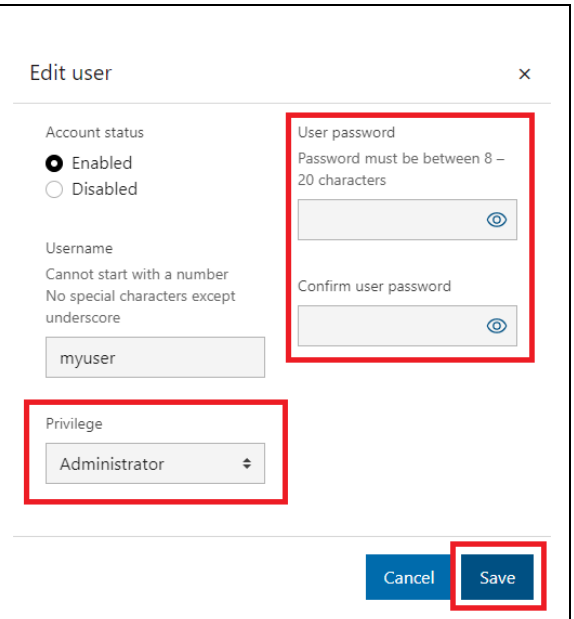
Étape_1	À partir d'un ordinateur distant ayant accès au système d'exploitation du serveur via SSH, RDP ou le port série de la plateforme, afficher la liste des utilisateurs et sélectionner l'ID de l'utilisateur à désactiver. InviteSE_ServeurLocal:~# **ipmitool user list [CANAL_LAN]**	
Étape_2	Désactiver 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.	

10.1.1.5 Configurer le niveau de privilège

10.1.1.5.1 En utilisant l'interface utilisateur Web

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

Étape_1	Dans le menu de gauche, cliquer sur **Security and access**, puis sur **User Management**.	
Étape_2	Sélectionner l'utilisateur à gérer dans la section **User management**.	

Étape_3	Modifier les champs du niveau de privilège ainsi que le mot de passe et confirmer la configuration en cliquant sur le bouton **Save**.	

10.1.1.5.2 En utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Lister les niveaux de privilèges disponibles. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/AccountService/Roles | jq**

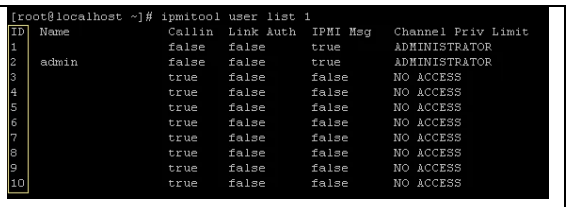
```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/AccountSe
rvice/Roles | jq
{
  "@odata.id": "/redfish/v1/AccountService/Roles",
  "@odata.type": "#RoleCollection.RoleCollection",
  "Description": "BMC User Roles",
  "Members": [
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/Administrator"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/Operator"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/ReadOnly"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/NoAccess"
    }
  ],
  "Members@odata.count": 4,
  "Name": "Roles Collection"
}
```

Étape_2	Changer le niveau de privilège. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/AccountService/Accounts/ [ID_UTILISATEUR] -- header 'Content-type: application/json' - -data '"{"RoleI d":" [ROLE] "}"' | jq**

```
$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Account
Service/Accounts/myuser --header 'Content-Type: application/json' --data '"{"RoleId": "Adm
inistrator"}"' | jq
{
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "Message": "Successfully Completed Request",
      "MessageArgs": [],
      "MessageId": "Base.1.8.1.Success",
      "MessageSeverity": "OK",
      "Resolution": "None"
    }
  ]
}
```

10.1.1.5.3 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] -C 17**.

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.	

10.1.2 Configurer et gérer les utilisateurs du NOS

Les modifications apportées à la configuration du NOS ne sont pas persistantes après le redémarrage du NOS. Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config.

Dans l'interface utilisateur Web du NOS :

Sélectionner **Maintenance**, **Configuration**, puis **Save startup-config**. Cliquer sur **Save Configuration** pour confirmer le changement.

Dans le CLI du NOS :

InviteCLI_NOSLocal:~(config-if)# **end**

InviteCLI_NOSLocal:~# **copy running-config startup-config**

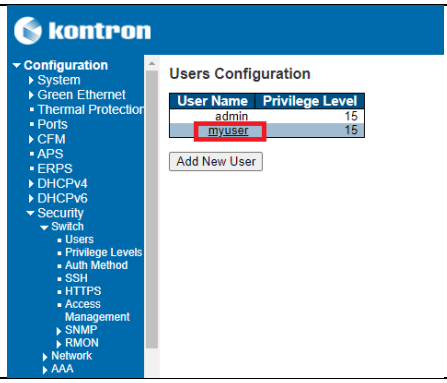
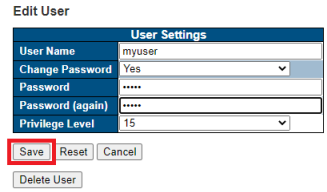
10.1.2.1 Configurer les utilisateurs du NOS en utilisant l'interface utilisateur Web du NOS

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

10.1.2.1.1 Modifier le mot de passe d'un utilisateur

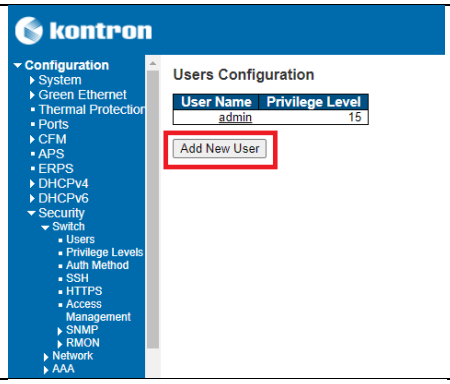
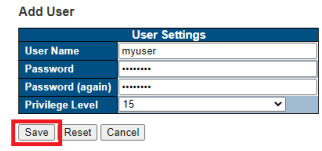
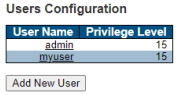
Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **Security**, **Switch**, puis **Users**.	

Étape_2	Cliquer sur l'utilisateur souhaité.	
Étape_3	Dans le champ **Change Password,** sélectionner **Yes** dans le menu déroulant.	
Étape_4	Saisir le mot de passe dans les champs **Password** et **Password (again)**.	
Étape_5	Cliquer sur **Save** pour confirmer.	
Étape_6	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.1.2.1.2 Ajouter un utilisateur

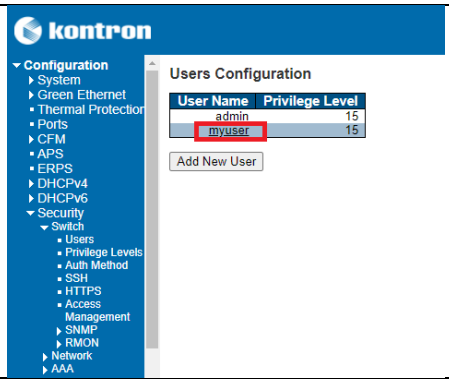
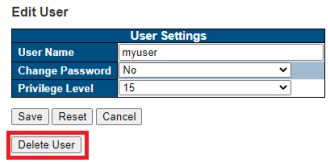
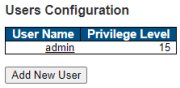
Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **Security**, **Switch**, puis **Users**.	
Étape_2	Cliquer sur le bouton **Add New User**.	
Étape_3	Remplir les champs obligatoires : **User Name**, **Password**, **Password (again)** et **Privilege Level**. **NOTE :** Pour plus d'information sur les différents niveaux de privilèges, cliquer sur le bouton d'aide situé dans le coin supérieur droit de la page de l'interface utilisateur Web du NOS.	
Étape_4	Cliquer sur le bouton **Save** pour ajouter l'utilisateur.	
Étape_5	Un nouvel utilisateur devrait être affiché dans la liste des utilisateurs.	
Étape_6	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.1.2.1.3 Supprimer un utilisateur

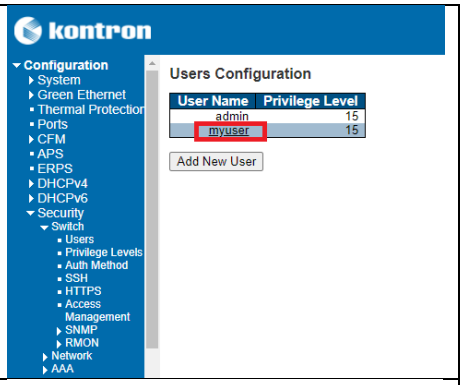
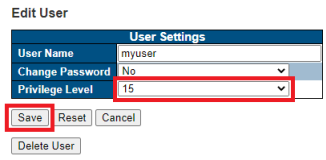
Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **Security**, **Switch**, puis **Users**.	

Étape_2	Cliquer sur l'utilisateur souhaité.	
Étape_3	Cliquer sur le bouton **Delete User**.	
Étape_4	L'utilisateur ne devrait plus être affiché dans la liste des utilisateurs.	
Étape_5	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.1.2.1.4 Configurer le niveau de privilège

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **Security**, **Switch**, puis **Users**.	
Étape_2	Cliquer sur l'utilisateur souhaité.	
Étape_3	Modifier le niveau de privilège à l'aide du menu déroulant prévu à cet effet. **NOTE :** Pour plus d'information sur les différents niveaux de privilèges, cliquer sur le bouton d'aide situé dans le coin supérieur droit de la page de l'interface utilisateur Web du NOS.	
Étape_4	Cliquer sur le bouton **Save** pour confirmer.	
Étape_5	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.1.2.2 Configurer les utilisateurs du NOS en utilisant le CLI du NOS

10.1.2.2.1 Modifier le mot de passe d'un utilisateur

Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Accéder au menu de configuration. InviteCLI_NOSLocal:~# **configure terminal**	`# configure terminal`
Étape_2	Modifier le mot de passe. InviteCLI_NOSLocal:~(config)# **username [NOM_UTILISATEUR] privilege [NIVEAU_DE_PRIVILÈGE] password unencrypted [NOUVEAU_MOT_DE_PASSE]**	`(config)# username user privilege 15 password unencrypted newPassword`
Étape_3	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.1.2.2.2 Ajouter un utilisateur

Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Accéder au menu de configuration. InviteCLI_NOSLocal:~# **configure terminal**	`# configure terminal`
Étape_2	Ajouter l'utilisateur en saisissant son nom d'utilisateur, son niveau de privilège et son mot de passe. InviteCLI_NOSLocal:~(config)# **username [NOM_UTILISATEUR] privilege [NIVEAU_DE_PRIVILÈGE] password unencrypted [MOT_DE_PASSE]**	`(config)# username user privilege 15 password unencrypted Password`
Étape_3	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.1.2.2.3 Supprimer un utilisateur

Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Accéder au menu de configuration. InviteCLI_NOSLocal:~# **configure terminal**	`# configure terminal`
Étape_2	Supprimer l'utilisateur. InviteCLI_NOSLocal:~(config)# **no username [NOM_UTILISATEUR]**	`(config)# no username myuser` `(config)#`
Étape_3	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.1.2.2.4 Configurer le niveau de privilège

Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Accéder au menu de configuration. InviteCLI_NOSLocal:~# **configure terminal**	`# configure terminal`
Étape_2	Pour modifier le niveau de privilège d'un utilisateur, reconfigurer l'utilisateur et modifier son niveau de privilège. InviteCLI_NOSLocal:~(config)# **username [NOM_UTILISATEUR] privilege [NOUVEAU_NIVEAU_DE_PRIVILÈGE] password unencrypted [MOT_DE_PASSE]**	`(config)# username user privilege 11 password unencrypted Password`
Étape_3	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.2 Configuration de la date et de l'heure

10.2.1 Configurer la date et l'heure du BMC

10.2.1.1 Informations générales sur la date et l'heure de la plateforme

La date et l'heure doivent être définies pour le BMC et pour le NOS. Ces informations seront utilisées par les journaux des événements du système lors de l'enregistrement des événements. L'UEFI/BIOS obtient automatiquement la date et l'heure du BMC lors du démarrage.

10.2.1.2 Configurer la date et l'heure du BMC

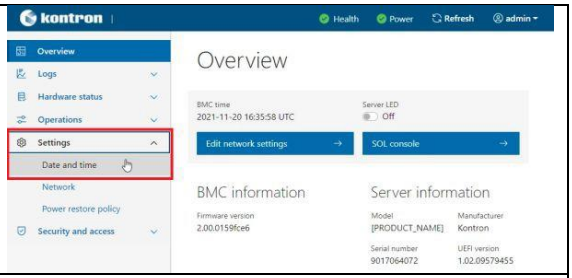
La date et l'heure du BMC peuvent être définies :

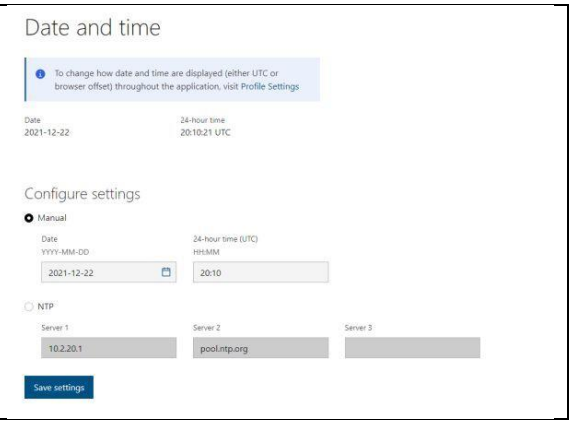
- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish
- En utilisant IPMI

10.2.1.2.1 Configurer la date et l'heure du BMC en utilisant l'interface utilisateur Web

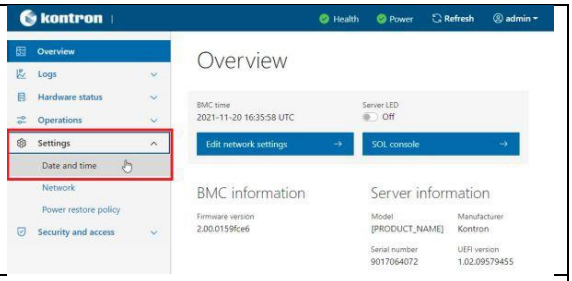
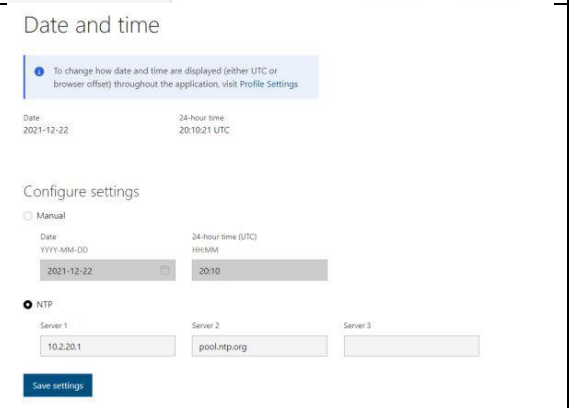
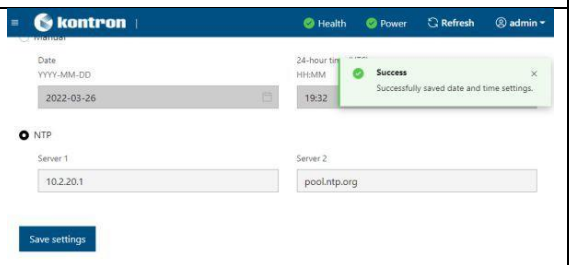
Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

10.2.1.2.1.1 Configurer la date et l'heure du BMC manuellement en utilisant l'interface utilisateur Web

Étape_1	Dans le menu de gauche, sélectionner **Settings**, puis **Date and time**.	
Étape_2	Sélectionner **Manual** et configurer la date et l'heure.	

Étape_3	Cliquer sur le bouton **Save settings**.	

10.2.1.2.1.2 Configurer la date et l'heure du BMC sur la base du service NTP en utilisant l'interface utilisateur Web

Étape_1	Dans le menu de gauche, sélectionner **Settings**, puis **Date and time**.	
Étape_2	Sélectionner **NTP**.	
Étape_3	Saisir une ou plusieurs adresses de serveurs NTP.	
Étape_4	Cliquer sur le bouton **Save settings**.	
Étape_5	Un message de réussite doit s'afficher lorsque la configuration est réussie.	

10.2.1.2.2 Configurer la date et l'heure du BMC en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

10.2.1.2.2.1 Configurer la date et l'heure du BMC manuellement en utilisant Redfish

Étape_1	Si le service NTP est activé, le désactiver. InviteSE_OrdinateurDistant:~$ **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/ Managers/bmc /NetworkProtocol -- header 'Content-Type: application/json' --data '"{"NTP": {"ProtocolEnabled": false}}"' | jq**
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Manager s/bmc/NetworkProtocol --header 'Content-Type: application/json' --data '"{"NTP": {"Protoco lEnabled": false}}"' | jq`
Étape_2	Définir la date et l'heure manuellement à l'aide de la commande suivante. InviteSE_OrdinateurDistant:~$ **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/ Managers/bmc -- header 'Content- Type: application/json' - -data '"{"DateTime": "[DATE_HEURE]"}"' | jq**

	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Manager s/bmc --header 'Content-Type: application/json' --data '"{"DateTime": "2021-12-21T18:36:59 +00:00"}"' | jq`
	`{`
	`  "DateTime": "2021-12-21T18:36:59+00:00"`
	`}`

Étape_3	Vérifier la date et l'heure actuelles du BMC. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/ Managers/bmc | jq.DateTime**

	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc | jq .DateTime`
	`{`
	`  "DateTime": "2021-12-21T18:39:59+00:00",`
	`}`

10.2.1.2.2.2 Configurer la date et l'heure du BMC sur la base du service NTP en utilisant Redfish

Étape_1	Ajouter le ou les serveurs NTP et activer le protocole. InviteSE_OrdinateurDistant:~$ **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/ Managers/bmc/NetworkProtocol -- header 'Content-Type: application/json' --data '"{"NTP": {"NTPServers": [[SERVEURS_NTP]], "ProtocolEnabled" : true}}"'. | jq**
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Manager s/bmc/NetworkProtocol --header 'Content-Type: application/json' --data '"{"NTP": {"NTPServ ers": ["pool.ntp.org","10.2.20.1"],"ProtocolEnabled": true}}"' | jq`
Étape_2	Vérifier la date et l'heure actuelles du BMC. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/ Managers/bmc | jq.DateTime**

	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc | jq .DateTime`
	`{`
	`  "DateTime": "2021-12-21T18:39:59+00:00",`
	`}`

10.2.1.2.3 Configurer la date et l'heure du BMC en utilisant IPMI

En utilisant IPMI, il est seulement possible de définir l'heure manuellement.

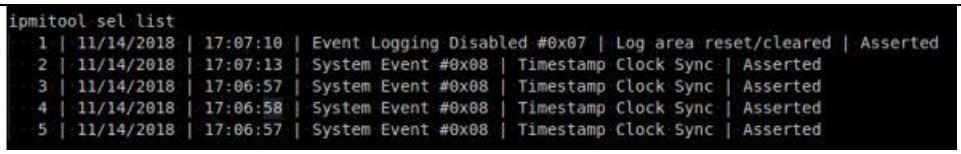
10.2.1.2.3.1 Configurer la date et l'heure du BMC manuellement en utilisant IPMI

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] -C 17**.

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 journal des événements système ont été correctement définies. InviteSE_ServeurLocal:~# **ipmitool sel time get**	

10.2.1.2.3.2 Limitation connue

Problème

Lorsque la date et l'heure du journal des événements système sont définies avec ipmitool, plusieurs entrées répétées d'événements système seront présentes dans la liste du SEL.	

Solution

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, suivre la procédure suivante.
NOTE : Les commandes peuvent varier en fonction du système d'exploitation.

Étape_1	Télécharger la plus récente version à partir de son référentiel. InviteSE_ServeurLocal:~# **git clone https://github.com/ipmitool/ipmitool.git**
Étape_2	Une fois les fichiers téléchargés, changer le répertoire pour le répertoire ipmitool. InviteSE_ServeurLocal:~# **cd ipmitool**
Étape_3	Installer ipmitool sur la plateforme (ou l'ordinateur distant). InviteSE_ServeurLocal:~# **./bootstrap &&./configure && make && make install**
Étape_4	Après l'installation d'ipmitool, ajouter le paramètre (flag) « -N 5 » avec la commande ipmitool sel set time. Ce paramètre définit le délai d'attente de la commande afin d'éviter que de multiples erreurs dupliquées ne soient enregistrées. InviteSE_ServeurLocal:~# **ipmitool sel time set "[MM/DD/YYYY HH:MM:SS]" -N 5**

10.2.2 Configurer la date et l'heure du NOS

Il n'est pas possible de définir la date et l'heure manuellement dans le NOS. Le service NTP ou PTP doit être utilisé comme source de temps.

Si aucune source NTP ou PTP n'est disponible sur le réseau, le système d'exploitation du client sur le serveur intégré peut faire office de serveur NTP. Consulter la documentation du système d'exploitation pour de l'information.

Les modifications apportées à la configuration du NOS ne sont pas persistantes après le redémarrage du NOS. Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config.

Dans l'interface utilisateur Web du NOS :

Sélectionner **Maintenance**, **Configuration**, puis **Save startup-config**. Cliquer sur **Save Configuration** pour confirmer le changement.

Dans le CLI du NOS :

InviteCLI_NOSLocal:~(config-if)# **end**

InviteCLI_NOSLocal:~# **copy running-config startup-config**

10.2.2.1 Configurer la source de temps du NOS sur la base du service NTP

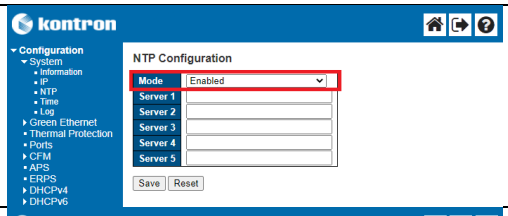
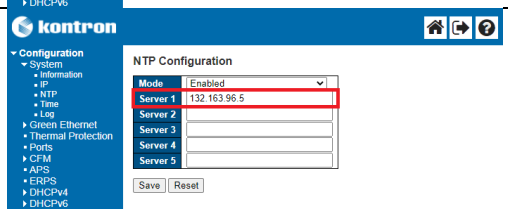
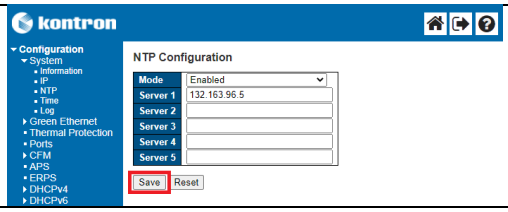
La source de temps du NOS peut être configurée :

- En utilisant l'interface utilisateur Web du NOS
- En utilisant le CLI du NOS

10.2.2.1.1 Configurer la source de temps du NOS sur la base du service NTP en utilisant l'interface utilisateur Web

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

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **System**, puis **NTP**.	
Étape_2	Activer le service NTP en changeant la valeur du menu déroulant **Mode** à **Enabled**.	
Étape_3	Entrer l'adresse ou le nom d'hôte du serveur NTP. **NOTE :** Pour pouvoir entrer le nom d'hôte d'un serveur, un service DNS doit être configuré.	
Étape_4	Répéter l'étape précédente pour ajouter plusieurs serveurs NTP si nécessaire.	
Étape_5	Cliquer sur le bouton **Save**.	
Étape_6	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.2.2.1.2 Configurer la source de temps du NOS sur la base du service NTP en utilisant le CLI

Accéder au CLI du NOS en utilisant l'une des méthodes SSH décrites dans la section Accéder au NOS.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	`# configure terminal`
Étape_2	Activer le service NTP. InviteCLI_NOSLocal:~(config)# **ntp** **NOTE :** Pour désactiver le service NTP, utiliser **no ntp**.	`(config)# ntp`

Étape_3	Configurer le serveur NTP.
	InviteCLI_NOSLocal:~(config)# **ntp server [ID_SERVEUR] ip-address [ADRESSE_IP_OU_NOM D'HÔTE]**
	
	NOTE : Pour pouvoir entrer le nom d'hôte d'un serveur, un service DNS doit être configuré.
		`(config)# ntp server 1 ip-address 132.163.96.5`
		OU
		`(config)# ntp server 1 ip-address pool.ntp.org`

Étape_4	Quitter le mode de configuration. InviteCLI_NOSLocal:~(config)# **exit**	`(config)# exit`

Étape_5	Vérifier la configuration NTP en affichant la liste des serveurs NTP.
	InviteCLI_NOSLocal:~ # **show ntp status**
		`# show ntp status`
		`NTP Mode : enabled`
		`Idx  Server IP host address (a.b.c.d) or a host name string`
		`---  ----------`
		`1  132.163.96.5`
		`2`
		`3`
		`4`
		`5`

Étape_6	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.2.2.2 Configurer la source de temps du NOS sur la base du service PTP

Pour plus d'information sur l'utilisation du service PTP comme source de temps, voir Configuration de la synchronisation.

10.2.2.3 Configurer le fuseau horaire et l'heure avancée du NOS

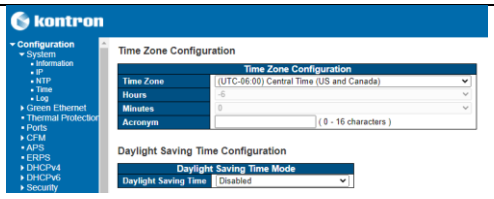
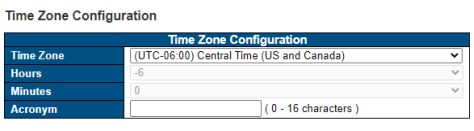
Le fuseau horaire et l'heure avancée du NOS peuvent être configurés :

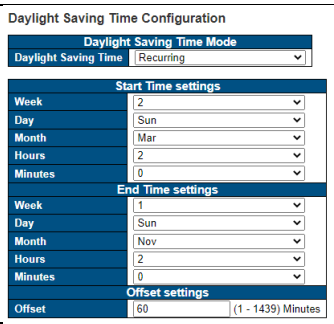
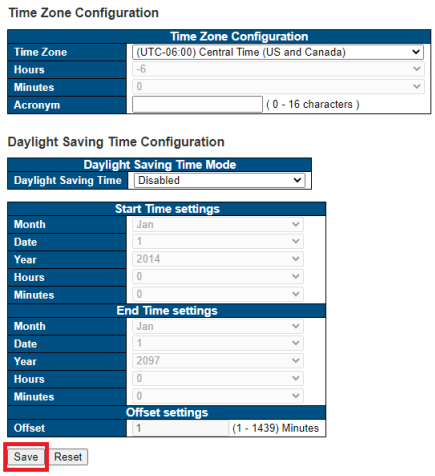
- En utilisant l'interface utilisateur Web du NOS
- En utilisant le CLI du NOS

10.2.2.3.1 Configurer le fuseau horaire et l'heure avancée du NOS en utilisant l'interface utilisateur Web

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

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **System**, puis **Time**.	
Étape_2	Configurer le fuseau horaire en le sélectionnant dans le menu déroulant **Time Zone**.	

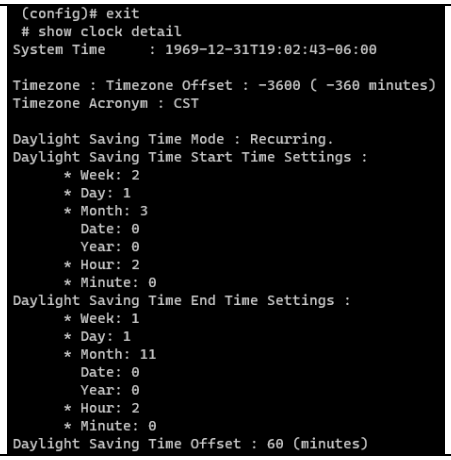
Étape_3	Configurer les paramètres de l'heure avancée.	
Étape_4	Cliquer sur **Save**.	
Étape_5	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.2.2.3.2 Configurer le fuseau horaire et l'heure avancée du NOS en utilisant le CLI

Accéder au CLI du NOS en utilisant l'une des méthodes SSH décrites dans la section Accéder au NOS.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal** `# configure terminal`
Étape_2	Régler manuellement les décalages de l'heure et des minutes. InviteCLI_NOSLocal:~(config)# **clock timezone [ACRONYME_FUSEAU_HORAIRE] [DÉCALAGE_HEURE] [DÉCALAGE_MINUTE]** `(config)# clock timezone CST -6 0`
Étape_3	Configurer l'heure avancée. InviteCLI_NOSLocal:~(config)# **clock summer-time [ACRONYME_FUSEAU_HORAIRE] date [MOIS_DÉPART] [JOUR_DÉPART] [ANNÉE_DÉPART] [HH:MM_DÉPART] [MOIS_FIN] [JOUR_FIN] [ANNÉE_FIN] [HH:MM_FIN] [DÉCALAGE]** **NOTE :** Cette commande définit les paramètres pour une année seulement. Ils devront être reprogrammés l'année suivante. OU InviteCLI_NOSLocal:~(config)# **clock summer-time [ACRONYME_FUSEAU_HORAIRE] recurring [SEMAINE_DÉPART] [MOIS_DÉPART] [JOUR_DÉPART 1=Dimanche] [HH:MM_DÉPART] [SEMAINE_FIN] [MOIS_FIN] [JOUR_FIN] [HH:MM_FIN] [DÉCALAGE_MINUTE]** **NOTE :** Cette commande définit les paramètres pour toutes les années. Aucune reprogrammation n'est nécessaire. `clock summer-time CDT recurring 2 1 3 2:00 1 1 11 2:00 60`

Étape_4	Vérifier la configuration du fuseau horaire. InviteCLI_NOSLocal:~(config)# **exit** InviteCLI_NOSLocal:~# **show clock detail**
	
Étape_5	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).

10.3 Configuration réseau

10.3.1 Configuration réseau du BMC

Pour configurer l'adresse IP réseau du BMC, un schéma doit être sélectionné et configuré :

- Une adresse IP statique
- Une adresse IP dynamique en utilisant DHCP

Par défaut, les adresses IP des interfaces réseau du BMC sont obtenues via le protocole DHCP.

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

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 le canal LAN 2 du BMC est désactivé et 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 les deux canaux LAN seront désormais désactivés.

Si votre accès est bloqué, une méthode d'accès pour laquelle aucune adresse IP connue n'est requise (voir ci-dessous) vous permettrait d'accéder à nouveau au système.

Sections pertinentes :

Découvrir les adresses IP de la plateforme

Architecture du produit

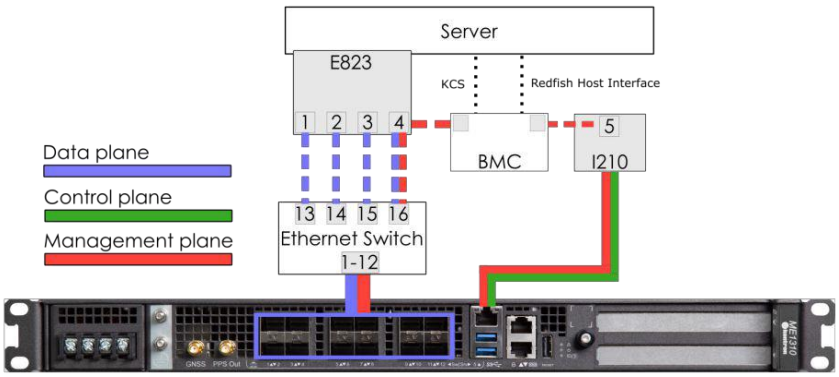
10.3.1.1 Choisir une méthode d'accès pour la configuration réseau du BMC

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 de l'UEFI/BIOS. Voir Accéder à l'UEFI/BIOS en utilisant une console série (connexion physique) pour les instructions d'accès.
- **Si l'adresse IP du BMC est inconnue et qu'un système d'exploitation est installé :**
    - Utiliser IPMI via KCS. Voir Accéder au BMC en utilisant IPMI (KCS) pour les instructions d'accès.
    - Utiliser le menu de configuration de l'UEFI/BIOS. Voir Accéder à l'UEFI/BIOS en utilisant une console série (connexion physique) pour les instructions d'accès.
- **Si l'adresse IP du BMC est connue et qu'un système d'exploitation est installé :**
    - Utiliser Redfish. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.
    - Utiliser l'interface utilisateur Web. Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.
    - Utiliser IPMI (vias KCS ou IOL) Voir Accéder au BMC en utilisant IPMI sur LAN (IOL) ou Accéder au BMC en utilisant IPMI (KCS) pour les instructions d'accès.
    - Utiliser le menu de configuration de l'UEFI/BIOS. Voir Accéder à l'UEFI/BIOS pour les instructions d'accès.

10.3.1.2 Architecture réseau du BMC

10.3.1.2.1 Option module d'E/S de commutation Ethernet



Dans une plateforme équipée d'un module d'E/S de commutation Ethernet, le BMC est accessible via deux connexions réseau. Selon l'interface de configuration utilisée, les noms des connexions réseau changent.

IPMI et UEFI /BIOS	Redfish et interface utilisateur Web	Connectivité de réseau
Canal LAN 1 (LAN channel 1)	eth0	Panneau avant Srv 5
Canal LAN 2 (LAN channel 1)	eth1	Port interne du serveur 4 → port 16 du commutateur*

* Le BMC peut alors communiquer via les ports SFP Sw1 à Sw12, selon la configuration du commutateur.

10.3.1.2.2 Option module d'E/S de connexion directe

Le développement de cette option est envisagé. Veuillez contacter le service des ventes de Kontron.

10.3.1.3 Activer ou désactiver une interface réseau du BMC

Cet objectif peut être atteint :

- En utilisant Redfish
- En utilisant l'interface utilisateur Web du BMC
- En utilisant IPMI

10.3.1.3.1 Activer ou désactiver une interface réseau du BMC en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Afficher la liste des interfaces réseau du BMC et noter l'URL de l'interface à activer ou à désactiver. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/Managers/bmc/EthernetInterfaces/ | jq**

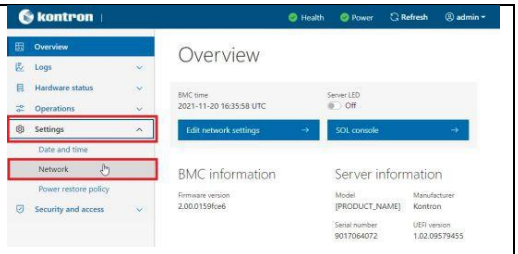
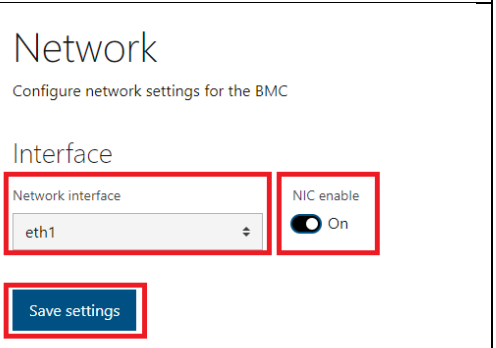
```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/Et
hernetInterfaces  | jq
{
  "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces",
  "@odata.type": "#EthernetInterfaceCollection.EthernetInterfaceCollection",
  "Description": "Collection of EthernetInterfaces for this Manager",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces/eth0"
    },
    {
      "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces/eth1"
    }
  ],
  "Members@odata.count": 2,
  "Name": "Ethernet Network Interface Collection"
}
```

Étape_2	Attribuer la valeur « true » à l'attribut InterfaceEnabled pour activer l'interface réseau ou la valeur « false » pour désactiver l'interface réseau. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/Managers/bmc/EthernetInterfaces/[NOM_INTERFACE] --header 'Content-Type: application/json' -- data '{"I nterfaceEnabled":[VALEUR]}' | jq**

```
$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/
EthernetInterfaces/eth1 --header 'Content-Type:application/json' --data '{"InterfaceEnabled": tr
ue}' | jq
```

10.3.1.3.2 Activer ou désactiver une interface réseau du BMC 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	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Settings**, puis sur **Network**.	
Étape_2	Dans le menu déroulant de la section **Interface**, sélectionner une interface réseau à configurer.	
Étape_3	Cliquer sur le bouton **NIC enable** pour activer ou désactiver l'interface réseau.	
Étape_4	Cliquer sur **Save settings**.	

10.3.1.3.3 Activer ou désactiver une interface réseau du BMC 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] -C 17**.

Étape_1	Activer ou désactiver une interface réseau du BMC InviteSE_ServeurLocal:~# **ipmitool lan set [CANAL_LAN] access [VALEUR]** Où [VALEUR] peut être ON ou OFF.	`[root@localhost ~]# ipmitool lan set 1 access on` `Set Channel Access for channel 1 was successful.`

10.3.1.4 Configurer une adresse IP statique

Cet objectif peut être atteint :

- En utilisant Redfish
- En utilisant l'interface utilisateur Web du BMC
- Utiliser le menu de configuration de l'UEFI/BIOS
- En utilisant IPMI

NOTE : Si un VLAN doit être configuré, voir Configurer un VLAN pour une interface réseau du BMC.

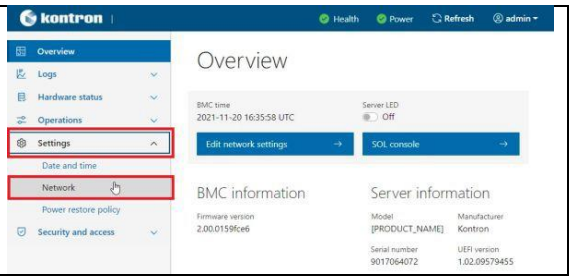
10.3.1.4.1 Configurer une adresse IP statique en utilisant Redfish

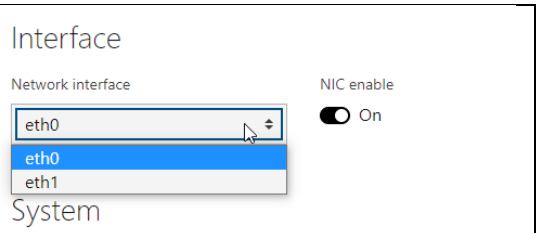
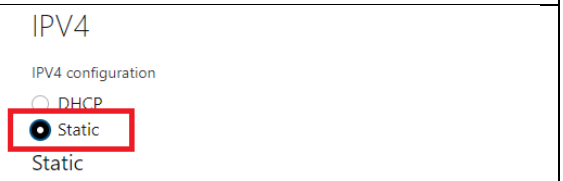
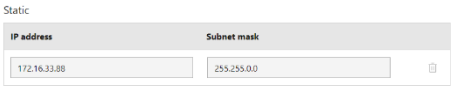
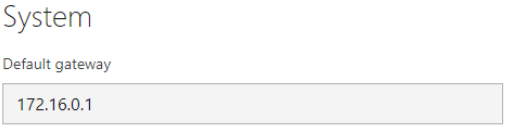
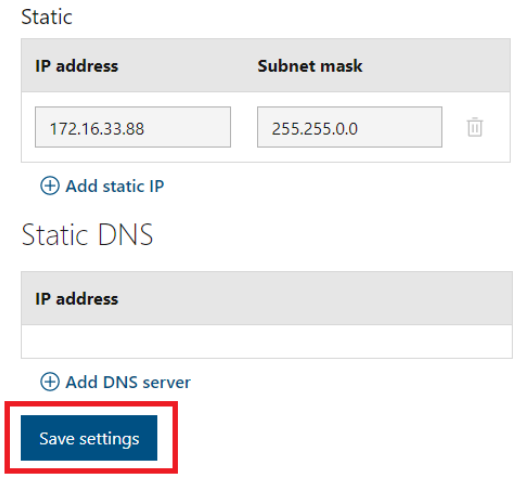
Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Pour modifier une adresse IP statique en utilisant Redfish, l'objet IPv4StaticAddresses d'une interface réseau doit être modifié : InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/Managers/bmc/EthernetInterfaces/[NOM_INTERFACE] --header 'Content-Type: application/json' -- data '{"IPv4StaticAddresses": [{"Address": "[ADRESSE_IP]","SubnetMask": "[MASQUE]", "Gateway" : "[PASSERELLE]"}]}' | jq**
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/EthernetInterfaces/eth1 --header 'Content-Type:application/json' --data '{"IPv4StaticAddresses": [{"Address": "172.16.182.32","SubnetMask": "255.255.0.0","Gateway": "172.16.0.1"}]}' | jq`

10.3.1.4.2 Configurer une adresse IP statique en utilisant l'interface utilisateur Web du BMC

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

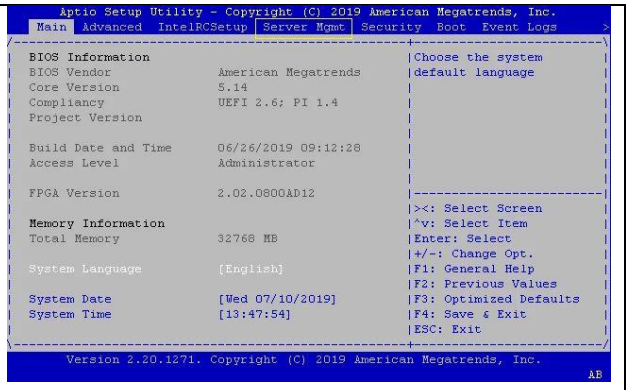
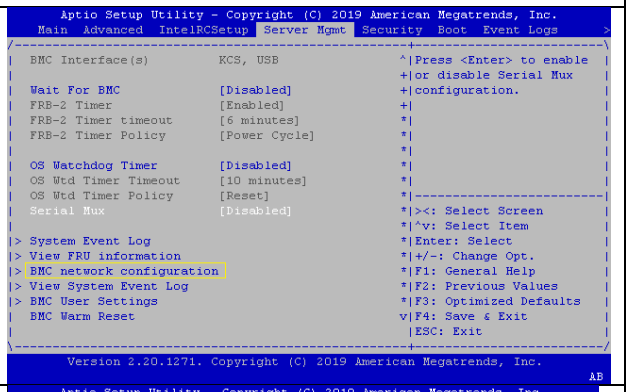
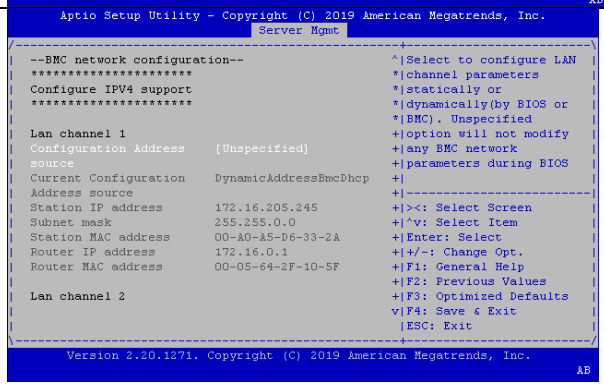
Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Settings**, puis sur **Network**.	

Étape_2	Sélectionner l'interface réseau à configurer dans le menu déroulant.	
Étape_3	Dans la section **IPV4**, sélectionner **Static**.	
Étape_4	Dans la section **Static**, définir les champs **IP address** et **Subnet mask**.	
Étape_5	Dans la section **System**, configurer le champ **Default gateway**.	
Étape_6	Cliquer sur **Save settings**.	

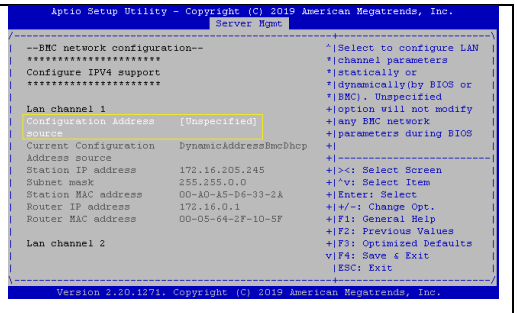
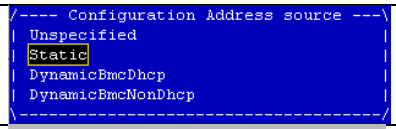
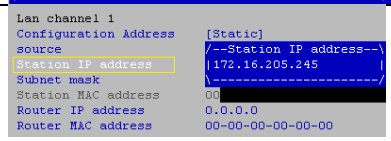
10.3.1.4.3 Configurer une adresse IP statique en utilisant le menu de configuration de l'UEFI/BIOS

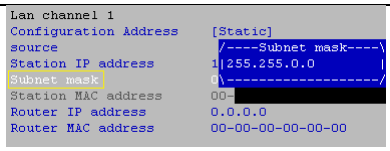
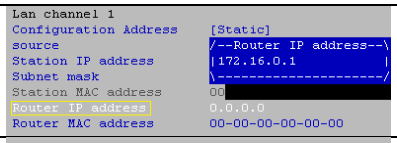
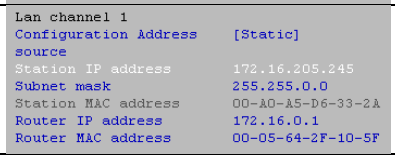
Voir Accéder à l'UEFI/BIOS pour les instructions d'accès.

10.3.1.4.3.1 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.	

10.3.1.4.3.2 Configurer une adresse IP statique en utilisant le menu de configuration de l'UEFI/BIOS

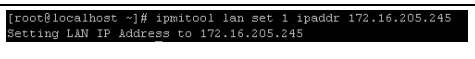
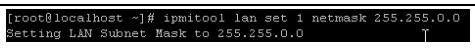
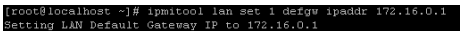
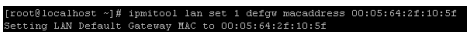
Étape_1	À partir du menu **BMC network configuration**, sélectionner l'option **Configuration Address source** pour l'interface LAN à configurer (canal LAN 1 dans cet exemple).	
Étape_2	Sélectionner **Static**.	
Étape_3	Modifier le paramètre **Station IP address**. **NOTE :** Il s'agit de l'adresse IP du BMC (**IP_GESTION_BMC**).	

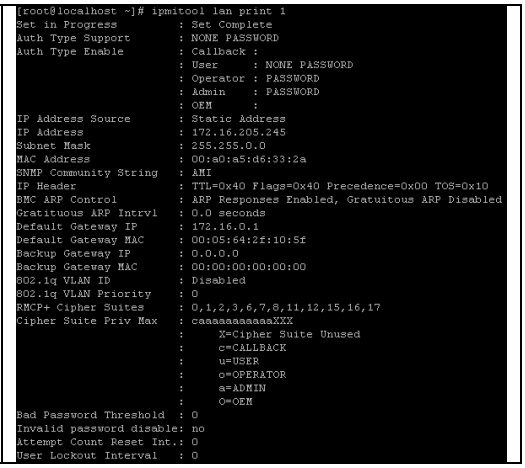
Étape_4	Modifier le paramètre **Subnet mask**.	
Étape_5	Modifier le paramètre **Router IP address**.	
Étape_6	Confirmer que la configuration a été modifiée et quitter le menu **BMC network configuration** en utilisant la touche **Échap [ESC]**.	

10.3.1.4.4 Configurer une adresse IP statique 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] -C 17**.

10.3.1.4.4.1 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.	
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.	
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.	
Étape_5	Définir l'adresse MAC de la passerelle par défaut. InviteSE_ServeurLocal:~# **ipmitool lan set [CANAL_LAN] defgw macaddress [MAC_ROUTEUR]**	

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

10.3.1.5 Configurer une adresse IP dynamique en utilisant DHCP

Cet objectif peut être atteint :

- En utilisant Redfish
- En utilisant l'interface utilisateur Web du BMC
- Utiliser le menu de configuration de l'UEFI/BIOS
- En utilisant IPMI

NOTE : Si un VLAN doit être configuré, voir Configurer un VLAN pour une interface réseau du BMC.

10.3.1.5.1 Configurer une adresse IP dynamique en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

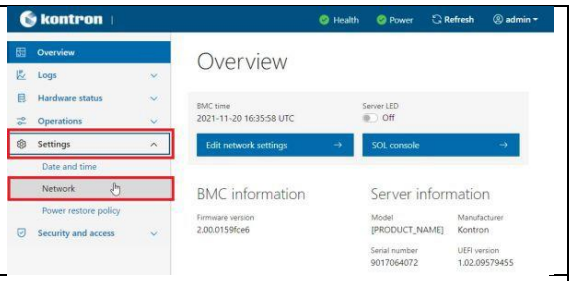
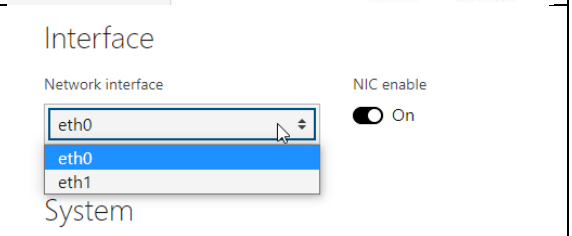
Étape_1	Pour activer la méthode d'adressage DHCP dans Redfish, mettre à jour l'interface réseau du BMC appropriée avec le champ DHCP. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE] /redfish/v1/Managers/bmc/EthernetInterfaces/ [NOM_INTERFACE] --header 'Content-Type: application/json' --data '{"DHCPv4": {"DHCPEnabled": true}}' | jq**

```
$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/
EthernetInterfaces/eth1 --header 'Content-Type:application/json' --data '{"DHCPv4": {"DHCPEnable
d": true}}' | jq
{
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "Message": "Successfully Completed Request",
      "MessageArgs": [],
      "MessageId": "Base.1.8.1.Success",
      "MessageSeverity": "OK",
      "Resolution": "None"
    }
  ]
}
```

10.3.1.5.2 Configurer une adresse IP dynamique en utilisant l'interface utilisateur Web du BMC

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

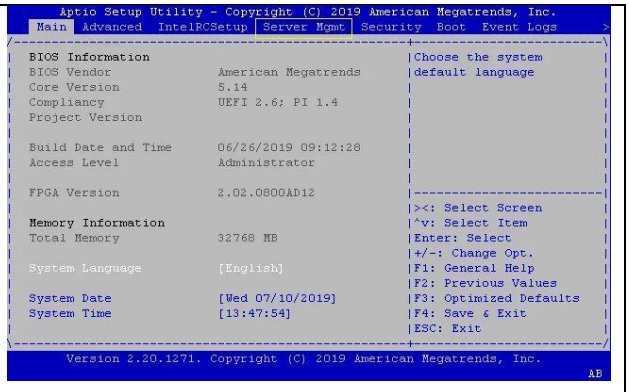
10.3.1.5.2.1 Configurer une adresse IP dynamique

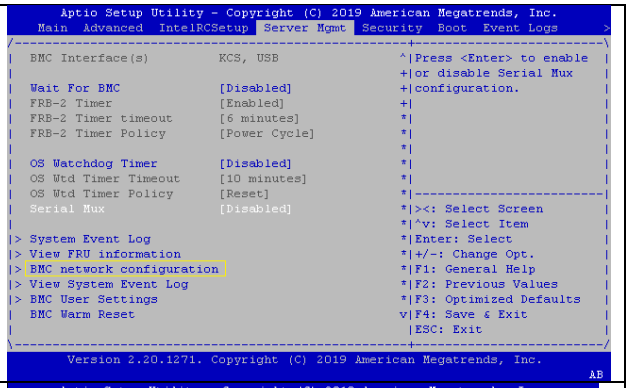
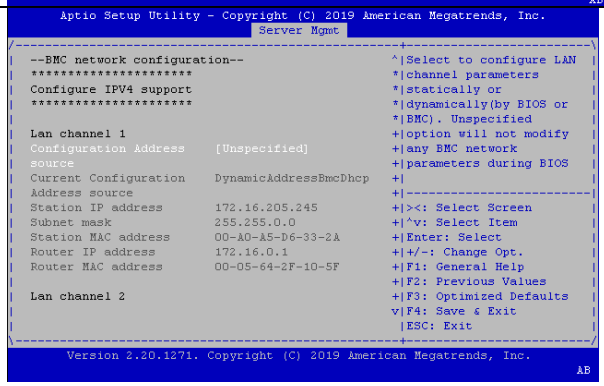
Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Settings**, puis sur **Network**.	
Étape_2	Sélectionner l'interface réseau à configurer dans le menu déroulant.	
Étape_3	Dans la section **IPV4**, sélectionner **DHCP**.	
Étape_4	Cliquer sur **Save settings**.	

10.3.1.5.3 Configurer une adresse IP dynamique en utilisant le menu de configuration de l'UEFI/BIOS

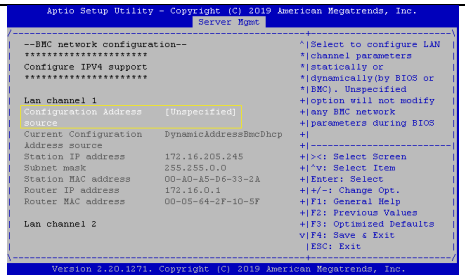
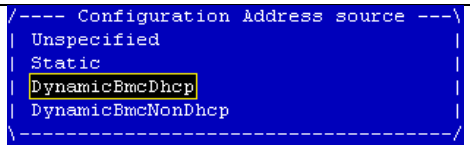
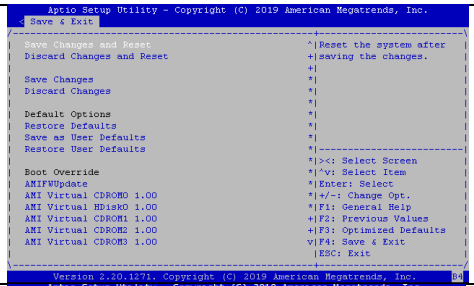
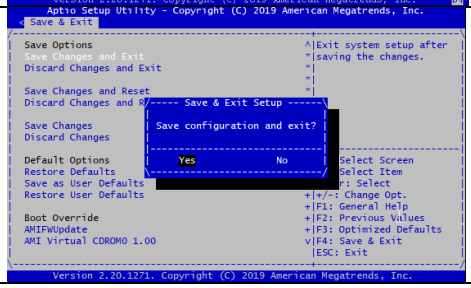
Voir Accéder à l'UEFI/BIOS pour les instructions d'accès.

10.3.1.5.3.1 Accéder au menu BMC network configuration

Étape_1	À partir du menu UEFI/BIOS, naviguer jusqu'à l'onglet **Server Mgmt**.	

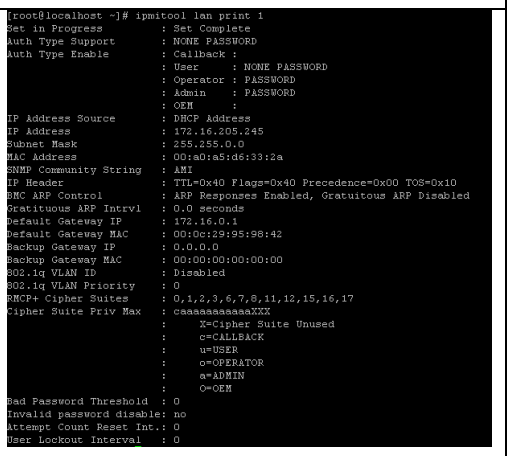
Étape_2	Sélectionner **BMC network configuration**.	
Étape_3	Le menu **BMC network configuration** s'affiche. **NOTE :** Lorsque la plateforme est démarrée après avoir été éteinte, l'UEFI/BIOS peut se charger avant que le BMC n'ait reçu son adresse IP. Dans ce cas, les informations du menu UEFI/BIOS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

10.3.1.5.3.2 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**. Cette opération réinitialise le serveur.	
Étape_5	Lorsque l'écran d'accueil de l'UEFI/BIOS s'affiche, appuyer sur la touche spécifiée pour accéder au menu de configuration de l'UEFI/BIOS. Ensuite, accéder au menu **Server Mgmt** et sélectionner **BMC network configuration**. L'adresse affichée est l'adresse IP du BMC (IP_GESTION_BMC).	

10.3.1.5.4 Configurer une adresse IP dynamique 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] -C 17**.

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).	

10.3.1.6 Configurer un VLAN pour une interface réseau du BMC

Compte tenu de l'architecture du ME1310, si un VLAN est attribué à l'interface réseau eth1 du BMC, le port 1/16 du commutateur doit refléter la configuration. S'assurer que le port 1/16 est membre du VLAN attribué. Voir Connexions internes et Configurer les VLAN du commutateur.

10.3.1.6.1 Attribuer un VLAN

Cet objectif peut être atteint :

- En utilisant Redfish
- En utilisant l'interface utilisateur Web du BMC
- En utilisant IPMI

10.3.1.6.1.1 Attribuer un VLAN en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Sélectionner une interface réseau du BMC et noter son URL. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET –url [URL_RACINE]/redfish/v1/Managers/bmc/EthernetInterfaces | jq**

	<pre>$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/EthernetInterfaces | jq
	{
	  "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces",
	  "@odata.type": "#EthernetInterfaceCollection.EthernetInterfaceCollection",
	  "Description": "Collection of EthernetInterfaces for this Manager",
	  "Members": [
	  {
	  "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces/eth0"
	  },
	  {
	  "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces/eth1"
	  }
	  ],
	  "Members@odata.count": 2,
	  "Name": "Ethernet Network Interface Collection"
	}</pre>

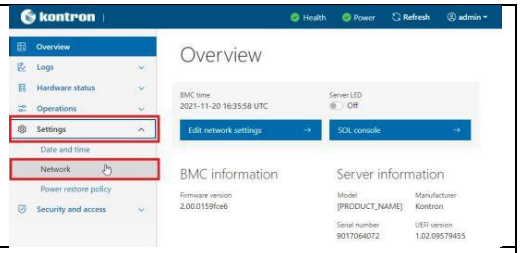
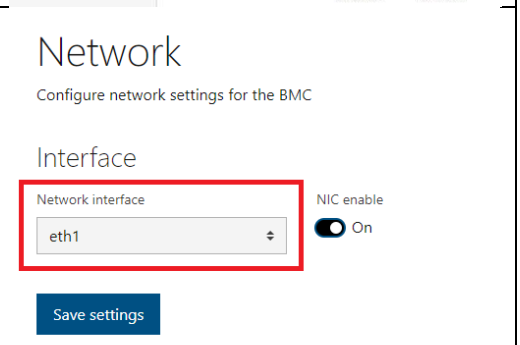
Étape_2	Ajouter un VLAN pour l'interface réseau du BMC sélectionnée à l'aide de la commande suivante. InviteSE_OrdinateurDistant:~# **curl -k -s --request POST --url [URL_RACINE]/redfish/v1/Managers/bmc/EthernetInterfaces/[NOM_INTERFACE]/VLANs --header 'Content-Type: application/json' --data '{"VLANEnable": true,"VLANI d": [ID_VLAN] }' | jq**

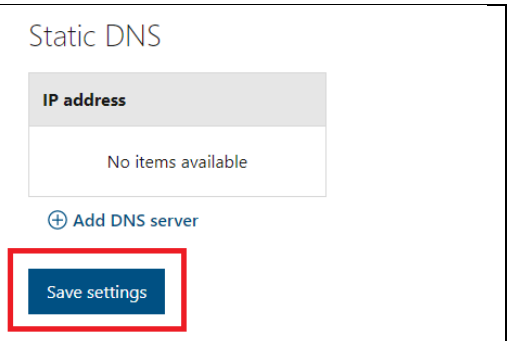
	<pre>$ curl -k -s --request POST --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/EthernetInterfaces/eth1/VLANs --header 'Content-Type:application/json' --data '{"VLANEnable": true,"VLANId": 1}' | jq
	{
	  "@Message.ExtendedInfo": [
	  {
	  "@odata.type": "#Message.v1_1_1.Message",
	  "Message": "The resource has been created successfully",
	  "MessageArgs": [],
	  "MessageId": "Base.1.8.1.Created",
	  "MessageSeverity": "OK",
	  "Resolution": "None"
	  }
	  ]
	}</pre>

Étape_3	Configurer une adresse IP pour l'interface VLAN créée à l'aide de l'une des méthodes Redfish décrites dans cette section.

10.3.1.6.1.2 Attribuer un VLAN en utilisant l'interface utilisateur Web du BMC

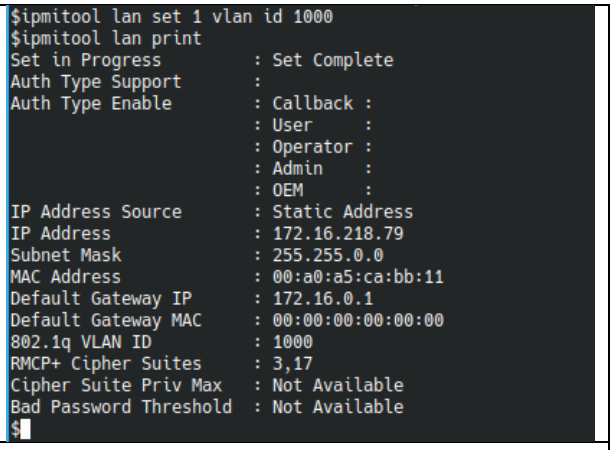
Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Settings**, puis sur **Network**.	
Étape_2	Dans le menu déroulant de la section **Interface**, sélectionner une interface réseau à configurer.	
Étape_3	Pour attribuer un VLAN, cocher la case appropriée dans la section **VLAN** et entrer l'ID du VLAN à associer à l'interface réseau.	

Étape_4	Cliquer sur **Save settings**.	
Étape_5	Configurer une adresse IP pour l'interface VLAN créée à l'aide de l'une des méthodes faisant appel à l'interface utilisateur Web décrites dans cette section.	

10.3.1.6.1.3 Attribuer un VLAN 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] -C 17**.

Étape_1	Associer un VLAN préconfiguré à une interface. InviteSE_ServeurLocal:~# **ipmitool lan set [CANAL_LAN] vlan id [ID_VLAN]**	
Étape_2	Configurer une adresse IP pour l'interface VLAN créée à l'aide de l'une des méthodes IPMI décrites dans cette section.	

10.3.1.6.2 Supprimer un VLAN

Cet objectif peut être atteint :

- En utilisant Redfish
- En utilisant l'interface utilisateur Web du BMC
- En utilisant IPMI

10.3.1.6.2.1 Supprimer un VLAN en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Sélectionner une interface réseau du BMC et noter son URL. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/Managers/bmc/EthernetInterfaces | jq**

	<pre>$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/EthernetInterfaces | jq
	{
	  "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces",
	  "@odata.type": "#EthernetInterfaceCollection.EthernetInterfaceCollection",
	  "Description": "Collection of EthernetInterfaces for this Manager",
	  "Members": [
	  {
	  "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces/eth0"
	  },
	  {
	  "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces/eth1"
	  }
	  ],
	  "Members@odata.count": 2,
	  "Name": "Ethernet Network Interface Collection"
	}</pre>

Étape_2	Afficher la liste des VLAN d'une interface réseau du BMC sélectionnée et noter l'URL du VLAN à supprimer. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/Managers/bmc/EthernetInterfaces/[NOM_INTERFACE]/VLANs | jq**

	<pre>$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/EthernetInterfaces/eth1/VLANs | jq
	{
	  "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces/eth1/VLANs",
	  "@odata.type": "#VLanNetworkInterfaceCollection.VLanNetworkInterfaceCollection",
	  "Members": [
	  {
	  "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces/eth1/VLANs/eth1_1"
	  }
	  ],
	  "Members@odata.count": 1,
	  "Name": "VLAN Network Interface Collection"
	}</pre>

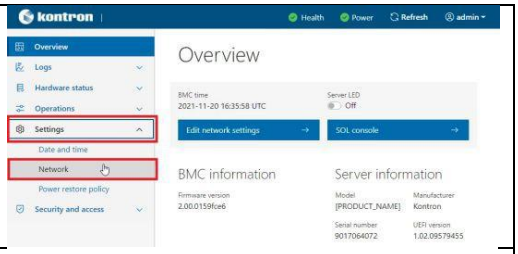
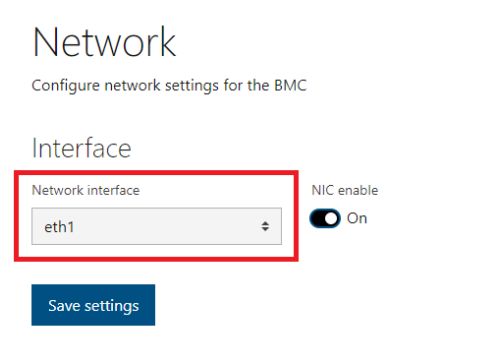
Étape_3	Accéder aux informations du VLAN afin de recueillir son ID. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/Managers/bmc/EthernetInterfaces/[NOM_INTERFACE]/VLANs/ [URL_VLAN] | jq.VLANId**

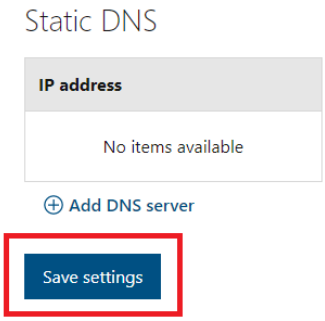
	<pre>$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/EthernetInterfaces/eth1/VLANs/eth1_1 | jq .VLANId
	[
	  1
	]</pre>

Étape_4	Supprimer le VLAN pour l'interface réseau du BMC sélectionnée à l'aide de la commande suivante. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/Managers/bmc/EthernetInterfaces/[NOM_INTERFACE]/VLANs/ [URL_VLAN] --header 'Content-Type: application/json' --data '{"VLANEnable": false, "VLANI d": [ID_VLAN] }' | jq**
	<pre>$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/EthernetInterfaces/eth1/VLANs/eth1_1 --header 'Content-Type:application/json' --data '{"VLANEnable": false,"VLANId": 1}' | jq</pre>

10.3.1.6.2.2 Supprimer un VLAN en utilisant l'interface utilisateur Web du BMC

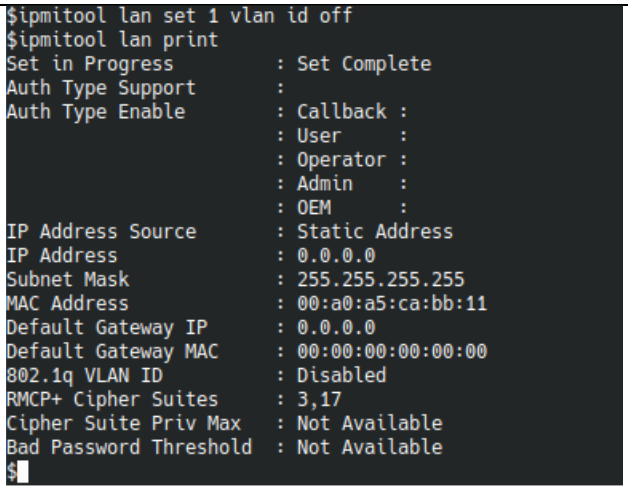
Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Settings**, puis sur **Network**.	
Étape_2	Dans le menu déroulant de la section **Interface**, sélectionner une interface réseau à configurer.	

Étape_3	Pour supprimer un VLAN, décocher la case appropriée dans la section **VLAN**.	
Étape_4	Cliquer sur **Save settings**.	

10.3.1.6.2.3 Supprimer un VLAN 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] -C 17**.

Étape_1	Définir l'ID du VLAN associé à une interface à **OFF**. InviteSE_ServeurLocal:~# **ipmitool lan set [CANAL_LAN] vlan id off**	

10.3.1.7 Configurer l'adresse IP de l'interface hôte Redfish du serveur intégré

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

Les ressources de BMC Redfish sont accessibles localement via le serveur intégré à l'aide de l'interface hôte Redfish interne et privée. Dans cette plateforme, la fonctionnalité est mise en œuvre à l'aide d'une interface USB vers LAN. La plupart des systèmes d'exploitation Linux modernes devraient intégrer la prise en charge de ce périphérique USB vers LAN. La procédure ci-dessous permet de configurer l'adresse IP utilisée pour l'interface hôte.

Étape_1	Trouver le nom de l'interface USB détectée dans Linux. Cela peut être fait en listant le nom « net » à partir du dossier sysfs.
	
	InviteSE_ServeurLocal:~# **ls /sys/bus/usb/drivers/rndis_host/*/net**
	
	Exemple avec CentOS 7 :
	`$ls /sys/bus/usb/drivers/rndis_host/1-3.2:1.0/net`
	`enp0s20f0u3u2`
	`$`
	Dans cet exemple, le nom découvert pour l'interface est **enp0s20f0u3u2**.
	Exemple avec Ubuntu :
	`$ls /sys/bus/usb/drivers/rndis_host/1-3.2\:1.0/net/`
	`enx00248c46642c`
	`$`
	Dans cet exemple, le nom découvert pour l'interface est **enx00248c46642c**.

Étape_2	Configurer une adresse IP statique en utilisant l'interface USB vers LAN
	InviteSE_ServeurLocal:~# **ip addr add 169.254.0.1/24 dev [NOM_INTERFACE]**
	
	`$ip addr add 169.254.0.1/24 dev enp0s20f0u3u2`
	`$ip addr show`
	`1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000`
	`link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00`
	`inet 127.0.0.1/8 scope host lo`
	`valid_lft forever preferred_lft forever`
	`inet6 ::1/128 scope host`
	`valid_lft forever preferred_lft forever`
	`2: eno5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000`
	`link/ether 00:a0:a5:dd:4a:10 brd ff:ff:ff:ff:ff:ff`
	`3: eno4: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000`
	`link/ether 00:00:00:00:03:14 brd ff:ff:ff:ff:ff:ff`
	`4: eno3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000`
	`link/ether 00:00:00:00:03:15 brd ff:ff:ff:ff:ff:ff`
	`5: enp0s20f0u3u2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000`
	`link/ether 00:24:8c:46:64:2c brd ff:ff:ff:ff:ff:ff`
	`inet 169.254.0.1/24 scope global enp0s20f0u3u2`
	`valid_lft forever preferred_lft forever`
	`6: eno2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000`
	`link/ether 00:00:00:00:03:16 brd ff:ff:ff:ff:ff:ff`
	`7: eno1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000`
	`link/ether 00:00:00:00:03:17 brd ff:ff:ff:ff:ff:ff`
	`$_`

Étape_3	Vous pouvez maintenant accéder à l'interface Redfish du BMC à l'aide de l'adresse IP de l'interface hôte Redfish interne.
	
	L'adresse IP du BMC est toujours **169.254.0.17**.
	InviteSE_ServeurLocal:~# **curl -k https://[NOM_UTILISATEUR]:[MOT_DE_PASSE]@169.254.0.17/redfish/v1/[URL]**
	
	`$curl -k https://admin:ready2go@169.254.0.17/redfish/v1/`
	`{`
	`"@odata.context": "/redfish/v1/$metadata#ServiceRoot.ServiceRoot",`
	`"@odata.id": "/redfish/v1",`
	`"@odata.type": "#ServiceRoot.v1_5_0.ServiceRoot",`
	`"AccountService": {`
	`"@odata.id": "/redfish/v1/AccountService"`
	`},`
	`"CertificateService": {`
	`"@odata.id": "/redfish/v1/CertificateService"`
	`},`
	`"Chassis": {`
	`"@odata.id": "/redfish/v1/Chassis"`
	`},`
	`"Id": "RootService",`
	`"JsonSchemas": {`
	`"@odata.id": "/redfish/v1/JsonSchemas"`
	`},`
	`"Links": {`
	`"Sessions": {`
	`"@odata.id": "/redfish/v1/SessionService/Sessions"`
	`}`
	`},`
	`"Managers": {`
	`"@odata.id": "/redfish/v1/Managers"`
	`},`
	`"Name": "Root Service",`
	`"RedfishVersion": "1.6.1",`
	`"Registries": {`
	`"@odata.id": "/redfish/v1/Registries"`
	`},`
	`"SessionService": {`
	`"@odata.id": "/redfish/v1/SessionService"`
	`},`
	`"Systems": {`
	`"@odata.id": "/redfish/v1/Systems"`
	`},`
	`"UUID": "46e90382-3e10-41f2-b743-a5a850139658",`
	`"UpdateService": {`
	`"@odata.id": "/redfish/v1/UpdateService"`
	`}`
	`}`
	`$`

10.3.2 Configuration du démarrage réseau UEFI

Les options de démarrage réseau suivantes sont prises en charge sur la plateforme :

- PXE
- Démarrage HTTP

Le démarrage réseau UEFI peut être configuré :

- En utilisant le menu UEFI/BIOS

10.3.2.1 Configurer le démarrage réseau UEFI en utilisant le menu UEFI/BIOS

10.3.2.1.1 Préalables

1	L'accès au menu UEFI/BIOS est nécessaire.
2	Un serveur de démarrage est configuré et détectable via DHCP. **NOTE :** L'adresse du serveur de démarrage ne peut pas être définie à l'aide d'une adresse IP statique.

Sections pertinentes :

Accéder à l'UEFI/BIOS

Configuration réseau du BMC

Adresses MAC

Mappage PCI

Architecture du produit

10.3.2.1.2 Configuration réseau de l'UEFI en utilisant le menu UEFI/BIOS

Les paramètres réseau de l'UEFI doivent être configurés pour que l'UEFI puisse communiquer avec un serveur de démarrage distant.

NOTE : Sur une plateforme équipée du module d'E/S de commutation Ethernet, les VLAN doivent être configurés pour tout trafic étiqueté VLAN provenant de l'interface 25GbE E823 du serveur. Voir Architecture du produit pour de l'information sur les interfaces réseau ou Configurer les VLAN pour le démarrage réseau UEFI pour des directives de configuration.

10.3.2.1.2.1 Identification des interfaces réseau

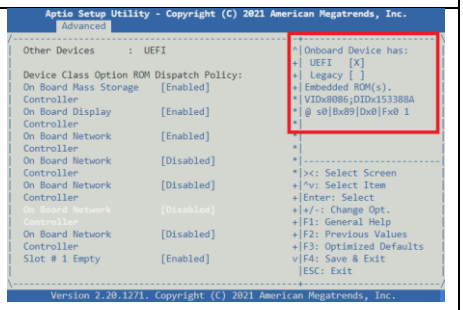
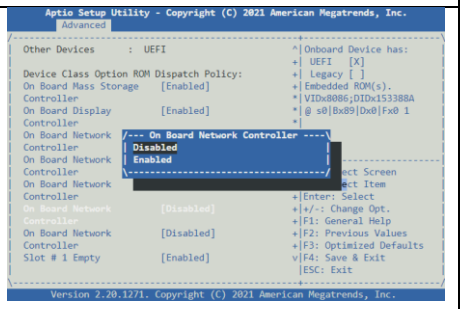
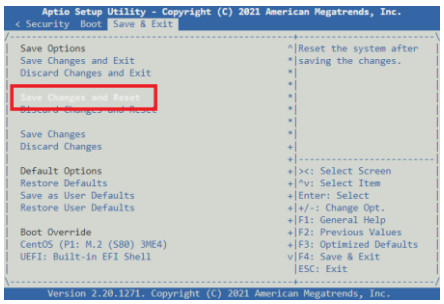
Au moins une interface réseau UEFI doit être configurée pour effectuer un démarrage réseau.

Dans le menu UEFI/BIOS, les interfaces réseau UEFI sont désignées par leur mappage PCI. Utiliser la colonne **Bus:Device.Function** pour identifier l'interface dans le menu UEFI/BIOS.

Appellation typique dans Linux	Vitesse (bps)	Appellation du port dans le NOS	Bus: Device. Function
eno1	25G	Ethernet 1/13	89:00.3
eno2	25G	Ethernet 1/14	89:00.2
eno3	25G	Ethernet 1/15	89:00.1
eno4	25G	Ethernet 1/16	89:00.0
eno5	1G	Sans objet	05:00.0

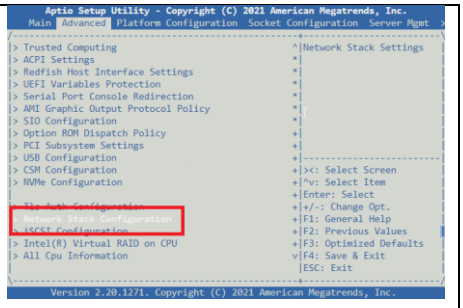
10.3.2.1.2.2 Activer le support UEFI pour les contrôleurs réseau installés

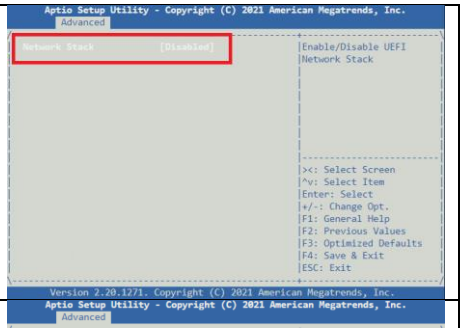
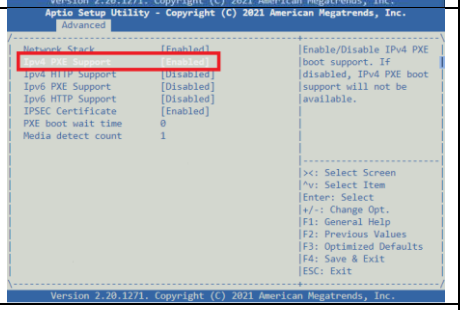
Voir le tableau Identification des interfaces réseau. Le texte de l'aide devrait correspondre à la colonne **Bus:Device.Function**.

Étape_1	Redémarrer la plateforme et accéder au menu de configuration de l'UEFI/BIOS.	
Étape_2	Naviguer vers le menu **Advanced** et entrer dans le sous-menu **Option ROM Dispatch Policy**.	
Étape_3	Identifier le contrôleur réseau à l'aide du texte d'aide.	
Étape_4	Activer ou désactiver les contrôleurs réseau souhaités.	
Étape_5	Sélectionner le menu **Save & Exit**, aller à **Save Changes and Reset** et appuyer sur **Entrée**.	

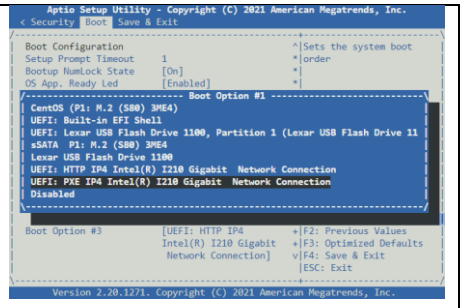
10.3.2.1.3 Configurer le démarrage réseau PXE en utilisant le menu UEFI/BIOS

10.3.2.1.3.1 Activer la prise en charge PXE

Étape_1	Dans le menu de configuration de l'UEFI/BIOS, sélectionner l'onglet **Advanced**, puis le sous-menu **Network Stack Configuration**.	

Étape_2	Si nécessaire, activer le **Network Stack**. **NOTE :** Si la pile réseau (network stack) est désactivée, le démarrage réseau UEFI l'est également.	
Étape_3	Activer ou désactiver **IPv4 PXE Support** et/ou **IPv6 PXE Support**.	
Étape_4	Sélectionner le menu **Save & Exit**, aller à **Save Changes and Reset** et appuyer sur **Entrée**.	

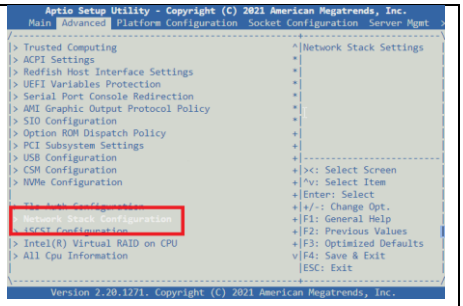
10.3.2.1.3.2 Exécuter le démarrage réseau PXE

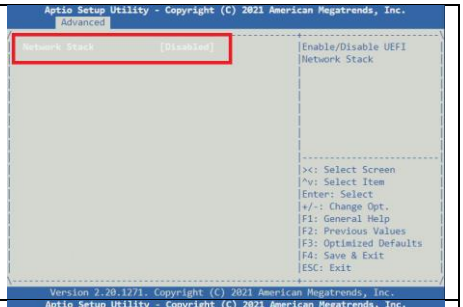
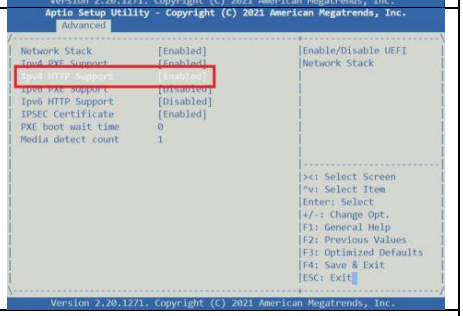
Étape_1	Dans le menu de configuration de l'UEFI/BIOS, naviguer jusqu'au menu **Boot**. Configurer l'ordre de démarrage comme souhaité. L'option de démarrage PXE doit être la première afin d'avoir la priorité sur les autres options de démarrage. **NOTE :** La fonction « Boot Override » peut également être utilisée pour choisir manuellement la priorité pour un démarrage unique.	
Étape_2	Sélectionner le menu **Save & Exit**, aller à **Save Changes and Reset** et appuyer sur **Entrée** pour confirmer et enregistrer le nouvel ordre de démarrage. La plateforme devrait démarrer en utilisant PXE.	

10.3.2.1.4 Configurer le démarrage réseau HTTP en utilisant le menu UEFI/BIOS

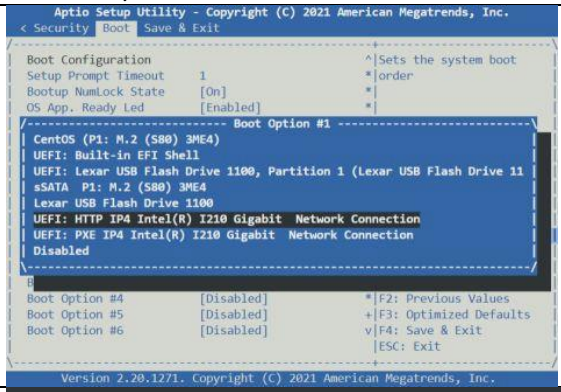
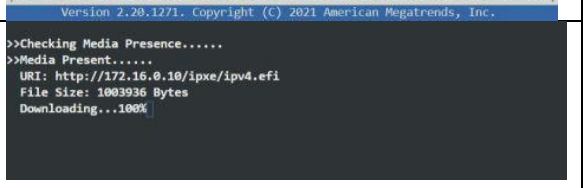
Le **Boot URL** peut être défini explicitement, mais il est très souvent transmis par le serveur DHCP au cours du processus de sélection de l'adresse IP. Veuillez consulter votre administrateur de réseau pour obtenir des informations sur votre installation.

10.3.2.1.4.1 Activer la prise en charge du démarrage HTTP

Étape_1	Dans le menu de configuration de l'UEFI/BIOS, sélectionner l'onglet **Advanced**, puis le sous-menu **Network Stack Configuration**.	

Étape_2	Si nécessaire, activer le **Network Stack**. **NOTE :** Si le réseau est désactivé, le démarrage réseau UEFI l'est également.	
Étape_3	Activer ou désactiver **IPv4 HTTP Support** et/ou **IPv6 HTTP Support**.	
Étape_4	Sélectionner le menu **Save & Exit**, aller à **Save Changes and Reset** et appuyer sur **Entrée**.	

10.3.2.1.4.2 Exécuter le démarrage réseau HTTP

Étape_1	Redémarrer la plateforme et accéder au menu de configuration de l'UEFI/BIOS.	
Étape_2	Dans le menu de configuration de l'UEFI/BIOS, naviguer jusqu'au menu **Boot**. Configurer l'ordre de démarrage comme souhaité. L'option de démarrage HTTP doit être la première afin d'avoir la priorité sur les autres options de démarrage. **NOTE :** La fonction « Boot Override » peut également être utilisée pour choisir manuellement la priorité pour un démarrage unique.	
Étape_3	Sélectionner le menu **Save & Exit**, aller à **Save Changes and Reset** et appuyer sur **Entrée** pour confirmer et enregistrer le nouvel ordre de démarrage. La plateforme devrait démarrer en utilisant le démarrage HTTP.	

10.3.2.2 Configurer des VLAN pour le démarrage réseau UEFI en utilisant l'UEFI

Sur une plateforme équipée du module d'E/S de commutation Ethernet, les VLAN doivent être configurés pour tout trafic étiqueté VLAN provenant de l'interface 25GbE E823 du serveur. Voir Configuration du commutateur pour connaître les procédures de configuration des VLAN faisant appel au système d'exploitation réseau du commutateur.

Le menu de configuration de l'UEFI/BIOS propose des options pour créer/configurer/supprimer des VLAN sur chacune des quatre interfaces 25GbE du E823 ainsi que sur l'interface 1GbE du I210 du serveur. Voir Architecture du produit pour plus d'information sur les interfaces réseau. Toutefois, les menus de configuration de l'UEFI/BIOS permettant de configurer les VLAN ne sont disponibles que lorsque les services réseau UEFI sont activés.

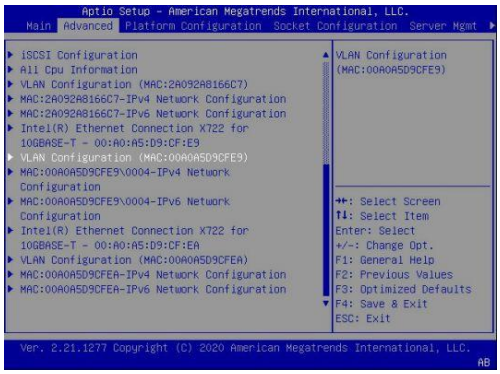
10.3.2.2.1 Configurer des VLAN pour le démarrage réseau UEFI en utilisant le menu UEFI/BIOS

Sections pertinentes :

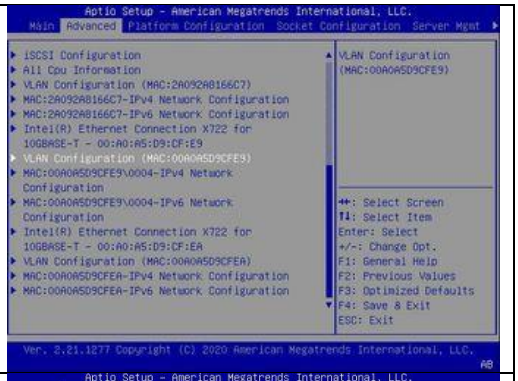
Accéder à l'UEFI/BIOS

Adresses MAC

10.3.2.2.1.1 Créer des VLAN

Étape_1	Dans le menu de configuration de l'UEFI/BIOS, sélectionner le menu **Advanced**, puis sélectionner une section **VLAN Configuration (MAC:xxxxxxxxxxxx)**. Sélectionner **Enter Configuration Menu**. **NOTE :** L'adresse MAC sera l'adresse MAC de l'interface 25GbE E823 ou 1GbE I210 à configurer.	
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.	
Étape_4	Ajouter d'autres VLAN si nécessaire en répétant 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. • 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 attribuer des VLAN à une autre interface 25GbE E823, si nécessaire.	
Étape_6	Appuyer sur **F4** pour enregistrer les changements et quitter.	

10.3.2.2.1.2 Supprimer des VLAN

Étape_1	Dans le menu de configuration de l'UEFI/BIOS, sélectionner le menu **Advanced**, puis sélectionner une section **VLAN Configuration (MAC:xxxxxxxxxxxx)**. Sélectionner **Enter Configuration Menu**. **NOTE :** L'adresse MAC sera celle du port 25GbE du E823 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, le VLAN 2002 sera supprimé et le VLAN 1001 sera maintenu.	
Étape_3	Répéter les étapes 1 à 2 pour supprimer des VLAN dans une autre interface 25GbE E823, si nécessaire.	
Étape_4	Appuyer sur **F4** pour enregistrer les changements et quitter.	

10.3.3 Configuration réseau du commutateur

Les modifications apportées à la configuration du NOS ne sont pas persistantes après le redémarrage du NOS. Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config.

Dans l'interface utilisateur Web du NOS :

Sélectionner **Maintenance**, **Configuration**, puis **Save startup-config**. Cliquer sur **Save Configuration** pour confirmer le changement.

Dans le CLI du NOS :

InviteCLI_NOSLocal:~(config-if)# **end**

InviteCLI_NOSLocal:~# **copy running-config startup-config**

10.3.3.1 Configurer des adresses IP pour accéder au NOS

Cette section est utilisée pour configurer les adresses IP permettant d'accéder aux interfaces de configuration et de gestion du système d'exploitation du système d'exploitation réseau (NOS). Il s'agit de l'application responsable de la mise en œuvre des fonctionnalités de transfert de paquets L2/L3.

L'une de ces fonctionnalités est la prise de décisions pour le transfert de paquets sur la base de la balise VLAN. Dans ce contexte, les adresses IP pour communiquer avec le NOS sont attachées à un VLAN défini dans la base de données du NOS. Le commutateur dispose toujours d'au moins un VLAN1 auquel une interface peut être attribuée. Voir Configurer les VLAN du commutateur pour connaître les procédures d'ajout de VLAN faisant appel au système d'exploitation réseau.

10.3.3.2 Ajouter une adresse IP pour une interface VLAN du NOS

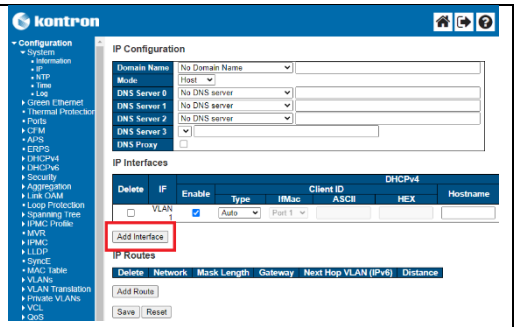
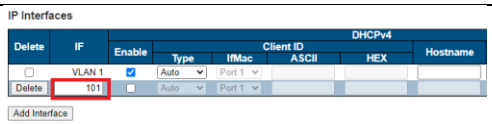
Cette action peut être faite :

- En utilisant l'interface utilisateur Web
- En utilisant le CLI

10.3.3.2.1 Ajouter une adresse IP pour une interface VLAN du NOS en utilisant l'interface utilisateur Web

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

10.3.3.2.1.1 Ajouter une interface VLAN dans le NOS

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **System**, puis **IP**.	
Étape_2	Cliquer sur le bouton **Add Interface**.	
Étape_3	Saisir l'ID numérique du VLAN. **NOTE :** Comme expliqué ci-dessus, le VLAN doit déjà exister pour ajouter l'adresse IP.	
Étape_4	Procéder à la configuration de l'adresse IP comme expliqué ci-dessous.	

Il existe deux options pour configurer les adresses IP :

- Configurer une adresse IP statique
- Configurer une adresse IP dynamique en utilisant DHCP

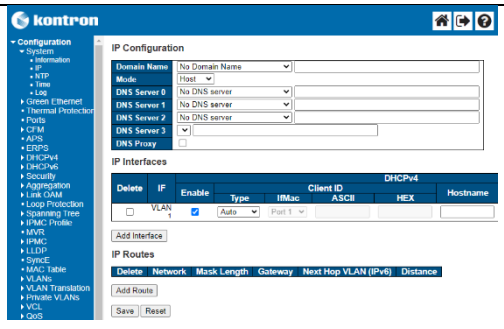
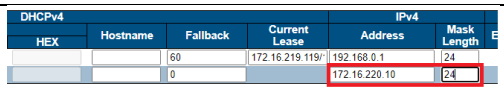
10.3.3.2.1.2 Configurer une adresse IP statique

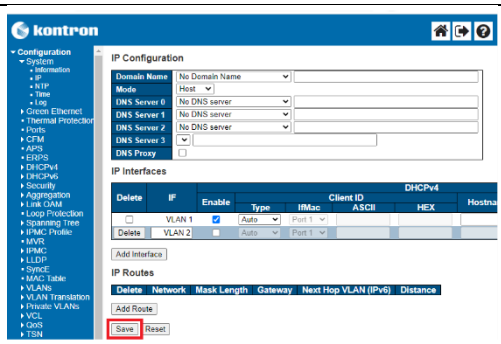
Sections pertinentes :

Configurer le routage statique

Configurer le service DNS

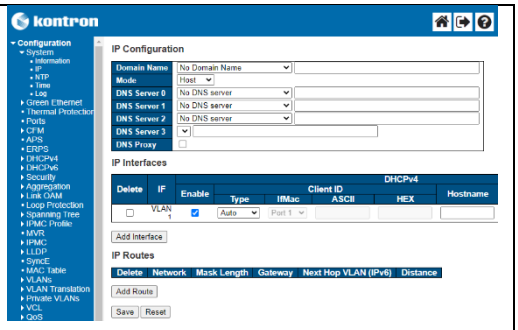
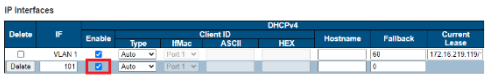
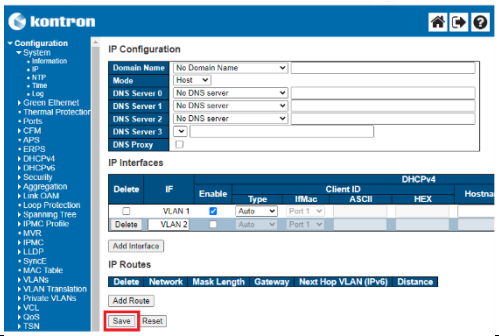
Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **System**, puis **IP**.	
Étape_2	Configurer manuellement l'adresse IP et la longueur du masque de réseau de l'interface VLAN.	

Étape_3	Cliquer sur le bouton **Save** pour confirmer.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.2.1.3 Configurer une adresse IP dynamique en utilisant DHCP

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **System**, puis **IP**.	
Étape_2	Activer DHCP en cochant la case associée à l'interface. Le champ **Hostname** permet au client DHCP d'utiliser un nom d'hôte différent de celui du NOS pour le champ de l'option 12 du DHCP. Le champ **Fallback** est un délai en secondes après lequel l'interface sera configurée en utilisant l'adresse IP statique dans les champs appropriés si une adresse ne peut être obtenue via DHCP.	
Étape_3	Cliquer sur le bouton **Save** pour confirmer.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.2.2 Ajouter une adresse IP pour une interface VLAN du NOS en utilisant le CLI

Voir Accéder au NOS pour les instructions d'accès.

10.3.3.2.2.1 Ajouter une interface VLAN dans le NOS en utilisant une adresse IP statique

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Entrer dans le mode de configuration d'une interface VLAN. Le VLAN doit avoir déjà été créé. InviteCLI_NOSLocal:~# **configure terminal** InviteCLI_NOSLocal:~(config)# **interface VLAN [ID_VLAN]**	`# configure terminal` `(config)# interface vlan 1`
Étape_2	Définir la source de l'adresse IP statique. InviteCLI_NOSLocal:~(config-if-vlan)# **ip address [ADRESSE_IP] [MASQUE]**	`(config-if-vlan)# ip address 192.168.0.1 255.255.255.0`
Étape_3	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.2.2.2 Ajouter une interface VLAN dans le NOS en utilisant DHCP

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Entrer dans le mode de configuration d'une interface VLAN. Le VLAN doit avoir déjà été créé. InviteCLI_NOSLocal:~# **configure terminal** InviteCLI_NOSLocal:~(config)# **interface VLAN [ID_VLAN]**	`# configure terminal` `(config)# interface vlan 1`
Étape_2	Définir la source de l'adresse IP sur DHCP. InviteCLI_NOSLocal:~(config-if-vlan)# **ip address dhcp** **NOTE :** Pour afficher l'adresse IP attribuée, utiliser la commande **do show ip interface**.	`(config-if-vlan)# ip address dhcp`
Étape_3	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.3 Supprimer une adresse IP pour une interface VLAN du NOS

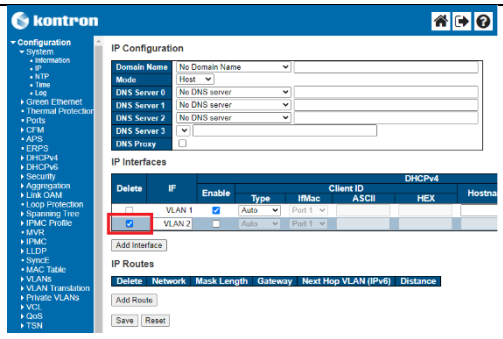
Cette action peut être faite :

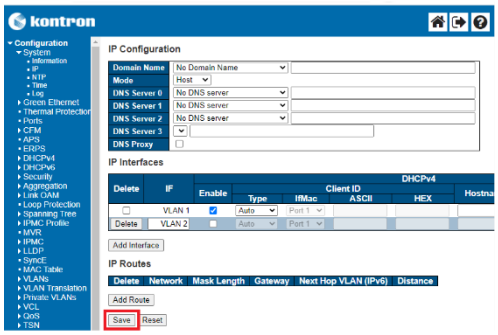
- En utilisant l'interface utilisateur Web
- En utilisant le CLI

10.3.3.3.1 Supprimer une adresse IP pour une interface VLAN du NOS en utilisant l'interface utilisateur Web

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

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **System**, puis **IP**.	
Étape_2	Sélectionner l'interface VLAN à supprimer.	

Étape_3	Cliquer sur le bouton **Save** pour confirmer.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.3.2 Supprimer une adresse IP pour une interface VLAN du NOS en utilisant le CLI

Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	`# configure terminal`
Étape_2	Supprimer le VLAN. InviteCLI_NOSLocal:~(config)# **no interface vlan [ID_VLAN]**	`(config)# no interface vlan 101`
Étape_3	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.4 Configurer le support HTTPS

Le support HTTPS doit être configuré. Cette action peut être faite :

- En utilisant l'interface utilisateur Web du NOS
- En utilisant le CLI du NOS

10.3.3.4.1 Configurer le support HTTPS en utilisant l'interface utilisateur Web

Deux protocoles permettent d'accéder au serveur Web : HTTP et HTTPS. Ils sont indépendants et peuvent être utilisés simultanément. Le commutateur réseau peut donc fonctionner dans l'un des trois modes suivants :

- **HTTP seulement** – Tous les renseignements sont transférés en texte clair (même les mots de passe). **Non sécurisé!** Les communications se font sur le port 80.
- **HTTPS seulement** – Tous les renseignements sont transférés dans des paquets chiffrés. **La communication est sécurisée.** Les requêtes HTTP sont automatiquement traduites en requêtes HTTPS. Les communications se font sur le port 443. **Un certificat est nécessaire pour HTTPS.**
- **HTTP et HTTPS** – Les utilisateurs peuvent utiliser n'importe lequel des deux protocoles. **Il s'agit de l'état par défaut, mais un certificat est nécessaire pour HTTPS.**

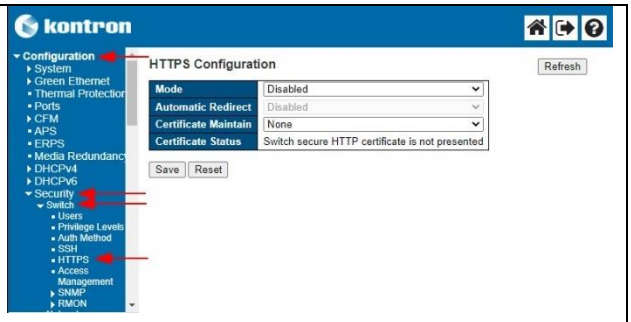
Pour que le protocole sécurisé HTTPS fonctionne, un certificat doit être installé. Voir la section Certificats ci-dessous.

10.3.3.4.1.1 Page de configuration HTTPS

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

Cette page est utilisée pour configurer les paramètres HTTPS et maintenir le certificat actuel sur le commutateur.

> Pour que le protocole sécurisé HTTPS fonctionne, un certificat doit être installé. À titre de mesure temporaire, le commutateur peut créer un certificat auto-signé, une solution sécurisée, mais qui ne peut être considérée comme une solution à long terme. Les utilisateurs devront fournir leur propre certificat, délivré par une autorité de certification valide.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **Security**, **Switch**, puis **HTTPS**.	
Étape_2	Sélectionner les paramètres souhaités pour **Mode**, **Automatic Redirect**, **Certificate Maintain** (en fonction de la valeur choisie, des champs supplémentaires seront disponibles) et **Certificate Status**. Le tableau ci-dessous explique les valeurs disponibles pour chaque champ.	
Étape_3	Cliquer sur le bouton **Save** pour confirmer.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.4.1.1.1 Valeurs disponibles pour les champs utilisés pour la configuration HTTPS

Champ	Description	Valeurs
Mode	Définit le mode de fonctionnement du protocole HTTPS.	Enabled : Le mode de fonctionnement HTTPS est activé. Disabled: Le mode de fonctionnement HTTPS est désactivé.

Champ	Description	Valeurs
Automatic Redirect	Définit le mode de fonctionnement de la redirection HTTPS. Cette configuration est requise uniquement lorsque le champ Mode est réglé sur Enabled. Lorsque la redirection est activée, la connexion HTTP est automatiquement redirigée vers la connexion HTTPS. Il est important de noter que le navigateur pourrait ne pas autoriser la redirection pour des raisons de sécurité, à moins que le navigateur ne fasse confiance au certificat du commutateur. Dans ce cas, une connexion HTTPS doit être initialisée manuellement. Lorsque la valeur de ce champ est à Enabled, le protocole HTTP est en réalité désactivé.	Enabled : Le mode de fonctionnement de la redirection HTTPS est activé. Disabled : Le mode de fonctionnement de la redirection HTTPS est désactivé.

Champ			Description	Valeurs
Certificate Maintain			Effectue la maintenance des certificats. Ce paramètre est opérationnel seulement lorsque le champ Mode est à Disabled.	None : Rien ne se passe. Delete : Supprime le certificat actuel. Upload : Télécharge le fichier de certificat PEM. Generate : Génère un nouveau certificat RSA auto-signé.
	Certificate Pass Phrase (disponible lorsque le champ Certificate Maintain est à Upload).		Contient la phrase de passe qui protège le certificat à télécharger.	

Champ			Description	Valeurs
	Certificate Upload (disponible lorsque le champ Certificate Maintainest à Upload).		Télécharge un fichier de certificat PEM dans le commutateur. Le fichier doit contenir le certificat et la clé privée. Si le certificat et la clé privée se trouvent dans deux fichiers distincts, utiliser la commande cat de Linux pour les combiner en un seul fichier PEM : cat my.cert my.key > my.pem Il est recommandé d'utiliser un certificat RSA, car la plupart des versions récentes des navigateurs ne prennent plus en charge les certificats DSA (ex. Firefox v37 et Chrome v39).	Web Browser : Télécharge un certificat via un navigateur Web. URL : Télécharge un certificat via une URL.
		File Upload (disponible lorsque le champ Certificate Upload est à Web Browser).	Permet aux utilisateurs de sélectionner le fichier à télécharger.	

Champ			Description	Valeurs
		URL (disponible lorsque le champ Certificate Upload est à URL).	Contient l'URL.	Format de l'URL : [PROTOCOLE]://[NOM_UTILISATEUR]:[MOT_DE_PASSE]@[ADRESSE_IP_HÔTE]:[PORT] [CHEMIN_ACCÈS_FICHIER]. Les protocoles pris en charge sont HTTP, HTTPS, TFTP et FTP. Par exemple : tftp://10.10.10.10/new_image_path/new_image.dat http://username:password@10.10.10.10:80/new_image_path/new_image.dat Un nom de fichier valide est une chaîne de texte composée de lettres de l'alphabet (A-Za-z), de chiffres (0-9), de points (.), de traits d'union (-) et de traits de soulignement (_). La longueur maximale est de 63 caractères et le trait d'union ne doit pas être le premier caractère. Un nom de fichier qui ne contient que '.' n'est pas autorisé.
Certificate Status			Affiche l'état actuel du certificat du commutateur.	Switch secure HTTP certificate is presented : Lorsqu'un certificat valide est présent. Switch secure HTTP certificate is not presented : Si aucun certificat valide n'est présent ou si le certificat a été supprimé. Switch secure HTTP certificate is generating.... : Lorsque le certificat auto-signé est en train d'être généré (attendre 1 minute et rafraîchir la page pour voir les résultats).

10.3.3.4.1.2 Certificats

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

Tous les certificats permettent au serveur Web de chiffrer les renseignements transférés.

Seuls les certificats obtenus auprès d'une autorité de certification (AC) de confiance peuvent garantir l'authenticité au moyen d'une chaîne de confiance.

Il y a trois façons d'insérer un certificat :

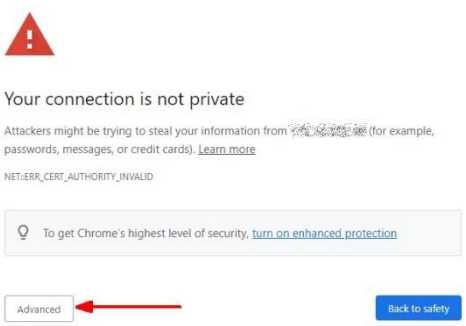
- **Générer un certificat auto-signé** – cette solution ne devrait être que temporaire. Il est sécurisé, mais pas sécuritaire. Les données sont chiffrées, mais ne sont pas fiables.
- **Télécharger un certificat à partir d'une URL**
- **Télécharger un certificat à partir du système de fichiers d'un utilisateur**

10.3.3.4.1.2.1 Générer un certificat auto-signé

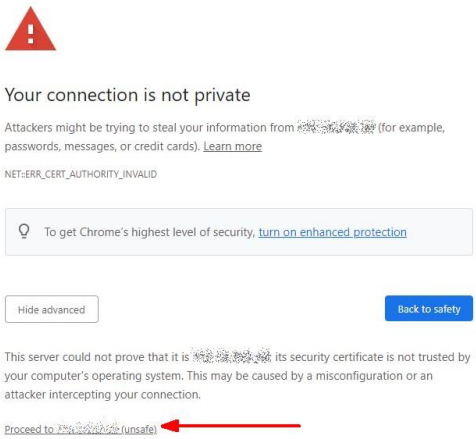
Un certificat auto-signé, qui ne devrait être utilisé que comme solution temporaire, permet de chiffrer la communication, mais ne peut pas certifier que le serveur est réellement ce qu'il prétend être.

NOTE : Le certificat auto-signé sera valide pour une période déterminée (ex. du 30 novembre 2021 à 00:00:01 au 30 novembre 2031 à 23:59:59).

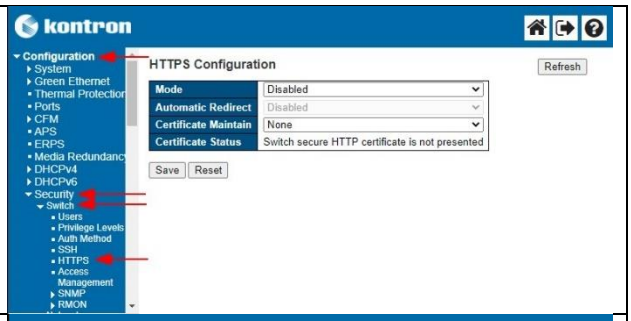
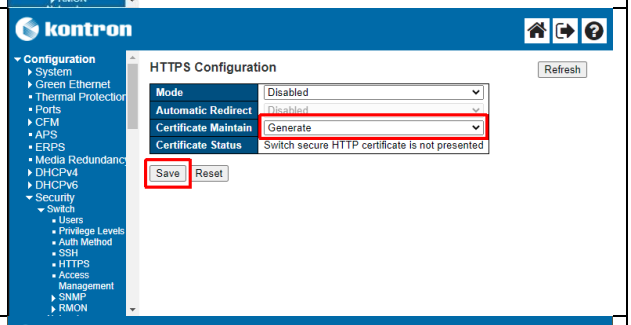
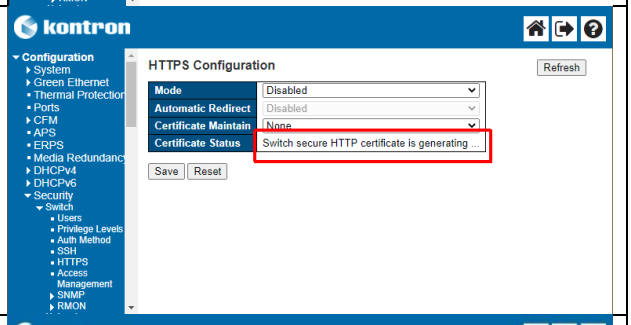
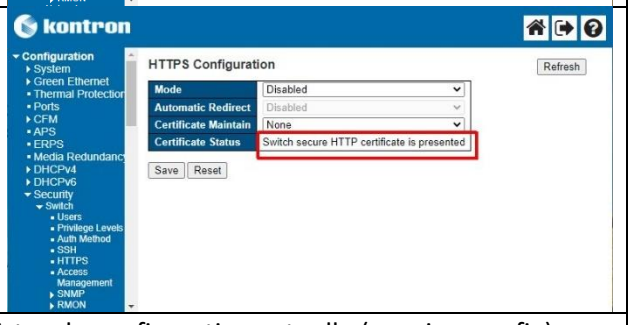
Si un certificat auto-signé est utilisé, le navigateur Web affichera un message d'avertissement avant que vous ne puissiez accéder à la page. Si c'est le cas, cliquer sur **Advanced**.



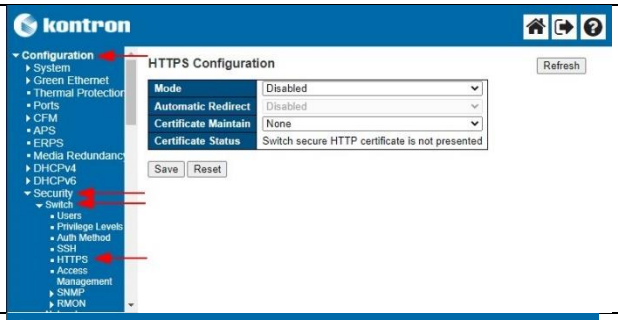
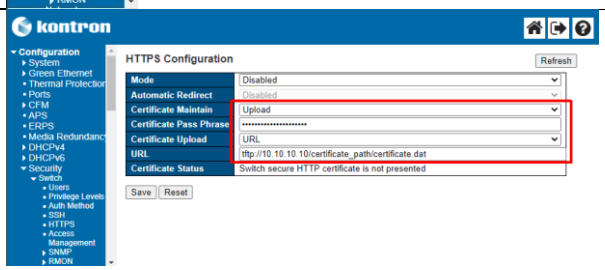
Cliquer ensuite sur le lien **Proceed to [ADRESSE_IP] (unsafe)**.



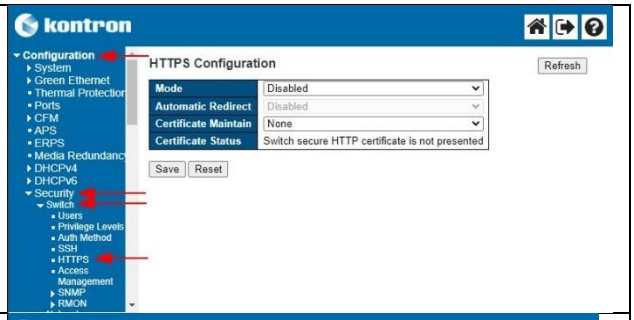
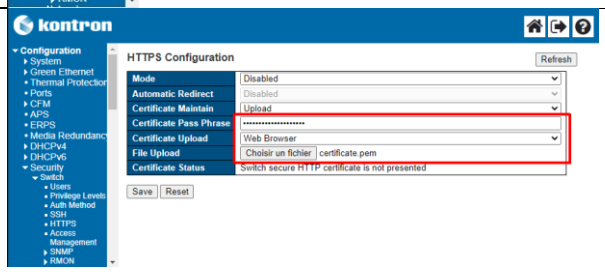
Dans l'interface utilisateur Web du commutateur, effectuer les étapes suivantes.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **Security**, **Switch**, puis **HTTPS**.	
Étape_2	Définir le champ **Certificat Maintain** à **Generate**.	
Étape_3	Cliquer sur **Save** pour confirmer.	
Étape_4	Le champ **Certificate Status** indiquera que le commutateur est en train de générer le certificat et se réactualisera automatiquement.	
Étape_5	Le champ **Certificate Status** indique que le certificat est présent.	
Étape_6	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

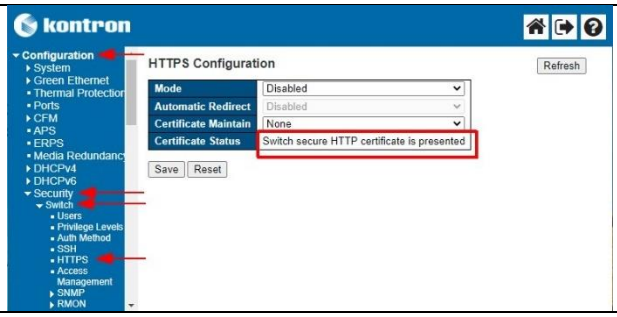
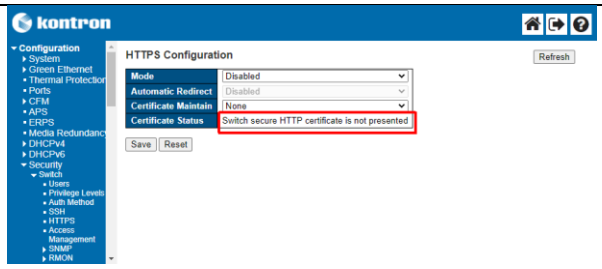
10.3.3.4.1.2.2 Télécharger un certificat à partir d'une URL

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **Security**, **Switch**, puis **HTTPS**.	
Étape_2	Définir le champ **Certificat Maintain** à **Upload**.	
Étape_3	Saisir la phrase de passe dans le champ **Certificate Pass Phrase**.	
Étape_4	Définir le champ **Certificate Upload** à **URL**.	
Étape_5	Saisir l'URL du certificat dans le champ **URL**.	
Étape_6	Cliquer sur **Save** pour confirmer.	
Étape_7	Le champ **Certificate Status** indique que le certificat est présent.	
Étape_8	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.4.1.2.3 Télécharger un certificat à partir du système de fichiers d'un utilisateur

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **Security**, **Switch**, puis **HTTPS**.	
Étape_2	Définir le champ **Certificat Maintain** à **Upload**.	
Étape_3	Saisir la phrase de passe dans le champ **Certificate Pass Phrase**.	
Étape_4	Définir le champ **Certificate Upload** à **Web Browser**.	
Étape_5	Dans le champ **File Upload**, cliquer sur **Choose a file** et naviguer afin de sélectionner le fichier souhaité.	
Étape_6	Cliquer sur **Save** pour confirmer.	
Étape_7	Le champ **Certificate Status** indique que le certificat est présent.	
Étape_8	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.4.1.2.4 Supprimer un certificat installé

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **Security**, **Switch**, puis **HTTPS**. S'assurer que le champ **Certificate Status** est à **Switch secure HTTP certificate is presented**.	
Étape_2	Définir le champ **Certificat Maintain** à **Delete**.	
Étape_3	Le champ **Certificate Status** indiquera ce qui suit : **Switch secure HTTP certificate is not presented**.	
Étape_4	Cliquer sur **Save** pour confirmer.	
Étape_5	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

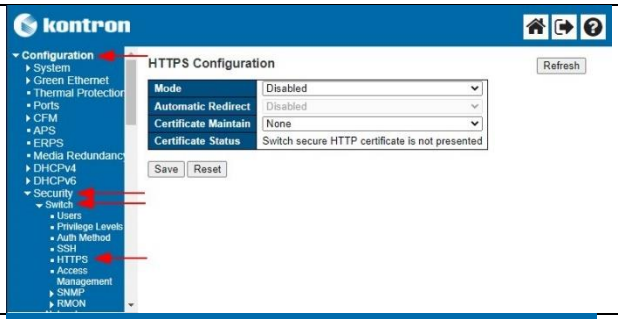
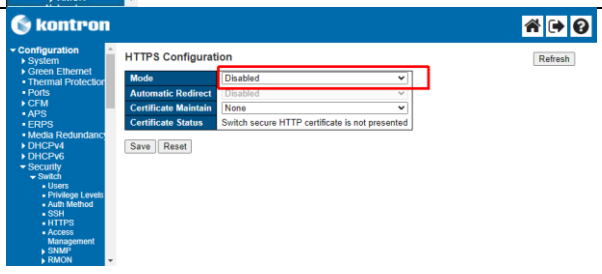
10.3.3.4.1.3 Configurer le protocole de l'interface

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

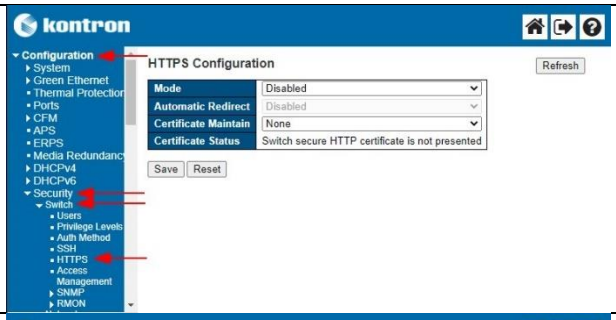
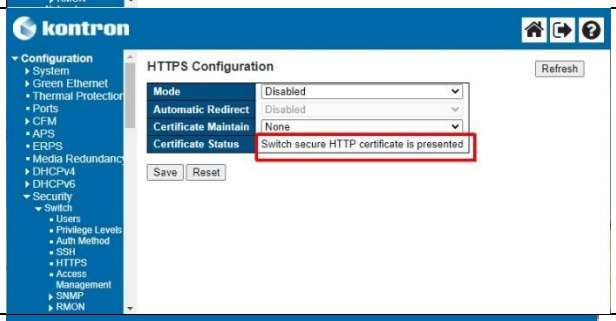
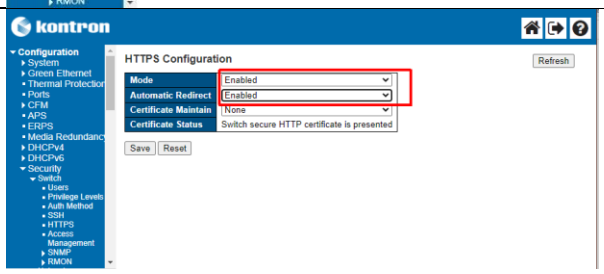
Il y a trois options pour configurer le protocole de l'interface :

- HTTP seulement
- HTTPS seulement
- HTTP et HTTPS

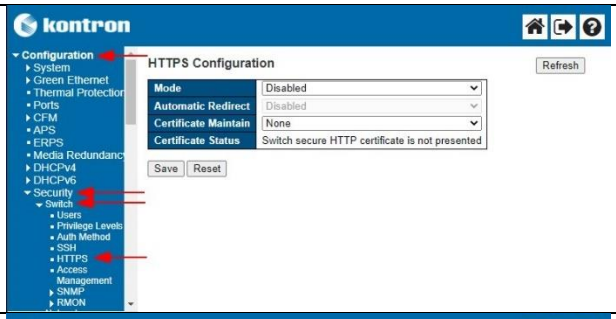
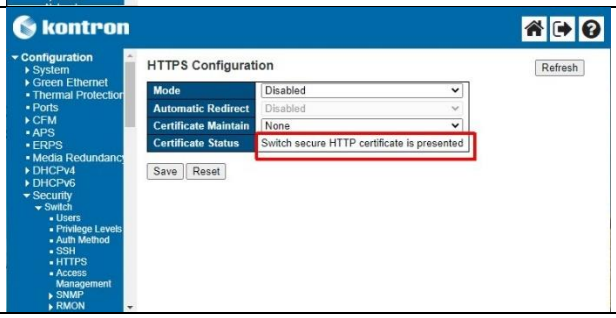
10.3.3.4.1.3.1 Configurer l'interface pour HTTP uniquement

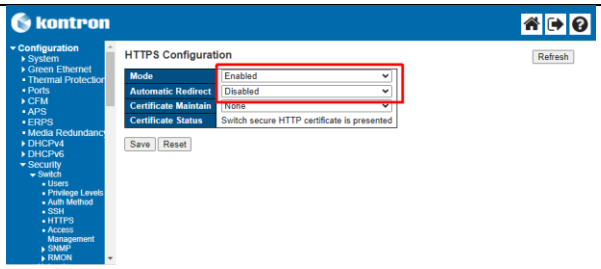
Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **Security**, **Switch**, puis **HTTPS**.	
Étape_2	Définir le champ **Mode** à **Disabled**.	
Étape_3	Cliquer sur **Save** pour confirmer.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.4.1.3.2 Configurer l'interface pour HTTPS uniquement

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **Security**, **Switch**, puis **HTTPS**.	
Étape_2	S’assurer que le champ **Certificate Status** est à **Switch secure HTTP certificate is presented**.	
Étape_3	Définir le champ **Mode** à **Enabled**.	
Étape_4	Définir le champ **Automatic Redirect** à **Enabled**.	
Étape_5	Cliquer sur **Save** pour confirmer.	
Étape_6	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.4.1.3.3 Configurer l'interface pour HTTP et HTTPS

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **Security**, **Switch**, puis **HTTPS**.	
Étape_2	S’assurer que le champ **Certificate Status** est à **Switch secure HTTP certificate is presented**.	
Étape_3	Définir le champ **Mode** à **Enabled**.	
Étape_4	Définir le champ **Automatic Redirect** sur **Disabled**.	

Étape_5	Cliquer sur **Save** pour confirmer.	
Étape_6	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.4.2 Configurer le support HTTPS en utilisant le CLI

Deux protocoles permettent d'accéder au serveur Web : HTTP et HTTPS. Ils sont indépendants et peuvent être utilisés simultanément. Le commutateur réseau peut donc fonctionner dans l'un des trois modes suivants :

- **HTTP seulement** – Tous les renseignements sont transférés en texte clair (même les mots de passe). **Non sécurisé!** Les communications se font sur le port 80.
- **HTTPS seulement** – Tous les renseignements sont transférés dans des paquets chiffrés. **La communication est sécurisée.** Les requêtes HTTP sont automatiquement traduites en requêtes HTTPS. Les communications se font sur le port 443. **Un certificat est nécessaire pour HTTPS.**
- **HTTP et HTTPS** – Les utilisateurs peuvent utiliser n'importe lequel des deux protocoles. **Il s'agit de l'état par défaut, mais un certificat est nécessaire pour HTTPS.**

Pour que le protocole sécurisé HTTPS fonctionne, un certificat doit être installé. Voir la section Certificats ci-dessous.

10.3.3.4.2.1 Afficher les états HTTP et HTTPS

Voir Accéder au NOS pour les instructions d'accès.

Pour connaître les états des différentes variables HTTP sécurisées, deux commandes peuvent être utilisées : **show ip http** (en mode normal) ou **do show ip http** (en mode configuration).

Étape_1	InviteCLI_NOSLocal:~# **show ip http**	NOS00A0A5E01CF4# show ip http Switch secure HTTP web server is disabled Switch secure HTTP web redirection is disabled Switch secure HTTP certificate is not presented

Champ	Description	Valeur
Switch secure HTTP web server is	Indique l'état du **serveur Web HTTP sécurisé du commutateur**. Lorsque l'état est **Enabled**, les communications HTTPS sécurisées via le port 443 sont disponibles. **NOTE :** Pour que l'état soit **Enabled**, un certificat **doit** être présent.	Enabled Disabled
Switch secure HTTP web redirection is	Lorsque l'état est **Enabled**, les communications HTTP sont redirigées vers le **serveur Web HTTP sécurisé du commutateur**. Cela signifie que le serveur Web HTTP n'est plus utilisé. **NOTE :** Pour que l'état soit **Enabled**, le paramètre **Switch secure HTTP web server** doit être défini à **Enabled** au préalable.	Enabled Disabled
Switch secure HTTP certificate is	Indique si un certificat est installé dans le système. La valeur **Presented** signifie qu'un certificat est installé et peut être utilisé pour le chiffrement HTTPS.	Presented Not presented

10.3.3.4.2.2 Certificats

Voir Accéder au NOS pour les instructions d'accès. Tous les certificats permettent au serveur Web de chiffrer les renseignements transférés.

Seuls les certificats obtenus auprès d'une autorité de certification (AC) de confiance peuvent garantir l'authenticité au moyen d'une chaîne de confiance.

Il y a trois façons d'insérer un certificat :

- **Générer un certificat auto-signé** – cette solution ne devrait être que temporaire. Il est sécurisé, mais pas sécuritaire. Les données sont chiffrées, mais ne sont pas fiables.
- **Télécharger un certificat à partir d'une URL**
- **Télécharger un certificat à partir du système de fichiers d'un utilisateur**

10.3.3.4.2.2.1 Afficher les commandes disponibles

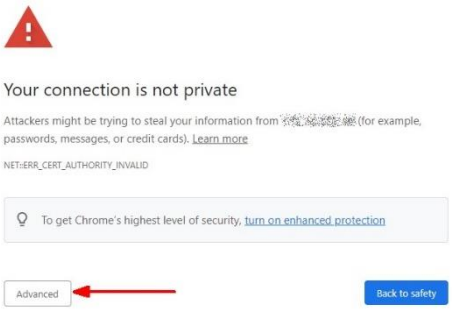
Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	NOS00A0A5E01CF4# configure terminal NOS00A0A5E01CF4(config)# ip http secure-certificate ? delete Delete the current certificate generate Generate a new self-signed RSA certificate upload Upload a certificate PEM file
Étape_2	Afficher les commandes disponibles. InviteCLI_NOSLocal:~(config)# **ip http secure-certificate ?**	

10.3.3.4.2.2.2 Générer un certificat auto-signé

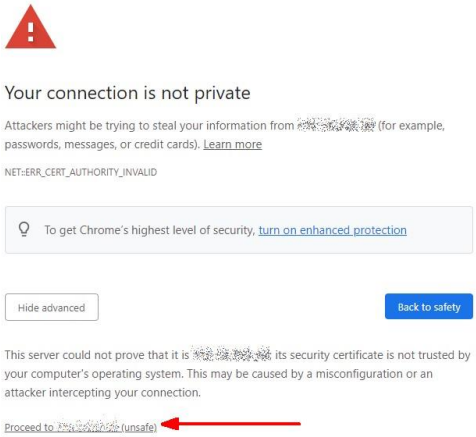
Un certificat auto-signé, qui ne devrait être utilisé que comme solution temporaire, permet de chiffrer la communication, mais ne peut pas certifier que le serveur est réellement ce qu'il prétend être.

NOTE : Le certificat auto-signé sera valide pour une période déterminée (ex. du 30 novembre 2021 à 00:00:01 au 30 novembre 2031 à 23:59:59).

Si un certificat auto-signé est utilisé, le navigateur Web affichera un message d'avertissement avant que vous ne puissiez accéder à la page. Si c'est le cas, cliquer sur **Advanced**.



Cliquer ensuite sur le lien **Proceed to [ADRESSE_IP] (unsafe)**.



Dans le CLI du NOS :

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	NOS00A0A5E01CF4# configure terminal NOS00A0A5E01CF4(config)# ip http secure-certificate generate
Étape_2	Générer un certificat. InviteCLI_NOSLocal:~(config)# **ip http secure-certificate generate**	
Étape_3	S'assurer que le certificat et le serveur Web HTTP sont correctement configurés. InviteCLI_NOSLocal:~# **do show ip http** **NOTE :** La génération d'un certificat peut prendre quelques secondes. S'il est toujours en cours de génération lors de la vérification de l'état, le CLI indiquera qu'il est en cours de génération.	NOS00A0A5E01CF4(config)# do show ip http Switch secure HTTP web server is disabled Switch secure HTTP web redirection is disabled Switch secure HTTP certificate is generating ...
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.4.2.2.3 Télécharger un certificat à partir d'une URL

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**
Étape_2	Télécharger le certificat. InviteCLI_NOSLocal:~(config)# **ip http secure-certificate upload [PROTOCOLE]://[NOM_UTILISATEUR]: [MOT_DE_PASSE]@ [ADRESSE_IP_HÔTE]: [PORT][CHEMIN_ACCÈS_FICHIER]** NOS00A0A5E01CF4# configure terminal NOS00A0A5E01CF4(config)# ip http secure-certificate upload tftp://10.10.10.10/certificate.pem
Étape_3	S'assurer que le certificat et le serveur Web HTTP sont correctement configurés. InviteCLI_NOSLocal:~# **do show ip http** **NOTE :** La génération d'un certificat peut prendre quelques secondes. S'il est toujours en cours de génération lors de la vérification de l'état, le CLI indiquera qu'il est en cours de génération. NOS00A0A5E01CF4(config)# do show ip http Switch secure HTTP web server is disabled Switch secure HTTP web redirection is disabled Switch secure HTTP certificate is generating ...
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).

10.3.3.4.2.2.4 Supprimer un certificat installé

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	NOS00A0A5E01CF4# configure terminal NOS00A0A5E01CF4(config)# ip http secure-certificate delete NOS00A0A5E01CF4(config)#
Étape_2	InviteCLI_NOSLocal:~(config)# **ip http secure-certificate delete**	
Étape_3	S'assurer que le certificat et le serveur Web HTTP sont correctement configurés. InviteCLI_NOSLocal:~# **do show ip http**	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.4.2.3 Configurer le protocole de l'interface

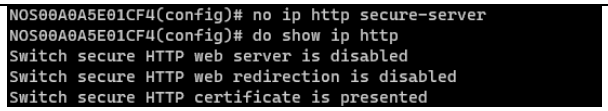
Voir Accéder au NOS pour les instructions d'accès.

Il y a trois options pour configurer le protocole de l'interface :

- HTTP seulement
- HTTPS seulement
- HTTP et HTTPS

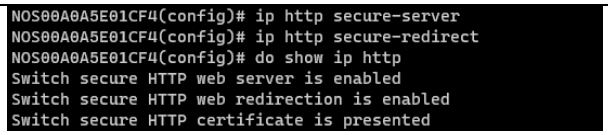
10.3.3.4.2.3.1 Configurer l'interface pour HTTP uniquement

Si l'interface est configurée pour HTTP seulement, le serveur web HTTP sécurisé du commutateur HTTPS sera désactivé, de même que la redirection Web HTTP sécurisée du commutateur.

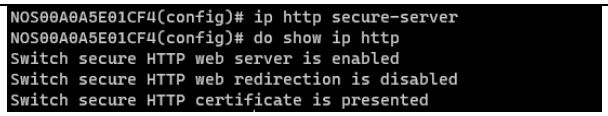
Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	
Étape_2	InviteCLI_NOSLocal:~(config)# **no ip http secure-server**	
Étape_3	S'assurer que le certificat et le serveur Web HTTP sont correctement configurés. InviteCLI_NOSLocal:~(config) # **do show ip http**	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.4.2.3.2 Configurer l'interface pour HTTPS uniquement

Pour configurer l'interface pour HTTPS seulement, le serveur HTTPS doit être activé et la redirection doit également être activée. Cela désactivera le serveur HTTP.

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	
Étape_2	Configurer l'interface pour HTTPS. InviteCLI_NOSLocal:~(config)# **ip http secure-server**	
Étape_3	Activer la redirection. InviteCLI_NOSLocal:~(config)# **ip http secure-redirect**	
Étape_4	S'assurer que le certificat et le serveur Web HTTP sont correctement configurés. InviteCLI_NOSLocal: ~(config) # **do show ip http**	
Étape_5	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.4.2.3.3 Configurer l'interface pour HTTP et HTTPS

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	
Étape_2	InviteCLI_NOSLocal:~(config)# **ip http secure-server**	
Étape_3	S'assurer que le certificat et le serveur Web HTTP sont correctement configurés. InviteCLI_NOSLocal: ~(config) # **do show ip http**	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.5 Configurer le service DNS

NOTE : Seuls les protocoles basés sur IPv4 ont été testés. Par conséquent, aucun protocole IPv6 n'a été documenté.

10.3.3.5.1 Configurer le nom de domaine

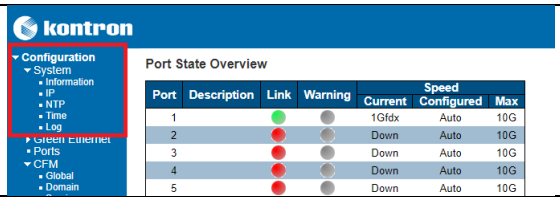
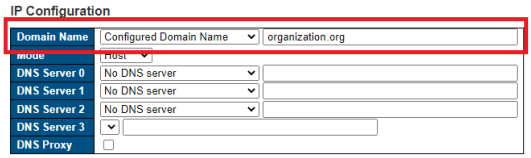
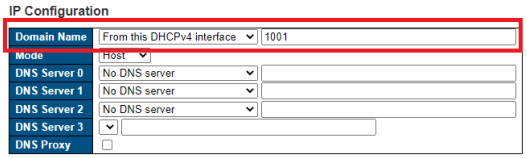
10.3.3.5.1.1 Configurer le nom de domaine en utilisant le CLI

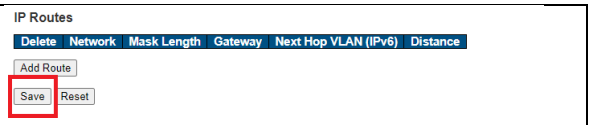
Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	`# configure terminal`

Étape_2	Trois méthodes de configuration du nom de domaine sont prises en charge. Un serveur peut être configuré à partir d'un nom de domaine local, de n'importe quelle interface VLAN compatible DHCPv4 ou d'une interface VLAN particulière compatible DHCPv4. Les exemples suivants couvrent toutes les méthodes.
	InviteCLI_NOSLocal:~# **ip domain name [NOM_DOMAINE]**
	InviteCLI_NOSLocal:~# **ip domain name dhcp ipv4**
	InviteCLI_NOSLocal:~# **ip domain name dhcp ipv4 interface vlan [ID_VLAN]**
	Pour désactiver le nom de domaine, utiliser le préfixe **no** avant la commande **domain name**.
	
	InviteCLI_NOSLocal:~# **no ip domain name**
		`(config)# ip domain name organization.org`
		`(config)# ip domain name dhcp ipv4`
		`(config)# ip domain name dhcp ipv4 interface vlan 1001`

Étape_3	Vérifier que la configuration a été effectuée avec succès. InviteCLI_NOSLocal:~# **do show ip domain**	`(config)# do show ip domain` `Current domain name is organization.org (managed by DHCPv4).`
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

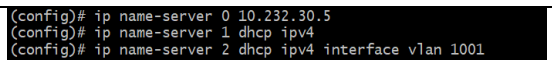
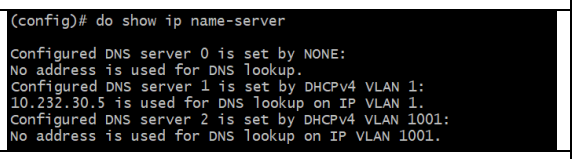
10.3.3.5.1.2 Configurer le nom de domaine en utilisant l'interface utilisateur Web

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **System**, puis **IP**.	
Étape_2	Dans la section **IP Configuration**, sélectionner la méthode de configuration dans le menu déroulant du champ **Domain Name**. Ensuite, si nécessaire, configurer la valeur dans la zone d'entrée adjacente. Les méthodes de configuration sont énumérées ci-dessous : • **No Domain Name** : Aucun nom de domaine ne sera utilisé. Aucune valeur n'est requise dans la zone d'entrée. • **Configured Domain Name** : Permet d'indiquer explicitement le nom du domaine local dans la zone d'entrée. S'assurer que le nom de domaine configuré correspond au nom de domaine assigné à votre organisation. • **From any DHCPv4 interfaces** : Le premier nom de domaine proposé par un bail DHCPv4 à une interface VLAN compatible DHCPv4 sera utilisé. Aucune valeur n'est requise dans la zone d'entrée. • **From this DHCPv4 interface** : Permet de spécifier l'interface VLAN compatible DHCPv4 privilégiée pour obtenir un nom de domaine.	Exemple pour la méthode **Configured Domain Name** :  Exemple pour la méthode **From this DHCPv4 Interface** : 

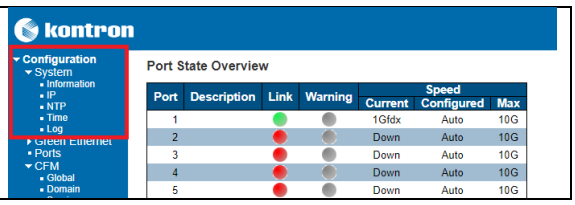
Étape_3	Cliquer sur le bouton **Save**.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

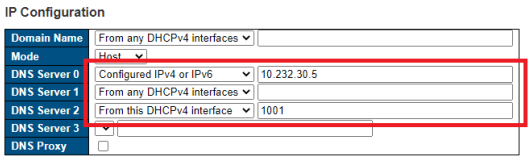
10.3.3.5.2 Configurer un serveur DNS

10.3.3.5.2.1 Configurer un serveur DNS en utilisant le CLI

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	
Étape_2	Jusqu'à 3 serveurs DNS peuvent être configurés dans le NOS. Les ID des serveurs DNS peuvent être compris entre 0 et 2. Trois méthodes sont prises en charge pour la configuration d'un serveur DNS. Un serveur peut être configuré à partir d'une adresse unicast IPv4 du serveur DNS, de n'importe quelle interface VLAN compatible DHCPv4 ou d'une interface VLAN particulière compatible DHCPv4. Les exemples suivants couvrent toutes les méthodes. InviteCLI_NOSLocal:~# **ip name-server [ID_SERVEUR_DNS] [ADRESSE_IP_SERVEUR_DNS]** InviteCLI_NOSLocal:~# **ip name-server [ID_SERVEUR_DNS] dhcp ipv4** InviteCLI_NOSLocal:~# **ip name-server [ID_SERVEUR_DNS] dhcp ipv4 interface vlan [ID_VLAN]** Pour désactiver un serveur DNS, utiliser le préfixe **no** avant la commande **name-server**. InviteCLI_NOSLocal:~# **no ip name-server [ID_SERVEUR_DNS]**	
Étape_3	Vérifier que la configuration a été effectuée avec succès. InviteCLI_NOSLocal:~# **do show ip name-server**	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.5.2.2 Configurer un serveur DNS en utilisant l'interface utilisateur Web

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **System**, puis **IP**.	

Étape_2	Dans la section **IP Configuration**, sélectionner la méthode de configuration du serveur DNS dans le menu déroulant. Ensuite, si nécessaire, configurer la valeur dans la zone d'entrée adjacente. Les méthodes de configuration sont énumérées ci-dessous : • **No DNS server** : Aucun serveur DNS ne sera utilisé. • **Configured IPv4** : Permet d'indiquer explicitement l'adresse unicast IPv4 du serveur DNS en notation décimale pointée dans la zone d'entrée. S'assurer que le serveur DNS configuré est accessible. • **From any DHCPv4 interfaces** : Le premier serveur DNS proposé par un bail DHCPv4 à une interface compatible DHCPv4 sera utilisé. • **From this DHCPv4 interface** : Permet de spécifier l'interface compatible DHCPv4 privilégiée pour obtenir un serveur DNS. Saisir un ID de VLAN dans la zone d'entrée.	
Étape_3	Cliquer sur le bouton **Save**.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.5.3 Configurer le proxy DNS

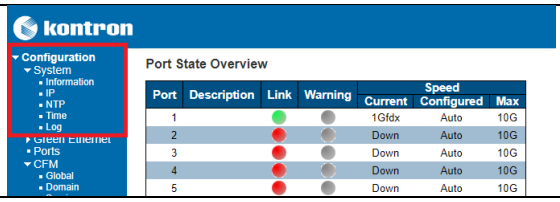
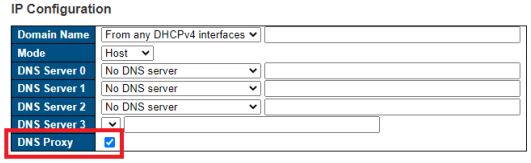
10.3.3.5.3.1 Configurer le proxy DNS en utilisant l'interface utilisateur Web

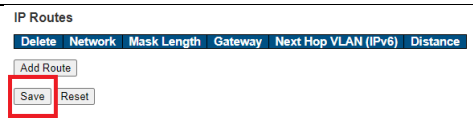
Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	`# configure terminal`

Étape_2	Pour activer le proxy DNS, utiliser la commande suivante.
	InviteCLI_NOSLocal:~(config)# **ip dns proxy**
	Pour désactiver le proxy DNS, utiliser la même commande avec le préfixe **no**.
	InviteCLI_NOSLocal:~(config)# **no ip dns proxy**
		`(config)# ip dns proxy`
		`(config)#`
		
		`(config)# no ip dns proxy`
		`(config)#`

Étape_3	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.3.3.5.3.2 Activer le proxy DNS en utilisant l'interface utilisateur Web

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **System**, puis **IP**.	
Étape_2	Dans la section **IP Configuration**, activer ou désactiver le proxy DNS en cochant la case **DNS Proxy**.	

Étape_3	Cliquer sur le bouton **Save**.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.4 Configuration des services du BMC

10.4.1 Configurer le service SNMP du BMC

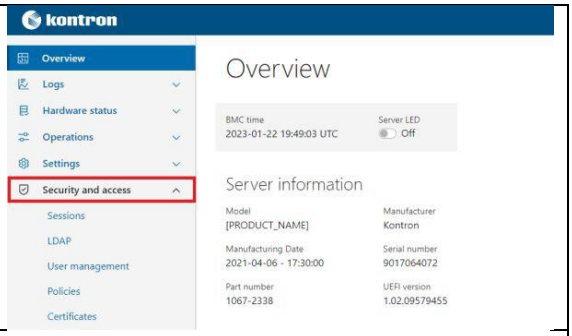
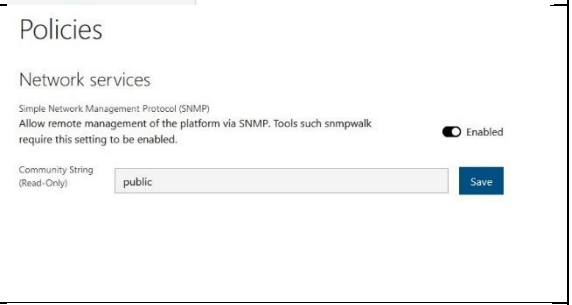
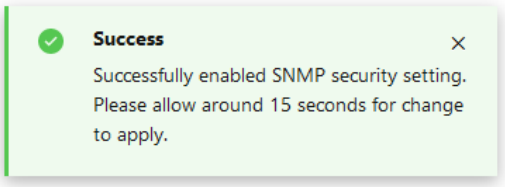
10.4.1.1 Configurer la gestion à distance SNMP

Le service SNMP du BMC peut être configuré :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish

10.4.1.1.1 Configurer la gestion à distance SNMP en utilisant l'interface utilisateur Web du BMC

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

Étape_1	Dans le menu de gauche, sélectionner **Security and access**, puis **Policies**.	
Étape_2	Activer ou désactiver la gestion à distance SNMP avec le bouton radio.	
Étape_3	Si la gestion à distance SNMP a été activée, saisir un nom unique dans le champ **Community String**.	
Étape_4	Cliquer sur le bouton **Save**.	
Étape_5	Un message de réussite doit s'afficher lorsque la configuration est réussie.	

10.4.1.1.2 Configurer la gestion à distance SNMP en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur.

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

Étape_1	Activer ou désactiver la gestion à distance SNMP avec la commande suivante. Les valeurs possibles pour [ENABLED] sont les suivantes : • true • false InviteSE_OrdinateurDistant:~$ **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/Managers/bmc/NetworkProtocol –header 'Content-Type: application/json' --data '{"SNMP":{"ProtocolEnabled":[ENABLED]}}' | jq**
	`curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/NetworkProtocol --header 'Content-Type: application/json' --data '{"SNMP":{"ProtocolEnabled":true}}' | jq`
Étape_2	Configurer le paramètre de la chaîne de communauté (Community String) de la gestion à distance SNMP. S'assurer que la variable [STRING] est une chaîne de communauté unique. InviteSE_OrdinateurDistant:~$ **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/Managers/bmc/NetworkProtocol –header 'Content-Type: application/json' --data '{"CommunityString":"[STRING]"}' | jq**
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/NetworkProtocol --header 'Content-Type: application/json' --data '{"CommunityString":"communitystring"}' | jq`

10.4.2 Configurer les abonnements aux événements du BMC

Section pertinente :

Configurer le service SNMP du BMC

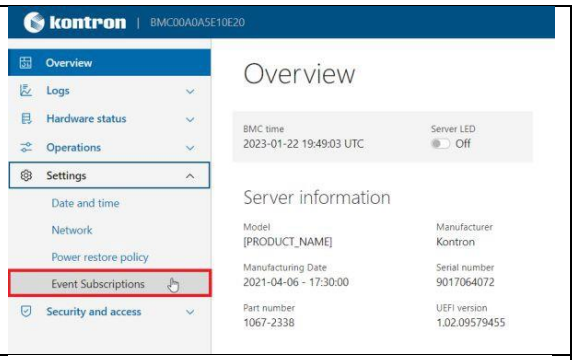
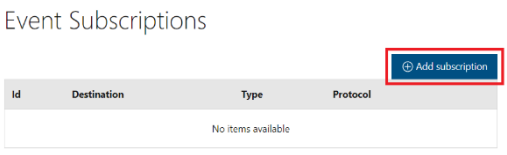
10.4.2.1 Configurer les traps SNMP

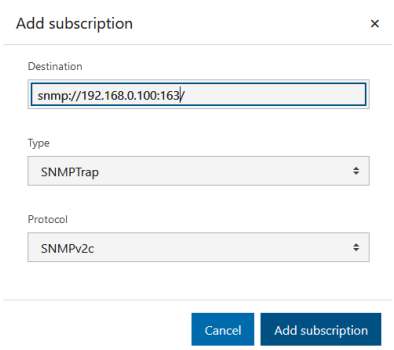
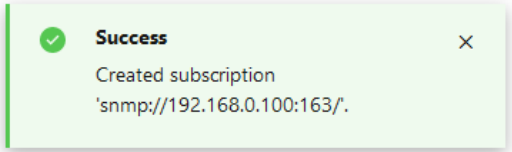
Les traps SNMP du BMC peuvent être configurés :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish

10.4.2.1.1 Configurer les traps SNMP en utilisant l'interface utilisateur Web du BMC

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

Étape_1	Dans le menu de gauche, sélectionner **Settings**, puis **Event Subscriptions**.	
Étape_2	Cliquer sur le bouton **Add subscription**.	

Étape_3	Dans le menu **Add subscription**, saisir l'adresse de destination dans le champ **Destination**. L'adresse de destination doit être formatée comme suit : **[PROTOCOLE]://[ADRESSE]:[PORT]/** **NOTE :** La barre oblique (/) à la fin de l'adresse de destination est obligatoire.	
Étape_4	Sélectionner **SNMPTrap** dans le menu déroulant **Type**.	
Étape_5	Sélectionner **SNMPv2c** dans le menu déroulant **Protocol**.	
Étape_6	Un message de succès devrait apparaître dans le coin supérieur droit lorsque la configuration est effectuée avec succès.	

10.4.2.1.2 Configurer les traps SNMP en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Ajouter un nouvel abonnement aux traps SNMP avec la commande suivante. InviteSE_OrdinateurDistant:~$ **curl -k -s --request POST –url [URL_RACINE]/redfish/v1/EventService/Subscriptions –header 'Content-Type: application/json' --data '{"Destination": "snmp://[SERVEUR]:[PORT]", "SubscriptionType": "SNMPTrap", "Protocol": "SNMPv2c"}' | jq**

```
curl -k -s --request POST --url https://admin:ready2go@172.16.182.31/redfish/v1/EventService/Sub
scriptions --header 'Content-Type: application/json' --data '{"Destination": "snmp://192.168.0.1
:163","SubscriptionType": "SNMPTrap","Protocol": "SNMPv2c"}' | jq
{
 "@Message.ExtendedInfo": [
  {
   "@odata.type": "#Message.v1_1_1.Message",
   "Message": "The resource has been created successfully",
   "MessageArgs": [],
   "MessageId": "Base.1.8.1.Created",
   "MessageSeverity": "OK",
   "Resolution": "None"
  }
 ]
}
```

10.5 Configuration du commutateur

Sections pertinentes :

Accéder au NOS

Accéder au système d'exploitation d'un serveur

Configuration et gestion des utilisateurs

Les modifications apportées à la configuration du NOS ne sont pas persistantes après le redémarrage du NOS. Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config.

Dans l'interface utilisateur Web du NOS :

Sélectionner **Maintenance**, **Configuration**, puis **Save startup-config**. Cliquer sur **Save Configuration** pour confirmer le changement.

Dans le CLI du NOS :

InviteCLI_NOSLocal:~(config-if)# **end**

InviteCLI_NOSLocal:~# **copy running-config startup-config**

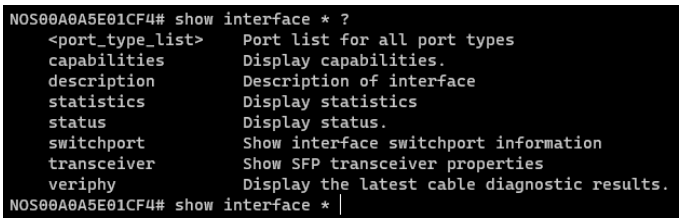
10.5.1 Outils d'aide

10.5.1.1 Aide de l'interface utilisateur Web du commutateur

Le menu d'aide de l'interface utilisateur Web du commutateur est exhaustif. Il devrait être utilisé pour configurer le système.

10.5.1.2 Aide du CLI du commutateur

Le CLI du commutateur contient une fonction d'aide contextuelle. Le symbole **?** permet d'afficher les prochains paramètres ou commandes possibles et leur description. Presque toutes les commandes de configuration ont une version « no » correspondante. La version « no » est syntaxiquement similaire (mais pas nécessairement identique) à la commande de configuration. Cependant, elle réinitialise les paramètres aux valeurs par défaut pour l'élément configurable ou désactive complètement l'élément.



10.5.2 Configurer le mappage des ports

10.5.2.1 Mappage des ports du commutateur

Le tableau suivant liste les ports physiques du commutateur Ethernet d'une plateforme ME1310 équipée du module d'E/S approprié. Il est important de noter que, dans le NOS, les ports physiques sont une catégorie d'interfaces. L'appellation du port est utilisée dans les commandes CLI (variable [**ID_INTERFACE**]) pour surveiller ou configurer le port correspondant. Comme montré ci-dessous, le mappage des ports du commutateur est configurable. Les ports du tableau ci-dessous seront actifs ou non selon le mappage des ports sélectionné.

Appellation du port dans le NOS	Composant connecté	Bus PCIe du serveur intégré
Ethernet 1/1	SFP Sw 1	S. O.
Ethernet 1/2	SFP Sw 2	S. O.
Ethernet 1/3	SFP Sw 3	S. O.
Ethernet 1/4	SFP Sw 4	S. O.
Ethernet 1/5	SFP Sw 5	S. O.
Ethernet 1/6	SFP Sw 6	S. O.
Ethernet 1/7	SFP Sw 7	S. O.
Ethernet 1/8	SFP Sw 8	S. O.
Ethernet 1/9	SFP Sw 9	S. O.
Ethernet 1/10	SFP Sw 10	S. O.

Appellation du port dans le NOS	Composant connecté	Bus PCIe du serveur intégré
Ethernet 1/11	SFP Sw 11	S. O.
Ethernet 1/12	SFP Sw 12	S. O.
Ethernet 1/13	eno1 *	00:89:00.3
Ethernet 1/14	eno2 *	00:89:00.2
Ethernet 1/15	eno3 *	00:89:00.1
Ethernet 1/16	eno4 *	00:89:00.0

* eno1-4 est la nomenclature Linux typique telle qu'elle apparaît dans le système d'exploitation du serveur intégré.

10.5.2.2 Choisir une configuration pour le mappage des ports

Contrairement à d'autres configurations, une modification du mappage des ports ne peut pas être appliquée immédiatement et nécessite de redémarrer le commutateur. Ainsi, ce type de modification n'a aucun impact sur la configuration actuelle (running-config), et il n'est donc pas nécessaire de copier la configuration actuelle dans la configuration de démarrage (copy running-config to startup-config) pour rendre le changement permanent.

Pour la même raison, le rechargement de la configuration par défaut du commutateur n'affecte pas le choix de la configuration pour le mappage des ports, car les paramètres par défaut sont rechargés dans la configuration courante (running-config) et sont volatils jusqu'à ce qu'ils soient copiés dans la configuration de démarrage (startup-config). La configuration par défaut pour le mappage des ports doit être sélectionnée manuellement en exécutant la commande **portmap cfg 0** en mode configuration, puis en redémarrant le commutateur.

10.5.2.2.1 Description des configurations disponibles pour le mappage des ports

Mappage des ports	Ports SFP actifs sur le panneau avant		Ports internes du serveur
0	12x SFP+ 10GbE	SFP1-12	4x 10GBASE-KR
1	7x SFP+ 10GbE	SFP1-7	4x 10GBASE-KR
	2x SFP28 25GbE	SFP9-10	
2	2x SFP+ 10GbE	SFP1-2	4x 10GBASE-KR
	4x SFP28 25GbE	SFP9-12	
3	4x SFP28 25GbE	SFP9-12	4x 25GBASE-KR

Les ports SFP qui ne figurent pas dans la liste des ports actifs ne peuvent pas être utilisés ni configurés. Les commandes de configuration CLI répondront par un message explicatif. L'interface utilisateur Web ne proposera pas les sélections non disponibles.

Le mappage des ports peut seulement être configuré en utilisant le CLI.

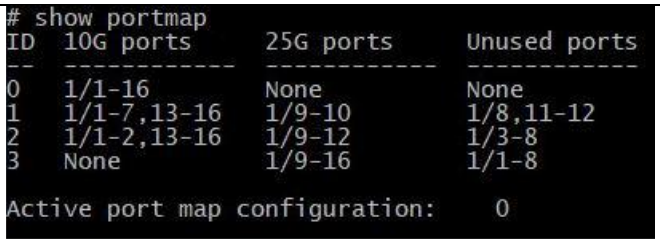
Accéder au CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

10.5.2.2.2 Lister les configurations disponibles pour le mappage des ports

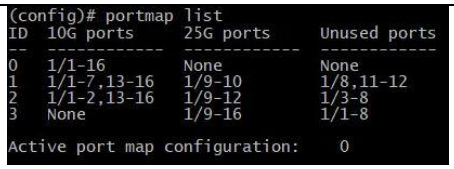
Diverses configurations sont disponibles pour le mappage des ports, permettant des combinaisons de ports 10GbE et 25GbE sans dépasser la limite totale d'allocation de la bande passante du commutateur.

Deux méthodes peuvent être utilisées pour lister les configurations disponibles et rapporter celle qui est active :

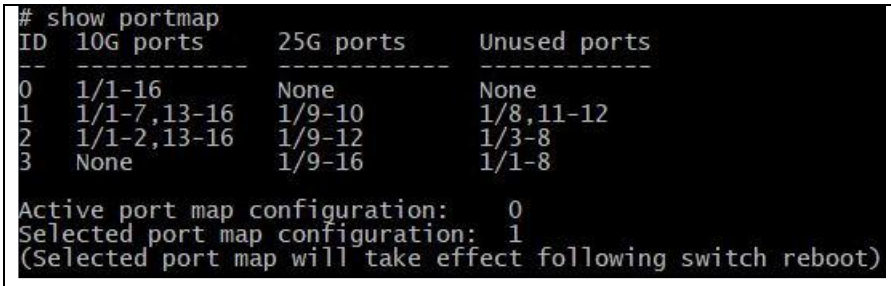
À partir du mode EXEC

Étape_1	Afficher les options pour la configuration du mappage des ports et la configuration active. InviteCLI_NOSLocal:~# **show portmap**	

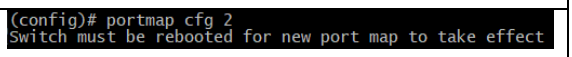
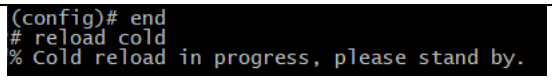
À partir du mode de configuration

Étape_1	Accéder au menu de configuration. InviteCLI_NOSLocal:~# **configure terminal**	
Étape_2	Afficher les options pour la configuration du mappage des ports et la configuration active. InviteCLI_NOSLocal:~(config)# **portmap list** **NOTE :** ID est la valeur du paramètre [**ID_PORTMAP**] utilisé dans les commandes.	

Pour les deux méthodes, si une configuration est choisie pour le mappage des ports et qu'elle diffère de la configuration active, mais qu'elle n'est pas encore appliquée parce que le commutateur n'a pas encore été redémarré, le CLI l'indiquera comme suit :



10.5.2.2.3 Choisir une configuration pour le mappage des ports

Étape_1	Accéder au menu de configuration. InviteCLI_NOSLocal:~# **configure terminal**	
Étape_2	Utiliser l'ID de la liste des configurations disponibles pour choisir la configuration souhaitée. InviteCLI_NOSLocal:~(config)# **portmap cfg [ID_PORTMAP]**	
Étape_3	Quitter le mode de configuration et redémarrer le commutateur pour que la nouvelle configuration soit effective. InviteCLI_NOSLocal:~(config)# **end** InviteCLI_NOSLocal:~# **reload cold**	

10.5.3 Vérifier l'état des liaisons

L'état des liaisons peut être vérifié :

- En utilisant le CLI
- En utilisant l'interface utilisateur Web du commutateur

10.5.3.1 Vérifier l'état des liaisons en utilisant le CLI

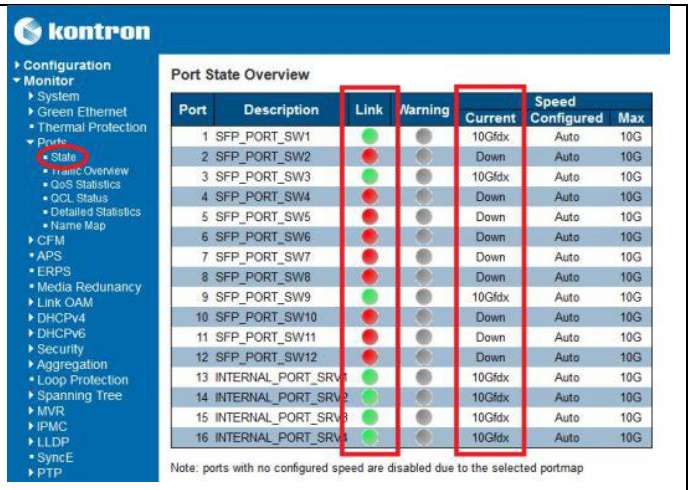
Accéder au CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

Étape_1	Vérifier l'état de toutes les liaisons. InviteCLI_NOSLocal:~# **show interface * status**

```
NOS00A0A5E24F56# show interface  * status
Interface  Mode     Speed   Max  Aneg       Media Type SFP Family   Link    Operational Warnings
---------- -------- ------- ---- ---------- ---------- ------------ ------- --------------------
Eth 1/1    Enabled  Auto    10G  No         SFP        10G Optical  10Gfdx
Eth 1/2    Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/3    Enabled  Auto    10G  No         SFP        10G Optical  10Gfdx
Eth 1/4    Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/5    Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/6    Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/7    Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/8    Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/9    Enabled  Auto    10G  No         SFP        10G DAC      10Gfdx
Eth 1/10   Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/11   Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/12   Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/13   Enabled  Auto    10G  Yes (Cl73) SFP        10G CuBP     10Gfdx
Eth 1/14   Enabled  Auto    10G  Yes (Cl73) SFP        10G CuBP     10Gfdx
Eth 1/15   Enabled  Auto    10G  Yes (Cl73) SFP        10G CuBP     10Gfdx
Eth 1/16   Enabled  Auto    10G  Yes (Cl73) SFP        10G CuBP     10Gfdx
```

10.5.3.2 Vérifier l'état des liaisons en utilisant l'interface utilisateur Web

Accéder à l'interface utilisateur Web du NOS. Voir Accéder au NOS pour les instructions d'accès.

Étape_1	Dans le menu de gauche, sélectionner **Monitor**, **Ports**, puis **State**. **NOTE :** Cette page est la page d'accueil par défaut lors de l'accès à l'interface utilisateur Web du NOS.	

10.5.4 Activer un port du commutateur

Les ports du commutateur peuvent être activés :

- En utilisant le CLI
- En utilisant l'interface utilisateur Web du commutateur

10.5.4.1 Activer un port du commutateur en utilisant le CLI

Accéder au CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Accéder au mode de configuration de l'interface.
	InviteCLI_NOSLocal:~# **configure terminal**
	InviteCLI_NOSLocal:~(config)# **interface [ID_INTERFACE]**
		`# configure terminal`
		`(config)# interface Ethernet 1/6`
		`(config-if)#`

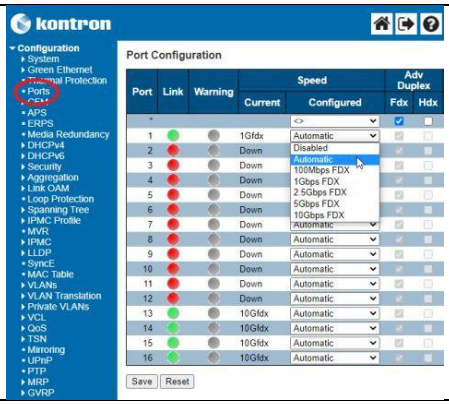
Étape_2	Activer l'interface. InviteCLI_NOSLocal:~(config-if)# **no shutdown**	`(config-if)# no shutdown`

Étape_3	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).

10.5.4.2 Activer un port du commutateur en utilisant l'interface utilisateur Web

Accéder à l'interface utilisateur Web du NOS. Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, puis **Ports**.	
Étape_2	Activer un port du commutateur en sélectionnant sa vitesse.	
Étape_3	Cliquer sur le bouton **Save** pour confirmer.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.5.5 Désactiver un port du commutateur

Les ports du commutateur peuvent être désactivés :

- En utilisant le CLI
- En utilisant l'interface utilisateur Web du commutateur

10.5.5.1 Désactiver un port du commutateur en utilisant le CLI

Accéder au CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Accéder au mode de configuration de l'interface.
	InviteCLI_NOSLocal:~# **configure terminal**
	InviteCLI_NOSLocal:~(config)# **interface [ID_INTERFACE]**
		`# configure terminal`
		`(config)# interface Ethernet 1/6`
		`(config-if)#`

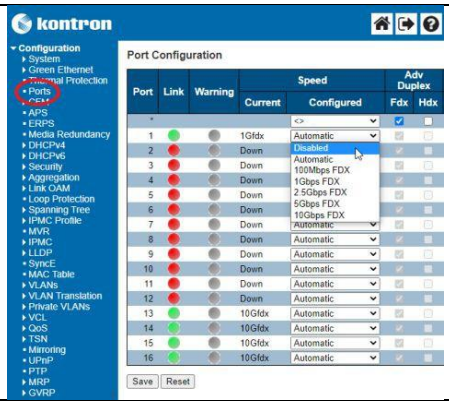
Étape_2	Désactiver l'interface. InviteCLI_NOSLocal:~(config-if)# **shutdown**	`(config-if)# shutdown`
Étape_3	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.5.5.2 Désactiver un port du commutateur en utilisant l'interface utilisateur Web

Accéder à l'interface utilisateur Web du NOS. Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, puis **Ports**.	

Étape_2	Désactiver un port du commutateur en changeant sa vitesse à **Disabled**.	
Étape_3	Cliquer sur le bouton **Save** pour confirmer.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.5.6 Modifier la vitesse de la liaison

La vitesse de la liaison peut être modifiée :

- En utilisant le CLI
- En utilisant l'interface utilisateur Web du commutateur

10.5.6.1 Modifier la vitesse de la liaison en utilisant le CLI

Accéder au CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

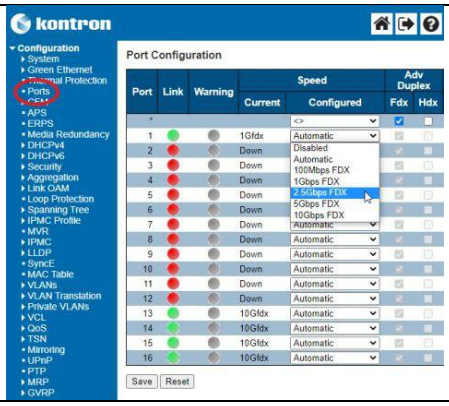
Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	`# configure terminal`
Étape_2	Entrer dans le mode de configuration de l'interface. InviteCLI_NOSLocal:~(config)# **interface [INTERFACE]**	`(config)# interface Eth 1/8`
Étape_3	Modifier la vitesse. InviteCLI_NOSLocal:~(config-if)# **speed [VITESSE]**	`(config-if)# speed auto 1000`
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.5.6.2 Modifier la vitesse de la liaison en utilisant l'interface utilisateur Web

Accéder à l'interface utilisateur Web du NOS. Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, puis **Ports**.	
Étape_2	Sélectionner une valeur dans le menu déroulant **Speed**.	
Étape_3	Cliquer sur le bouton **Save** pour confirmer.	

Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).

10.5.7 Configurer les VLAN du commutateur

Plusieurs configurations associées aux VLAN peuvent être effectuées en utilisant le CLI ou l'interface utilisateur Web du commutateur :

- Afficher les VLAN
- Créer un VLAN
- Supprimer un VLAN
- Configurer un port en tant que membre

10.5.7.1 Afficher les VLAN

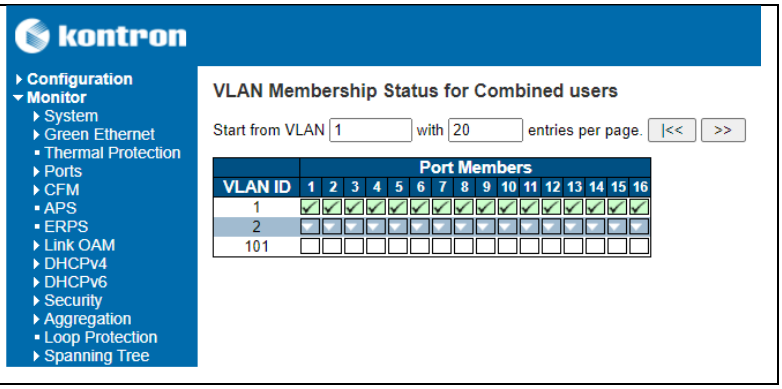
10.5.7.1.1 Afficher les VLAN en utilisant le CLI

Accéder au CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

Étape_1	Afficher l'état des VLAN pour chaque port du commutateur. InviteCLI_NOSLocal:~# **show vlan**	NOS00A0A5E01C4F# show vlan VLAN Name Interfaces ---- ---------- ---------- 1 default Eth 1/1-6 2 VLAN0002 Eth 1/7 3 VLAN0003 Eth 1/8-9

10.5.7.1.2 Afficher les VLAN en utilisant l'interface utilisateur Web

Accéder à l'interface utilisateur Web du NOS. Voir Accéder au NOS pour les instructions d'accès.

Étape_1	Dans le menu de gauche, sélectionner **Monitor**, **VLANs**, puis **Membership**. Les ports membres des VLAN devraient s'afficher.	

10.5.7.2 Créer un VLAN

10.5.7.2.1 Créer un VLAN en utilisant le CLI

Accéder au CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

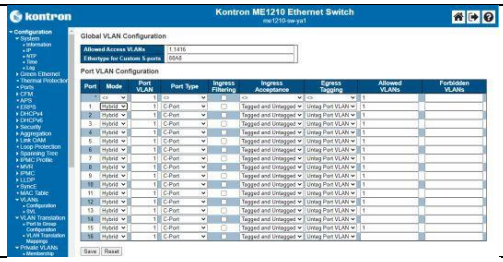
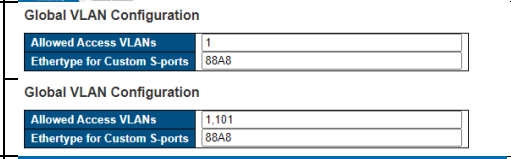
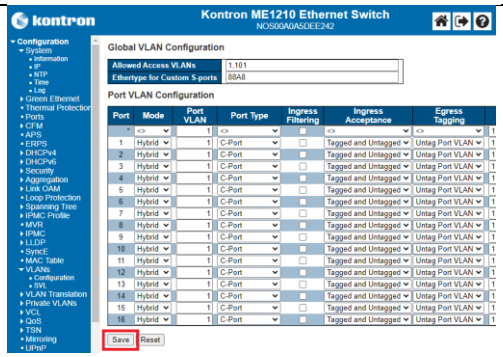
Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	# configure terminal
Étape_2	Créer un nouveau VLAN. InviteCLI_NOSLocal:~(config)# **vlan [ID_VLAN]**	(config)# vlan 9 (config-vlan)#
Étape_3	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.5.7.2.2 Créer un VLAN en utilisant l'interface utilisateur Web

Accéder à l'interface utilisateur Web du NOS. Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **VLANs**, puis **Configuration**.	
Étape_2	Dans la section **Global VLAN Configuration**, ajouter le ou les VLAN souhaités à la liste **Allowed Access VLANs**. **NOTE :** La liste des VLAN doit être délimitée par des virgules entre chaque ID d'interface.	
Étape_3	Cliquer sur le bouton **Save**.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.5.7.3 Supprimer un VLAN

10.5.7.3.1 Supprimer un VLAN en utilisant le CLI

Accéder au CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

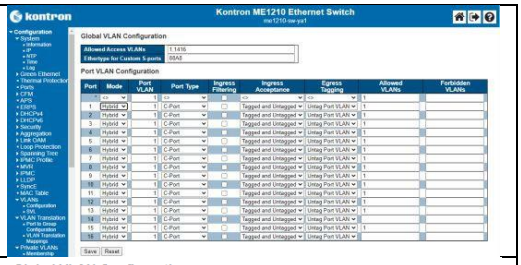
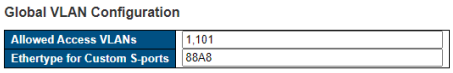
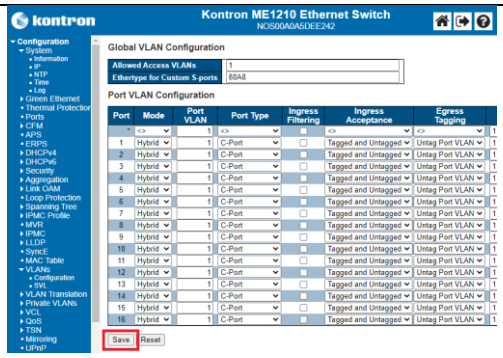
Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	`# configure terminal`
Étape_2	Supprimer un VLAN avec la commande suivante. InviteCLI_NOSLocal:~(config)# **no vlan [ID_VLAN]**	`(config)# no vlan 9` `(config)#`
Étape_3	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.5.7.3.2 Supprimer un VLAN en utilisant l'interface utilisateur Web

Accéder à l'interface utilisateur Web du NOS. Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **VLANs**, puis **Configuration**.	
Étape_2	Dans la section **Global VLAN Configuration**, supprimer le ou les VLAN souhaités de la liste **Allowed Access VLANs**.	 Global VLAN Configuration Allowed Access VLANs: 1,101 Ethertype for Custom S-ports: 88A8 Global VLAN Configuration Allowed Access VLANs: 1 Ethertype for Custom S-ports: 88A8
Étape_3	Cliquer sur le bouton **Save**.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.5.7.4 Configurer la liste des VLAN dont un port est membre

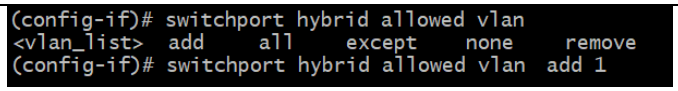
> La configuration par défaut du mode des ports du commutateur dans le NOS de la plateforme est « hybrid ». Par conséquent, la documentation ne détaille pas les commandes relatives aux modes « access » ou « trunk ».

10.5.7.4.1 Configurer l'appartenance à un port en utilisant le CLI

Accéder au CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

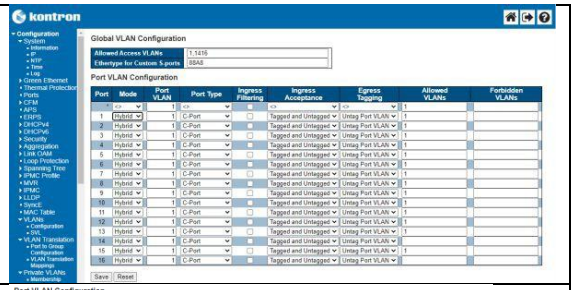
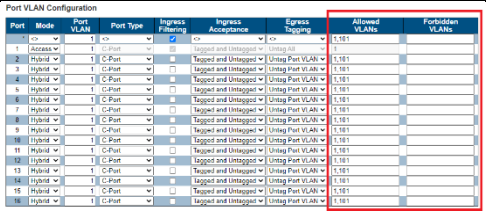
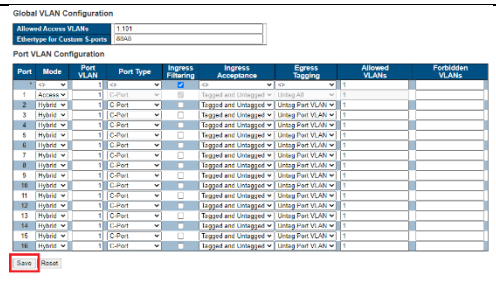
Étape_1	Entrer dans le mode de configuration de l'interface. InviteCLI_NOSLocal:~# **configure terminal** InviteCLI_NOSLocal:~(config)# **interface [ID_INTERFACE]**	`# configure terminal` `(config)# interface Ethernet 1/3`

Étape_2	Procéder à la configuration de l'appartenance au port. Interroger la fonction d'aide intégrée en utilisant le signe **?** pour voir les configurations possibles. Description des commandes de configuration de l'appartenance des VLAN : Ajouter un ou plusieurs VLAN avec la commande **add**. Ajouter tous les VLAN actuellement définis avec la commande **all**. Exclure un ou plusieurs VLAN avec la commande **except**. Exclure tous les VLAN actuellement définis avec la commande **none**. Supprimer un ou plusieurs VLAN avec la commande **remove**. • InviteCLI_NOSLocal:~(config-if)# **switchport hybrid allowed vlan add [ID_VLAN]**	
Étape_3	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.5.7.4.2 Configurer un port en tant que membre en utilisant l'interface utilisateur Web

Accéder à l'interface utilisateur Web du NOS. Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **VLANs**, puis **Configuration**.	
Étape_2	Configurer l'appartenance aux ports en utilisant les deux dernières colonnes. La liste des VLAN doit être délimitée par des virgules entre chaque ID d'interface ou un trait d'union pour décrire une plage. Exemple : 1,101-103,4093 Ce qui équivaut à : 1,101,102,103,4093	
Étape_3	Cliquer sur le bouton **Save** pour confirmer.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.5.8 Configurer le routage statique

Le routage statique peut être configuré :

- En utilisant le CLI
- En utilisant l'interface utilisateur Web du commutateur

10.5.8.1 Configurer le routage statique en utilisant le CLI

Accéder au CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant le CLI.

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal:~# **configure terminal**	`# configure terminal`
Étape_2	Configurer le routage statique. InviteCLI_NOSLocal:~(config)# **ip route [ADRESSE_HÔTE] [MASQUE_RÉSEAU] [ADRESSE_PASSERELLE]**	`(config)# ip route 192.168.3.0 255.255.255.0 172.16.0.3`
Étape_3	Quitter le mode de configuration. InviteCLI_NOSLocal:~(config)# **exit**	

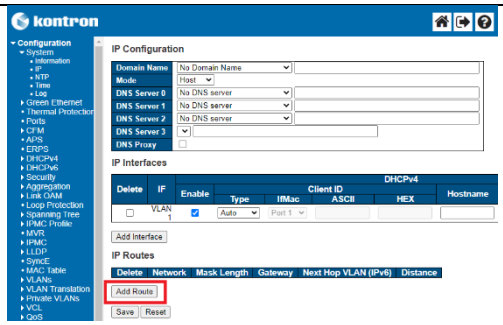
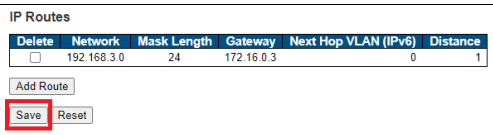
Étape_4	Afficher la liste des routes pour confirmer que la route statique a été ajoutée. InviteCLI_NOSLocal:~# **show ip route**	`# show ip route`
		`Codes: C - connected, S - static`
		`* - FIB route, D - DHCP installed route`
		`D* 0.0.0.0/0 [253/0] via 172.16.0.1, VLAN 1, 18:33:31`
		`C* 172.16.0.0/16 is directly connected, VLAN 1, 18:33:31`
		`S* 192.168.3.0/24 [1/0] via 172.16.0.3, VLAN 1, 18:33:31`

Étape_5	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.5.8.2 Configurer le routage statique en utilisant l'interface utilisateur Web

Accéder à l'interface utilisateur Web du NOS. Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, **System**, puis **IP**.	
Étape_2	Cliquer sur le bouton **Add Route**.	
Étape_3	Procéder à la configuration : • Saisir l'adresse de l'hôte dans la colonne **Network**. • Saisir le masque de réseau en nombre de bits dans la colonne **Mask Length**. Saisir l'adresse de la passerelle dans la colonne **Gateway**. • Configurer les paramètres **Next Hop VLAN (IPv6)** et **Distance**, si requis.	
Étape_4	Cliquer sur le bouton **Save** pour confirmer.	
Étape_5	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.5.9 Gérer la configuration du commutateur

La configuration du commutateur peut être gérée :

- En utilisant le CLI
- En utilisant l'interface utilisateur Web du commutateur

10.5.9.1 Gérer la configuration du commutateur en utilisant le CLI

Accéder au CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

10.5.9.1.1 Afficher la configuration actuelle en utilisant le CLI

Étape_1	Afficher la configuration actuelle. InviteCLI_NOSLocal:~# **show running-config**	NOS00A0A5E10E54# show running-config Building configuration... username admin privilege 15 password encrypted 4114dc09c554cbc78c5d5916ca7d0267a66c020fb4abeac88b9085191dea74e127c29e0f5fdf14e100c82f46d2410c830045931f03770addac2c9f1bf89d4227 ! vlan 1 ! ! ! ! spanning-tree mst name 00-a0-a5-e1-0e-54 revision 0 ! ! ptp ext output auto ptp rs422 main-auto ser proto rmc ! -- more --, next page: Space, continue: g, quit: ^C

10.5.9.1.2 Sauvegarder la configuration actuelle en utilisant le CLI

Les modifications apportées à la configuration du commutateur ne sont pas persistantes après le redémarrage du commutateur. Pour préserver les configurations personnalisées, utiliser la commande suivante.

Étape_1	Sauvegarder la configuration actuelle. InviteCLI_NOSLocal:~# **copy running-config startup-config**	# copy running-config startup-config Building configuration... % Saving 1555 bytes to flash:startup-config #

10.5.9.1.3 Rétablir la configuration par défaut en utilisant le CLI

NOTE : Cette procédure équivaut à réinitialiser les configurations par défaut du commutateur. Toutes les modifications apportées à la configuration seront perdues.

Étape_1	Rétablir la configuration par défaut. InviteCLI_NOSLocal:~# **reload defaults**	# reload defaults % Reloading defaults. Please stand by.
Étape_2	Pour rendre le retour aux valeurs par défaut permanent, utiliser la commande suivante. InviteCLI_NOSLocal:~# **copy running-config startup-config**	# copy running-config startup-config Building configuration... % Saving 1555 bytes to flash:startup-config

10.5.9.2 Gérer la configuration du commutateur en utilisant l'interface utilisateur Web

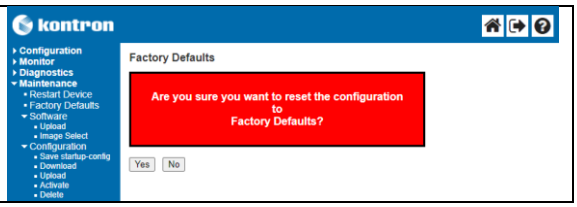
Accéder à l'interface utilisateur Web du NOS. Voir Accéder au NOS pour les instructions d'accès.

10.5.9.2.1 Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web

Les modifications apportées à la configuration du commutateur ne sont pas persistantes après le redémarrage du commutateur. Pour préserver les configurations personnalisées, utiliser la commande suivante.

Étape_1	Dans le menu de gauche, sélectionner **Maintenance**, **Configuration**, puis **Save startup-config**.	
Étape_2	Cliquer sur le bouton **Save Configuration**.	

10.5.9.2.2 Rétablir la configuration par défaut en utilisant l’interface utilisateur Web

Étape_1	Dans le menu de gauche, sélectionner **Maintenance**, puis **Factory Defaults**.	
Étape_2	Appuyer sur le bouton **Yes** pour confirmer le choix.	

10.6 Configuration de la synchronisation

Cette section s'applique uniquement aux plateformes équipées du module d'E/S de commutation Ethernet.

La synchronisation de la plateforme doit être configurée pour que tous les composants communiquent efficacement. Sur cette plateforme, le ToD (heure du jour) et la synchronisation de la phase peuvent être obtenus à partir du module GNSS intégré ou d'un GM (grandmaster) PTP accessible par le NOS via une connexion réseau au commutateur.

- Lorsque le module GNSS est utilisé, il transfère les informations au NOS, qui peut devenir un GM (grandmaster) PTP s'il est configuré en conséquence.
- Lorsqu'un GM (grandmaster) PTP accessible via une connexion réseau est utilisé, il transfère les informations au NOS pour synchroniser son instance BC (boundary clock) ou TSC (time slave clock).

Le commutateur peut ensuite servir de source de synchronisation pour d'autres composants en ayant recours à une combinaison de protocole de temps de précision (PTP) et d’Ethernet synchrone (SyncE). Les composants suivants peuvent également être synchronisés :

- Appareils esclaves PTP/SyncE connectés aux ports du commutateur de la plateforme
- Horloge matérielle PTP du contrôleur Ethernet E823 du serveur intégré de la plateforme
- Heure du système du NOS (via PTP)

Cette section décrit comment configurer la synchronisation pour les différents composants concernés.

Sections pertinentes :

Accéder au NOS

Accéder au système d'exploitation d'un serveur

Configuration et gestion des utilisateurs

10.6.1 Module GNSS intégré

10.6.1.1 Configuration d'usine

Le module GNSS NEO-M9N est configuré lors de la fabrication de la plateforme. Les configurations minimales suivantes sont effectuées pour s'assurer qu'il fonctionne correctement avec le NOS du commutateur Ethernet.

Élément	Description	Valeur par défaut	Valeur dans cette plateforme
CFG-NAVSPG-DYNMODEL	Modèle dynamique de la plateforme	0 (Portable)	2 (Stationary)
CFG-UART1-BAUDRATE	Débit en bauds du UART1	38400	115200

10.6.1.2 Configurer le retard du câble d'antenne

Il est fortement recommandé de configurer la compensation du retard du câble d'antenne pour obtenir une synchronisation précise.

Élément	Description	Valeur par défaut	Valeur dans cette plateforme
CFG-TP-ANT_CABLEDELAY	Retard du câble d'antenne	50 ns	Défini par l'utilisateur

Pour modifier les paramètres du module GNSS (NEO-M9N), utiliser ubxtool de la suite logicielle gpsd pour Linux qui s'exécute dans le serveur intégré.

> Il est nécessaire d'utiliser la version 3.22 de la suite logicielle gpsd. Pour plus d'information, consulter le site https://gpsd.gitlab.io/gpsd/index.html.

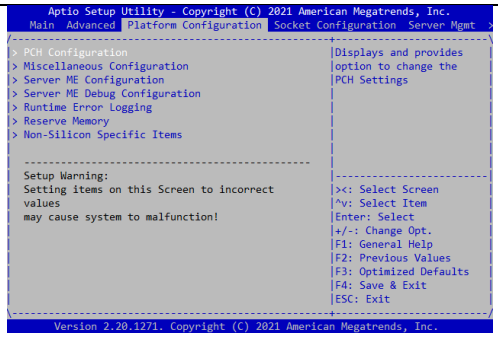
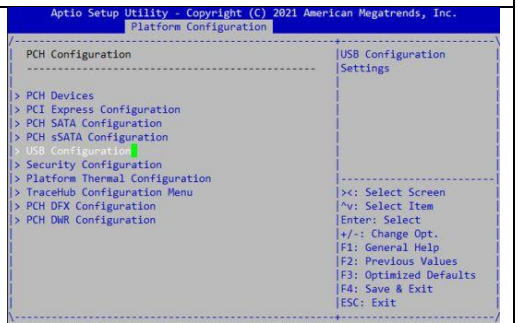
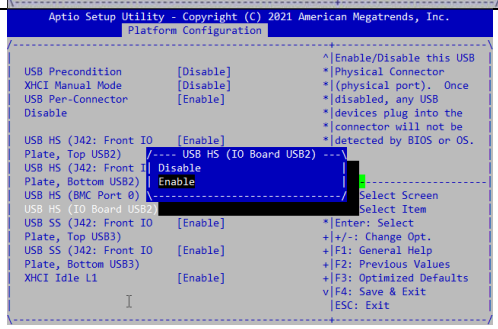
> Les modifications apportées à d'autres paramètres ne sont pas prises en charge. Par exemple, si une modification est apportée au débit en bauds, cela empêchera le NOS de recevoir le ToD (heure du jour) du module GNSS.

> Il est fortement recommandé de vérifier la compensation du retard en utilisant la sortie PPS de la plateforme et/ou PTP pour faire une comparaison avec une référence provenant d'un équipement de test sur site au moment de l'installation.

10.6.1.2.1 Vérifier l'état du port USB reliant le module GNSS au serveur interne

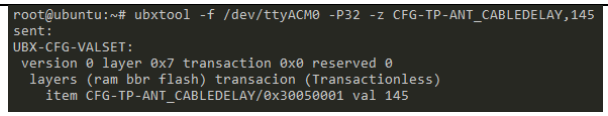
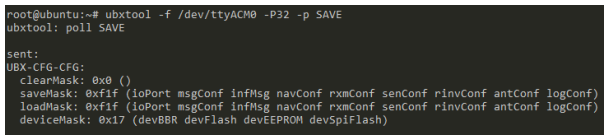
Par défaut, le port USB reliant le serveur intégré au module GNSS est désactivé.

Ouvrir une session dans le menu de configuration de l'UEFI/BIOS. Voir Accéder à l'UEFI/BIOS pour les instructions d'accès.

Étape_1	Dans le menu de configuration de l'UEFI/BIOS, naviguer jusqu'à l'onglet **Platform Configuration** et sélectionner **PCH Configuration**.	
Étape_2	Sélectionner **USB Configuration**.	
Étape_3	Sélectionner **USB HS** (**IO Board USB2**) et s'assurer que son état est à **Enable**.	

10.6.1.2.2 Configurer le retard de l’antenne

Ouvrir une session dans le serveur. Voir Accéder au système d'exploitation d'un serveur pour les instructions d'accès.

Étape_1	Configurer le retard du câble d'antenne. Dans cet exemple, la valeur sera fixée à 145 ns. InviteSE_Serveur:~# **ubxtool -f /dev/ttyACM0 -P32 -z CFG-TP-ANT_CABLEDELAY,[RETARD_CÂBLE]**	
Étape_2	Enregistrer la configuration dans la mémoire flash. InviteSE_Serveur:~# **ubxtool -f /dev/ttyACM0 -P32 -p SAVE**	

Avec la configuration par défaut, le module GNSS est automatiquement disponible pour une utilisation par le commutateur Ethernet. Le module GNSS devient la source de synchronisation lorsque l'instance PTP 0 est configurée en mode maître (master) uniquement. Le module peut également être activé en tant que source de synchronisation en mode BC (boundary clock). Le processus est décrit ci-dessous.

Les informations fournies par le module GNSS peuvent être utilisées simultanément par le serveur interne via l'interface USB, si nécessaire. Cette fonctionnalité est particulièrement intéressante pour les renseignements relatifs au positionnement ou à la surveillance dans l'application de l'utilisateur. L'utilisation de cette interface pour la synchronisation n'est pas recommandée car sa précision est très limitée. Si l'application exécutée sur le serveur intégré est associée à des exigences de synchronisation strictes, configurer le commutateur Ethernet pour le protocole PTP sur un ou plusieurs des ports 1/13 à 1/16 et utiliser LinuxPTP pour synchroniser le contrôleur Ethernet E823 du serveur intégré en heure et en date. Le processus est décrit ci-dessous.

Les applications Linux peuvent modifier la configuration du module GNSS. Ainsi, l'utilisation de la connexion USB au module GNSS peut causer des problèmes au niveau des opérations PTP du commutateur Ethernet. Les utilisateurs sont entièrement responsables de veiller au bon fonctionnement lors de l’utilisation de ce type de connexion.

10.6.2 PTP basé sur IEEE 1588

10.6.2.1 Sortie PPS

Section pertinente :

Sortie SMA PPS

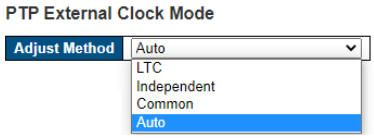
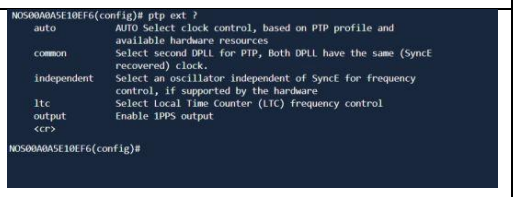
La sortie PPS est toujours activée et délivre une impulsion de 100 ms dont le front montant est aligné avec le retour à zéro du compteur ToD du domaine PTP 0.

La sortie PPS a un décalage inférieur à 10 ns par rapport à la phase PTP du commutateur intégré au niveau du connecteur SMA. Toute longueur de câble externe doit être compensée lors des mesures de synchronisation.

10.6.2.2 Configurer le paramètre PTP External Clock Mode du NOS

Le seul paramètre configurable est la méthode d'ajustement de l'horloge. Le réglage par défaut « auto » équivaut à « common » pour les profils IEEE1588 et G.8275.1. Les méthodes disponibles sont les suivantes :

- **Common** : L'horloge PTP utilise la DPLL matérielle pour l'ajustement de la fréquence PTP avec la fréquence SyncE comme référence si elle est disponible. Disponible uniquement pour l'instance d'horloge 0.
- **Independant** : L'horloge PTP utilise la DPLL matérielle pour l'ajustement de la fréquence PTP avec seulement l'oscillateur local comme référence de fréquence. Cela ne s'applique qu'à un déploiement où la référence SyncE n'est pas considérée comme valide pour l'instance d'horloge PTP. Disponible uniquement pour l'instance d'horloge 0.
- **LTC (Local Time Counter)** : L'instance d'horloge PTP utilise le compteur de temps local du commutateur Ethernet pour l'ajustement de la fréquence. Il s'agit de la seule option pour les instances d'horloge 1 à 3 puisque la DPLL matérielle est liée à l'instance d'horloge 0. Il est important de noter que cela signifie également que si l'instance d'horloge 0 est synchronisée avec un maître (master), les fréquences des compteurs de temps local (LTC) pour les instances d'horloge 1 à 3 seront déterminées par ce maître (master).

Interface utilisateur Web du NOS	CLI du NOS
	

10.6.2.3 Créer une instance PTP pour le NOS

Les informations suivantes sont basées sur le profil de télécom ITU-T G.8275.1. Cependant, d'autres profils PTP sont disponibles et les commandes peuvent être facilement adaptées.

10.6.2.3.1 Configurer le commutateur en tant que T-GM (Telecom Grandmaster) conformément à ITU-T G.8275.1

Le commutateur peut être configuré en tant que T-GM (Telecom Grandmaster) (horloge de référence primaire) en utilisant l'interface utilisateur Web ou le CLI du NOS. Les exemples suivants montrent les configurations minimales utilisant des valeurs par défaut pour la plupart des paramètres. Seules les valeurs critiques sont incluses dans les exemples. Toutefois, des configurations supplémentaires seront probablement nécessaires.

10.6.2.3.1.1 Préalable

1	Pour obtenir des résultats significatifs, le module GNSS intégré doit acquérir des informations de synchronisation. Une antenne appropriée doit être connectée à l'entrée GNSS du châssis. Voir le brochage et les caractéristiques électriques de l'entrée RF SMA GNSS.

10.6.2.3.1.2 Configurer le commutateur en tant que T-GM (Telecom Grandmaster) en utilisant le CLI

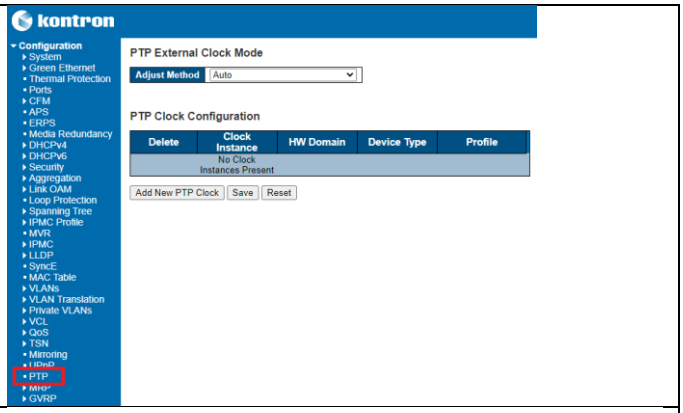
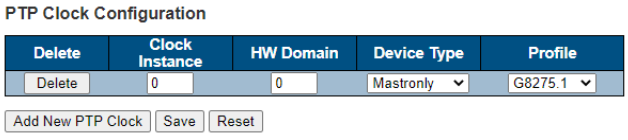
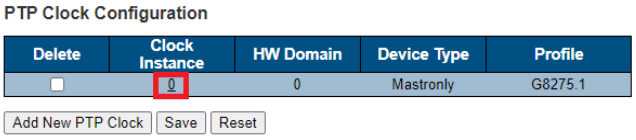
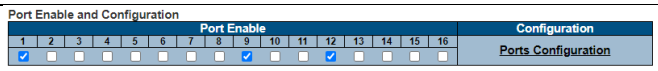
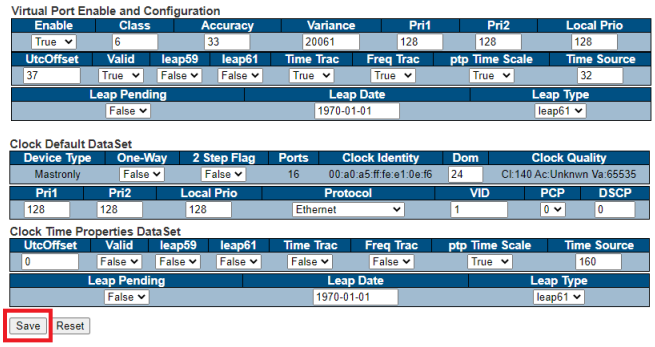
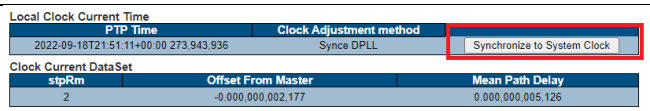
Ouvrir une session dans le CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

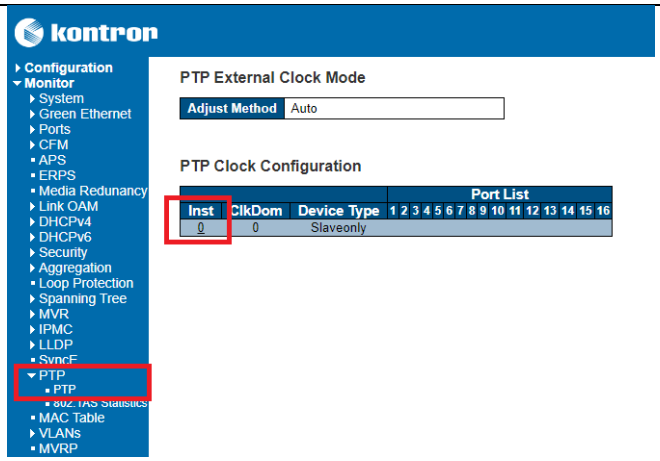
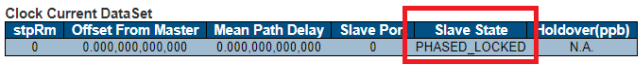
Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal# **configure terminal**	NOS00A0A5E10EF6# configure terminal NOS00A0A5E10EF6(config)#
Étape_2	Créer l'instance d'horloge PTP **0**. Ajouter ensuite la ou les interfaces souhaitées à **ptp 0**, l'instance d'horloge créée. InviteCLI_NOSLocal(config)# **ptp 0 mode master profile g8275.1** **NOTE :** La modification du type de filtre (**filter-type**) par défaut n'est pas prise en charge dans cette configuration.	NOS00A0A5E10EF6(config)# ptp 0 mode master profile g8275.1
Étape_3	Les éléments suivants configurent le jeu de données PTP communiqué par l'instance. Les valeurs obtenues sont valides lorsque l'instance a atteint l'état PHASE_LOCKED. InviteCLI_NOSLocal(config)# **ptp 0 virtual-port time-property utc-offset 37 valid time-traceable freq-traceable ptptimescale time-source 32** **ptp 0 virtual-port class 6** **ptp 0 virtual-port accuracy 33** **ptp 0 virtual-port variance 20061** **NOTE :** La valeur du paramètre **utc-offset** varie dans le temps et doit être déterminée en fonction de la valeur actuelle.	NOS00A0A5E10EF6(config)# $req-traceable ptptimescale time-source 32 NOS00A0A5E10EF6(config)# ptp 0 virtual-port class 6 NOS00A0A5E10EF6(config)# ptp 0 virtual-port accuracy 33 NOS00A0A5E10EF6(config)# ptp 0 virtual-port variance 20061
Étape_4	(Optionnel) Définir l'heure du système du NOS à partir de l'instance PTP. InviteCLI_NOSLocal(config)# **ptp system-time set** **NOTE :** Le protocole NTP doit être désactivé pour pouvoir régler l'heure du système du NOS en utilisant l'instance PTP. Le protocole NTP peut être désactivé avec la commande **no ntp**.	NOS00A0A5E10EF6(config)# ptp system-time set System clock synch mode (Set System time from PTP time)
Étape_5	Ajouter des interfaces à l'instance PTP. InviteCLI_NOSLocal(config)# **interface Ethernet 1/1,9,12** InviteCLI_NOSLocal(config-if)# **ptp 0**	NOS00A0A5E10EF6(config)# interface Ethernet 1/1,9,12 NOS00A0A5E10EF6(config-if)# ptp 0
Étape_6	Terminer la configuration. InviteCLI_NOSLocal(config-if)# **end**	NOS00A0A5E10EF6(config-if)# end NOS00A0A5E10EF6#
Étape_7	Vérifier l'état actuel de ptp 0. InviteCLI_NOSLocal# **show ptp 0** **NOTE :** La valeur à atteindre pour le paramètre **Slave State** est **PHASE_LOCKED**. Les étapes intermédiaires pouvant être affichées sont **FREQ_LOCKING**, **FREQ_LOCKED** et **HOLDOVER**. Le temps nécessaire pour atteindre **PHASE_LOCKED** varie en fonction de nombreux facteurs, dont l'état du module GNSS. Cinq minutes suffisent généralement.	NOS00A0A5E10EF6# show ptp 0 Dynamic data for PTP Clock Instance 0: PTP Time: 2022-06-29T16:25:43+00:00 902,081,031 Clock Slave state: Slave Port: 0 Slave State: PHASED_LOCKED Filter Mode: PACKET Holdover (ppb): N.A. Clock Current DataSet: Steps Removed: 0 Offset From Master: 0.000,000,000,000 Mean Path Delay: 0.000,000,000,000

Étape_8	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).

10.6.2.3.1.3 Configurer le commutateur en tant que T-GM (Telecom Grandmaster) en utilisant l'interface utilisateur Web

Ouvrir une session dans le CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, puis **PTP**.	
Étape_2	Dans la section **PTP Clock Configuration**, configurer le paramètre **Clock Instance**. Ensuite, définir le paramètre **Device Type** à **Mastronly** et le paramètre **Profile** à **G8275.1**. Enfin, cliquer sur le bouton **Save**.	
Étape_3	Cliquer sur le numéro dans le champ **Clock Instance** afin d'accéder à la page **PTP Clock's Configuration and Status**. **NOTE :** La modification du type de filtre (**filter-type**) par défaut n'est pas prise en charge dans cette configuration.	
Étape_4	Dans la section **Port Enable and Configuration**, sélectionner les ports sur lesquels activer le PTP.	
Étape_5	Dans la section **Virtual Port Enable and Configuration**, configurer l'instance d'horloge PTP avec les valeurs suivantes : • Enable : True • Class : 6 • Accuracy : 33 • Variance : 20061 • UtcOffset : 37 • Valid : True • Time Trac : True • Freq Trac : True • ptp Time Scale : True • Time Source : 32 S'assurer que l'ID du VLAN (paramètre **VID**) correspond à l'un des VLAN autorisés pour le ou les ports sélectionnés.	
Étape_6	Cliquer sur le bouton **Save**.	
Étape_7	Définir la source de temps du système à PTP en cliquant sur **Synchronize to System Clock**.	

Étape_8	Dans le menu de gauche, sélectionner **Monitor**, puis **PTP** et à nouveau **PTP**. Cliquer sur le numéro d'instance de l'horloge **PTP** souhaitée.	
Étape_9	Dans la section **Clock Current DataSet**, s'assurer que le paramètre **Slave State** est dans l'état souhaité. **NOTE :** La valeur à atteindre pour le paramètre **Slave State** est **PHASE_LOCKED**. Les étapes intermédiaires pouvant être affichées sont **FREQ_LOCKING**, **FREQ_LOCKED** et **HOLDOVER**. Le temps nécessaire pour atteindre **PHASE_LOCKED** varie en fonction de nombreux facteurs. À titre de référence, moins de 5 minutes sont généralement nécessaires.	
Étape_10	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.6.2.3.2 Configurer le commutateur en tant que T-BC (Telecom Boundary Clock) conformément à ITU-T G.8275.1

Le commutateur peut être configuré en tant que T-BC (Telecom Boundary Clock) en utilisant l'interface utilisateur Web ou le CLI du NOS.

Le port virtuel peut être activé pour la T-BC (Telecom Boundary Clock), comme c'est le cas pour la configuration en tant que T-GM (Telecom Grandmaster). Dans ce cas, il participe à l'algorithme BMCA comme n'importe quel autre maître (master) étranger PTP.

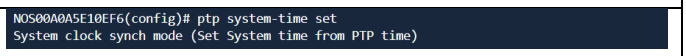
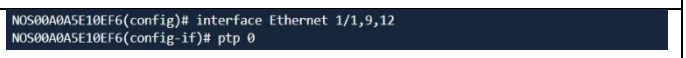
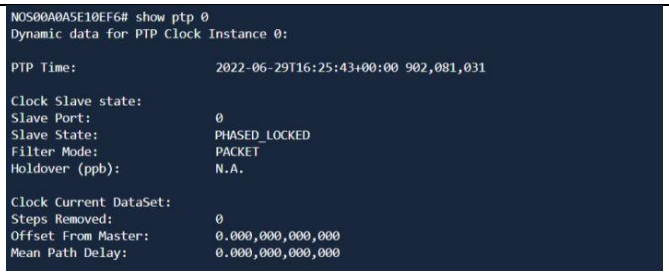
10.6.2.3.2.1 Préalable

1	Un T-GM (Telecom Grandmaster) G.8275.1 doit être connecté à la plateforme via un port SFP du commutateur intégré pour obtenir des résultats significatifs.

10.6.2.3.2.2 Configurer le commutateur en tant que T-BC (Telecom Boundary Clock) en utilisant le CLI

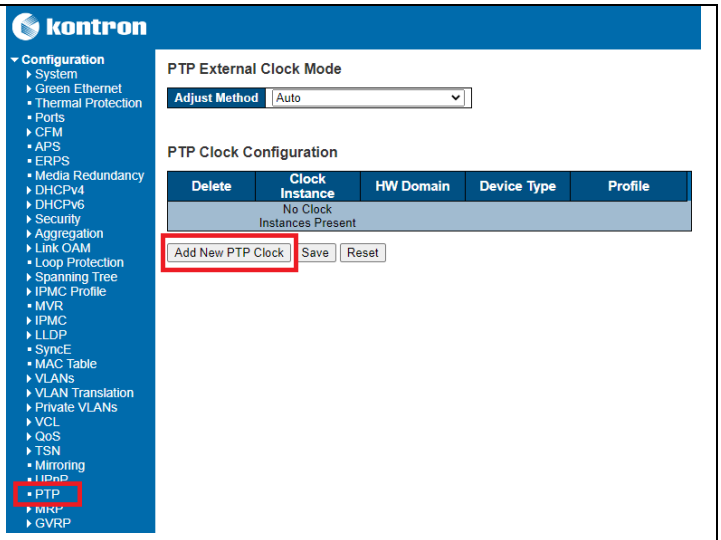
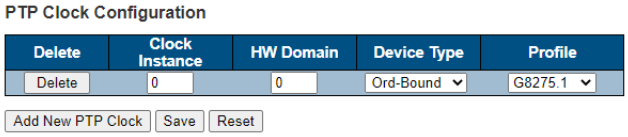
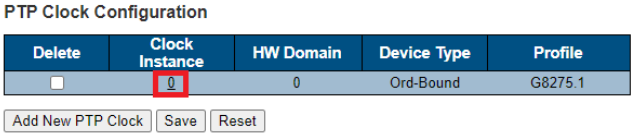
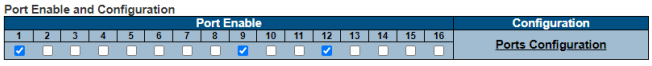
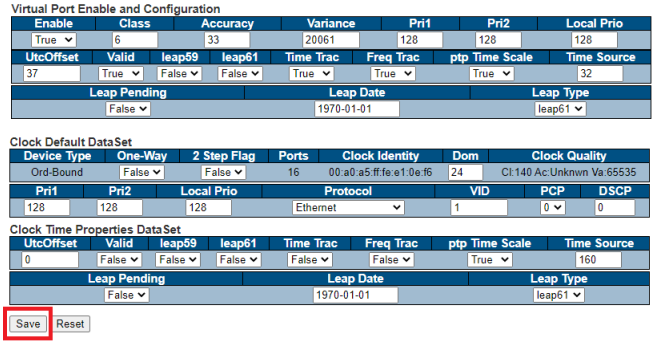
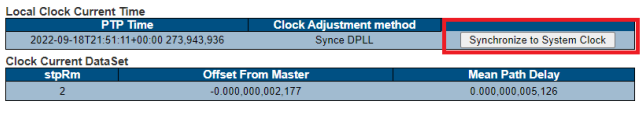
Ouvrir une session dans le CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

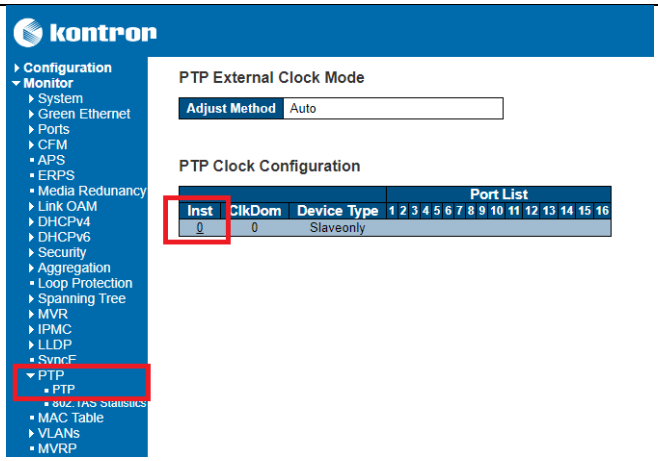
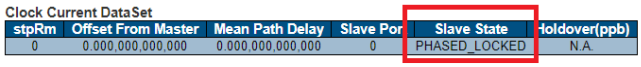
Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal# **configure terminal**	NOS00A0A5E10EF6# configure terminal NOS00A0A5E10EF6(config)#

Étape_2	Créer l'instance d'horloge PTP **0**. Ajouter ensuite la ou les interfaces souhaitées à **ptp 0**, l'instance d'horloge créée. InviteCLI_NOSLocal(config)# **ptp 0 mode boundary profile g8275.1** **NOTE :** La modification du type de filtre (**filter-type**) par défaut n'est pas prise en charge dans cette configuration.	
Étape_3	(Optionnel) Définir l'heure du système du NOS à partir de l'instance PTP. InviteCLI_NOSLocal(config)# **ptp system-time set** **NOTE :** Le protocole NTP doit être désactivé pour pouvoir régler l'heure du système du NOS en utilisant l'instance PTP. Le protocole NTP peut être désactivé avec la commande **no ntp**.	
Étape_4	Ajouter des interfaces à l'instance PTP. Cela comprend les interfaces connectées au potentiel T-GM du réseau ainsi que les interfaces connectées aux horloges esclaves (slave) en aval (T-BC ou T-TSC). Les ports passent automatiquement en mode maître (master) ou esclave (slave). InviteCLI_NOSLocal(config)# **interface Ethernet 1/1,9,12** InviteCLI_NOSLocal(config-if)# **ptp 0**	
Étape_5	Terminer la configuration. InviteCLI_NOSLocal(config-if)# **end**	
Étape_6	Vérifier l'état actuel de ptp 0. InviteCLI_NOSLocal# **show ptp 0** **NOTE :** La valeur à atteindre pour le paramètre **Slave State** est **PHASE_LOCKED**. Les étapes intermédiaires pouvant être affichées sont **FREQ_LOCKING**, **FREQ_LOCKED** et **HOLDOVER**. Le temps nécessaire pour atteindre **PHASE_LOCKED** varie en fonction de nombreux facteurs. À titre de référence, moins de 5 minutes sont généralement nécessaires.	
Étape_7	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.6.2.3.2.3 Configurer le commutateur en tant que T-BC (Telecom Boundary Clock) en utilisant l'interface utilisateur Web

Ouvrir une session dans l'interface utilisateur Web du NOS. Voir Accéder au NOS pour les instructions d'accès.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, puis **PTP**. Cliquer sur le bouton **Add New PTP Clock**.	
Étape_2	Dans la section **PTP Clock Configuration**, configurer le paramètre **Clock Instance**. Ensuite, définir le paramètre **Device Type** à **Ord-Bound** et le paramètre **Profile** à **G8275.1**. Enfin, cliquer sur le bouton **Save**.	
Étape_3	Cliquer sur le numéro dans le champ **Clock Instance** afin d'accéder à la page **PTP Clock's Configuration and Status**.	
Étape_4	Dans la section **Port Enable and Configuration**, sélectionner les ports sur lesquels activer le PTP. Cela comprend les interfaces connectées au potentiel T-GM du réseau ainsi que les interfaces connectées aux horloges esclaves (slave) en aval (T-BC ou T-TSC). Les ports passent automatiquement en mode maître (master) ou esclave (slave).	
Étape_5	Dans la section **Virtual Port Enable and Configuration**, configurer l'instance d'horloge PTP. S'assurer que l'ID du VLAN (paramètre **VID**) correspond à l'un des VLAN autorisés pour le ou les ports sélectionnés.	
Étape_6	Cliquer sur le bouton **Save**.	
Étape_7	Définir la source de temps du système à PTP en cliquant sur **Synchronize to System Clock**.	

Étape_8	Dans le menu de gauche, sélectionner **Monitor**, puis **PTP** et à nouveau **PTP**. Cliquer sur le numéro d'instance de l'horloge PTP souhaitée.	
Étape_9	Dans la section **Clock Current DataSet**, s'assurer que le paramètre **Slave State** est dans l'état souhaité. **NOTE :** La valeur à atteindre pour le paramètre **Slave State** est **PHASE_LOCKED**. Les étapes intermédiaires pouvant être affichées sont **FREQ_LOCKING**, **FREQ_LOCKED** et **HOLDOVER**. Le temps nécessaire pour atteindre **PHASE_LOCKED** varie en fonction de nombreux facteurs. À titre de référence, moins de 5 minutes sont généralement nécessaires.	
Étape_10	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.6.2.4 Configurer le serveur interne en tant que T-TSC (Telecom Time Slave Clock) conformément à ITU-T G.8275.1

Pour synchroniser avec précision l'heure du système et les interfaces réseau du serveur interne, utiliser LinuxPTP.

NOTE : Une version récente de LinuxPTP est nécessaire pour la prise en charge de la norme G.8275.1. La version 3.1 est utilisée ici. Ce logiciel doit être téléchargé et compilé car les distributions Linux peuvent ne proposer que des versions plus anciennes dans les dépôts de paquets.

NOTE : Les exemples sont fournis à des fins de démonstration uniquement. Consulter la documentation de votre distribution Linux pour configurer correctement les services PTP via le système d'initialisation du système d'exploitation.

Les options **masterOnly** et **slaveOnly** ci-dessous sont respectivement renommées **serverOnly** et **clientOnly** dans l'arborescence source actuelle de LinuxPTP. Si une version plus récente que la 3.1 est utilisée, la configuration ci-dessous doit être adaptée.

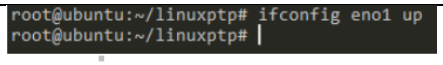
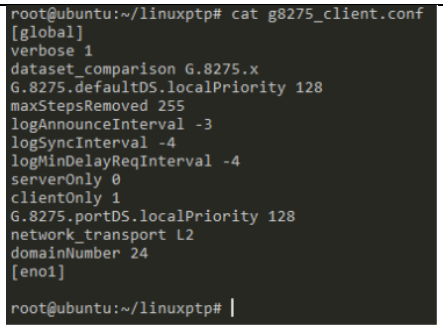
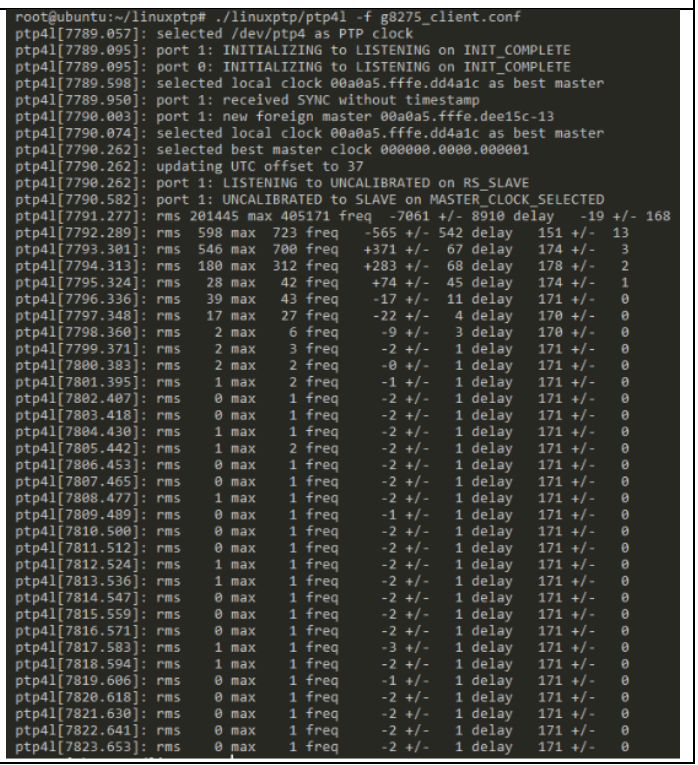
10.6.2.4.1 Synchroniser l'horloge matérielle PTP du contrôleur E823

10.6.2.4.1.1 Préalable

1	Le commutateur doit être configuré en tant que T-GM (Telecom Grandmaster) ou T-BC (Telecom Boundary Clock) comme expliqué ci-dessus. Dans l'exemple ci-dessous, l'interface 1/13 du commutateur intégré est utilisée et doit être configurée pour l'instance d'horloge PTP appropriée. Cela permet de se connecter à la connexion **eno1** du serveur intégré.

10.6.2.4.1.2 Procédure

Ouvrir une session dans le serveur. Voir Accéder au système d'exploitation d'un serveur pour les instructions d'accès.

Étape_1	S’assurer que l'interface réseau est opérationnelle. InviteSE_Serveur:~# **ifconfig eno1 up**	
Étape_2	Créer un fichier de configuration nommé **g8275_client.conf** avec le contenu suivant. InviteSE_Serveur:~# **cat g8275_client.conf** **[global]** **verbose 1** **dataset_comparison G.8275.x** **G.8275.defaultDS.localPriority 128** **maxStepsRemoved 255** **logAnnounceI nterval -3** **logSyncI nterval -4** **logMinDelayReqI nterval -4** **masterOnly 0** **slaveOnly 1** **G.8275.portDS.localPriority 128** **network_transport L2** **domainNumber 24** **[eno1]**	
Étape_3	Exécuter ptp4l. InviteSE_Serveur:~# **./linuxptp/ptp4l -f g8275_client.conf**	

10.6.2.4.2 Synchroniser l'heure du système du serveur intégré

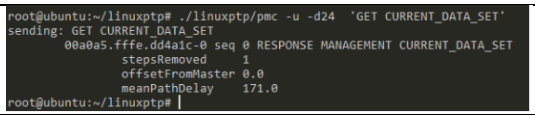
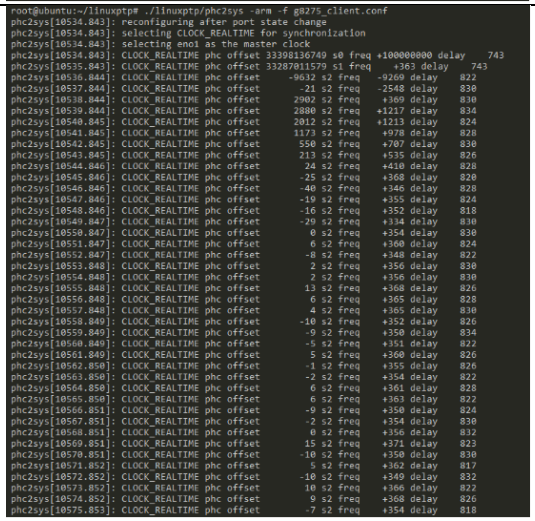
10.6.2.4.2.1 Préalable

1	Une instance ptp4l qui s’exécute sur le système d'exploitation de la plateforme doit être présente avant ce test.

S’assurer qu'aucun démon de synchronisation du temps (NTP ou autre) n'est en cours d'exécution, car il pourrait causer de l'interférence.

10.6.2.4.2.2 Procédure

Ouvrir une session dans le serveur. Voir Accéder au système d'exploitation d'un serveur pour les instructions d'accès.

Étape_1	Vérifier l'état du service ptp4l en cours d'exécution. InviteSE_Serveur:~# **./linuxptp/pmc -u -d24 'GET CURRENT_DATA_SET'**	
Étape_2	Synchroniser l'horloge matérielle physique (PHC) avec l'horloge du système. InviteSE_Serveur:~# **./linuxptp/phc2sys -arm -f g8275_client.conf**	

10.6.3 Configurer l'Ethernet synchrone

L'Ethernet synchrone (SyncE) (ITU-T G.8262) est pris en charge de même que le message d'état de synchronisation (SSM) sur le canal de messages de synchronisation Ethernet (ESMC) tel que défini dans ITU-T G.8264. Pour permettre la distribution de la fréquence à certains ou à tous les ports, deux ports doivent être choisis comme sources SyncE. Dans cet exemple, les ports 1/1 et 1/2 seront utilisés.

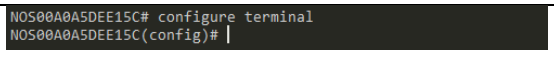
10.6.3.1 Préalable

1	Une source d'horloge SyncE valide provenant d'un équipement réseau externe est nécessaire.

La synchronisation des ports réseau du serveur intégré (interfaces 1/13-1/16) n'est pas pertinente puisque l'architecture d'horloge de la plateforme s'en charge automatiquement.

10.6.3.2 Configurer l'Ethernet synchrone en utilisant le CLI

Ouvrir une session dans le CLI du NOS. Voir Accéder au NOS pour les instructions d'accès.

Étape_1	Entrer dans le mode de configuration. InviteCLI_NOSLocal# **configure terminal**	

<table>
<tr><td>Étape_2</td><td>Désigner les interfaces auxquelles les sources de synchronisation d'horloge seront connectées. Il est possible de configurer jusqu'à deux sources.
NOTE : La source d'horloge numéro 3 est verrouillée sur l'horloge de la station qui n'est pas utilisée dans cette plateforme.
Le SSM peut être activé sur :
• Les interfaces sources d'horloge où la source enverra des messages d'état. Noter que les interfaces sources ne seront pas utilisées par le commutateur à moins que les messages SSM appropriés ne soient reçus.
• Les interfaces où le commutateur intégré de la plateforme sera une source SyncE pour lier les partenaires qui attendent des messages SSM afin de permettre leur synchronisation.
Dans cet exemple :
• Les interfaces 1/1 et 1/2 sont connectées à des sources SyncE envoyant des messages d’état SSM. Elles sont donc désignées et configurées pour le service SSM pour surveiller les sources.
• Les interfaces 1/3-1/12 configurées pour le service SSM peuvent être utilisées par les partenaires de liaison qui ont besoin d'une source SyncE et qui attendent des messages d’état SSM.
InviteCLI_NOSLocal(config)# network-clock clk-source 1 nominate interface Ethernet 1/1
InviteCLI_NOSLocal(config)# network-clock clk-source 2 nominate interface Ethernet 1/2
InviteCLI_NOSLocal(config)# interface Ethernet 1/1-12
InviteCLI_NOSLocal(config-if)# network-clock synchronization ssm</td><td><pre>NOS00A0A5DEE15C(config)# net$clk-source 1 nominate interface Ethernet 1/1
NOS00A0A5DEE15C(config)# net$ock clk-source 2 nominate interface Ethernet 1/2
NOS00A0A5DEE15C(config)# interface Ethernet 1/1-12
NOS00A0A5DEE15C(config-if)# network-clock synchronization ssm
NOS00A0A5DEE15C(config-if)#</pre></td></tr>
<tr><td>Étape_3</td><td>Terminer la configuration.
InviteCLI_NOSLocal(config-if)# end</td><td><pre>NOS00A0A5DEE15C(config-if)# end
NOS00A0A5DEE15C#</pre></td></tr>
<tr><td>Étape_4</td><td>Vérifier l'état des ports.
InviteCLI_NOSLocal# show network-clock</td><td><pre>NOS00A0A5DEE15C# show network-clock

Selector State is: Locked to 1

Alarm State is:
Clk: 1   2   3
LOCS: FALSE   TRUE   TRUE
SSM: FALSE   FALSE   FALSE
WTR: FALSE   FALSE   FALSE

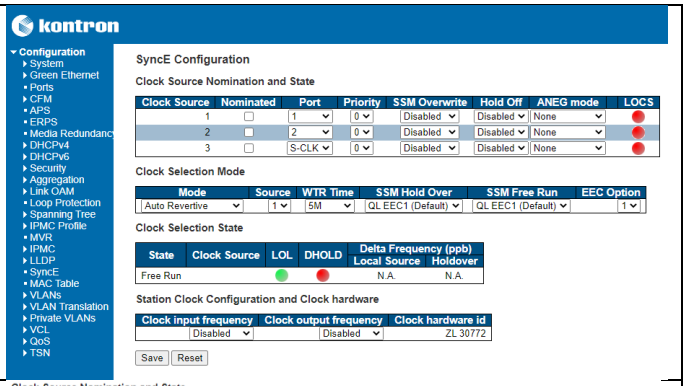
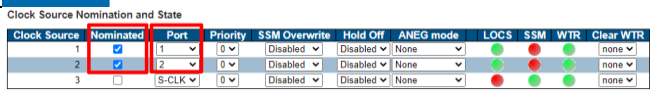
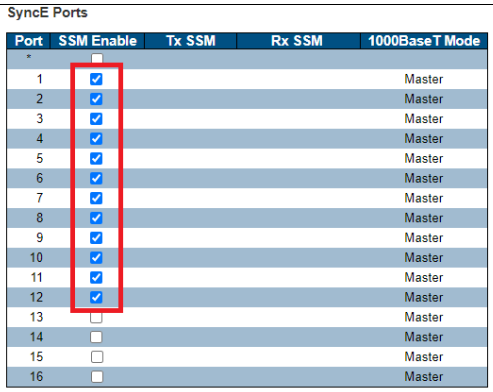
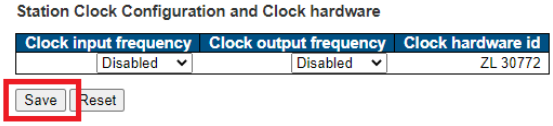
LOL: FALSE
DHOLD: FALSE

SSM State is:
Interface   Tx SSM   Rx SSM Mode
Ethernet 1/1   QL_DNU   QL_PRC Master
Ethernet 1/2   QL_LINK   QL_LINK Master
Ethernet 1/3   QL_PRC   QL_FAIL Master
Ethernet 1/4   QL_LINK   QL_LINK Master
Ethernet 1/5   QL_LINK   QL_LINK Master
Ethernet 1/6   QL_LINK   QL_LINK Master
Ethernet 1/7   QL_LINK   QL_LINK Master
Ethernet 1/8   QL_LINK   QL_LINK Master
Ethernet 1/9   QL_PRC   QL_FAIL Master
Ethernet 1/10   QL_LINK   QL_LINK Master
Ethernet 1/11   QL_LINK   QL_LINK Master
Ethernet 1/12   QL_LINK   QL_LINK Master

NOS00A0A5DEE15C#</pre></td></tr>
<tr><td>Étape_5</td><td colspan="2">(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).</td></tr>
</table>

10.6.3.3 Configurer l’Ethernet synchrone en utilisant l’interface utilisateur Web

Ouvrir une session dans l’interface utilisateur Web du NOS. Voir Accéder au NOS pour les instructions d'accès.

Étape_1	Dans le menu de gauche, sélectionner **Configuration**, puis **SyncE**.	
Étape_2	Dans la section **Clock Source Nomination and State**, désigner (**Nominate**) et sélectionner le numéro d'interface (nomenclature générale 1/x où x est la sélection ciblée ici) où les sources de synchronisation d'horloge seront connectées. Il est possible de configurer jusqu'à deux sources. **NOTE :** La source d'horloge numéro 3 est verrouillée sur l'horloge de la station qui n'est pas utilisée dans cette plateforme. Dans l'exemple, les interfaces 1/1 et 1/2 sont connectées à des sources SyncE et sont donc configurées pour les sources d'horloge 1 et 2.	
Étape_3	Dans la section **SyncE Ports**, le service SSM peut être activé sur : • Les interfaces sources d'horloge où la source enverra des messages d'état. Noter que les interfaces sources ne seront pas utilisées par le commutateur à moins que les messages SSM appropriés ne soient reçus. • Les interfaces où le commutateur intégré de la plateforme sera une source SyncE pour lier les partenaires qui attendent des messages SSM afin de permettre leur synchronisation. Dans l'exemple : • Les interfaces 1/1 et 1/2 sont connectées à des sources SyncE envoyant des messages d'état SSM. Elles sont donc configurées pour le service SSM pour surveiller les sources. • Les interfaces 1/3-1/12 peuvent être utilisées par les partenaires de liaison qui ont besoin d'une source SyncE et qui attendent des messages d'état SSM.	
Étape_4	Cliquer sur le bouton **Save**.	
Étape_5	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

10.7 Configuration des options UEFI/BIOS

Section pertinente :

Gestion de l'alimentation de la plateforme

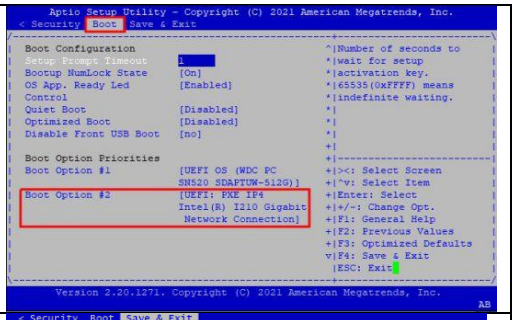
Les options peuvent être configurées :

- En utilisant le menu UEFI/BIOS
- Via le BMC en utilisant Redfish

10.7.1 Configurer les options UEFI/BIOS via le menu UEFI/BIOS

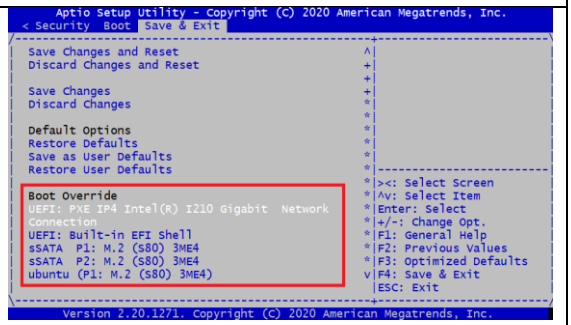
Accéder à l'UEFI/BIOS. Voir Accéder à l'UEFI/BIOS pour les instructions d'accès.

10.7.1.1 Modifier l'ordre de démarrage (boot order)

Étape_1	Dans le menu de configuration de l'UEFI/BIOS, naviguer jusqu'au menu **Boot**. Configurer l'ordre de démarrage comme souhaité.	
Étape_2	Sélectionner le menu **Save & Exit**, aller à **Save Changes and Reset** et appuyer sur **Entrée** pour confirmer et enregistrer le nouvel ordre de démarrage.	

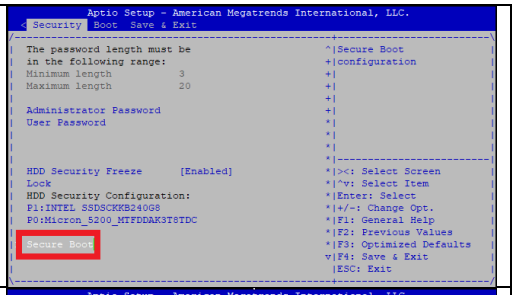
10.7.1.2 Modifier l'ordre de démarrage pour un démarrage unique

Il s'agit d'une option non persistante qui permet de démarrer sur un périphérique particulier tout en conservant l'ordre de démarrage normal.

Étape_1	Redémarrer la plateforme et accéder au menu de configuration de l'UEFI/BIOS.	
Étape_2	Naviguer jusqu'au menu **Save & Exit** et ensuite jusqu'à la section **Boot Override**.	

10.7.1.3 Activer le démarrage sécurisé

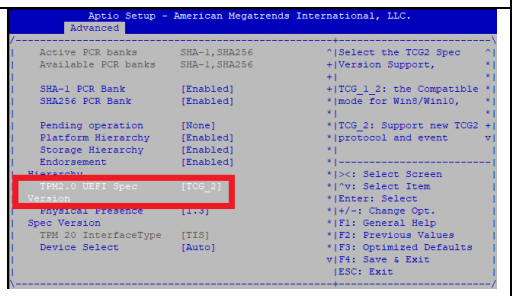
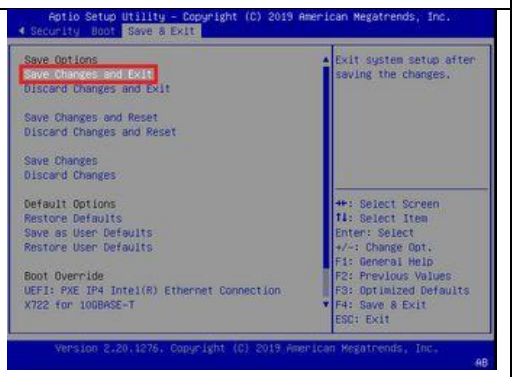
Les notes d'application suivantes sont nécessaires pour générer des clés de démarrage sécurisé et les configurer : Générer des clés de démarrage sécurisé personnalisées et Installer des clés de démarrage sécurisé personnalisées.

Étape_1	Naviguer jusqu'à l'onglet **Security** et accéder au sous-menu **Secure Boot**.	
Étape_2	Sélectionner l'option **Secure Boot** et la mettre à **Enabled**.	
Étape_3	Utiliser les notes d'application mentionnées ci-dessus comme référence pour générer et configurer les clés de démarrage sécurisé.	
Étape_4	Sélectionner le menu **Save & Exit**, aller à **Save Changes and Exit** et appuyer sur **Entrée** pour confirmer.	

10.7.1.4 Exécuter un verrouillage de sécurité du disque dur (HDD Security Freeze Lock)

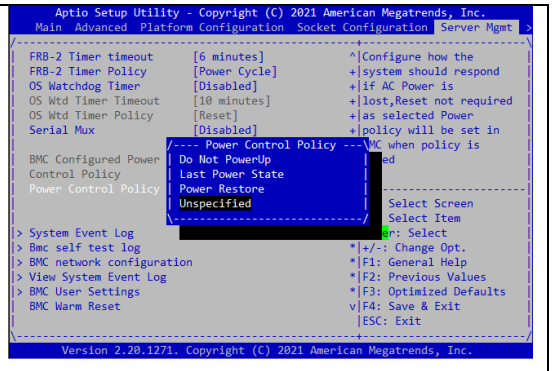
Étape_1	Naviguer jusqu'à l'onglet **Security** et activer ou désactiver l'option **HDD Security Freeze Lock**.	
Étape_2	Sélectionner le menu **Save & Exit**, aller à **Save Changes and Exit** et appuyer sur **Entrée** pour confirmer.	

10.7.1.5 Configurer le TPM

Étape_1	Sélectionner le menu **Advanced**, aller à **Trusted Computing** et sélectionner **Security Device Support**. Vérifier que l'option est à **Enable**. Valeurs possibles : [**Enable** / Disable] **NOTE :** Le TPM doit être inséré pour voir le menu.	
Étape_2	Dans le menu **Advanced** et la section **Trusted Computing**, sélectionner **TPM2.0 UEFI Spec Version** et définir la spécification applicable. Valeurs possibles : [TCG_1_2 / **TCG_2**] **NOTE :** Le TPM doit être inséré pour voir le menu.	
Étape_3	Dans le menu **Advanced** et la section **Trusted Computing**, sélectionner **Device Select** et définir le composant applicable. Valeurs possibles : [TPM 1.2 / TPM 2.0 / **Auto**] **NOTE :** Le TPM doit être inséré pour voir le menu.	
Étape_4	Sélectionner le menu **Save & Exit**, aller à **Save Changes and Exit** et appuyer sur **Entrée** pour confirmer.	

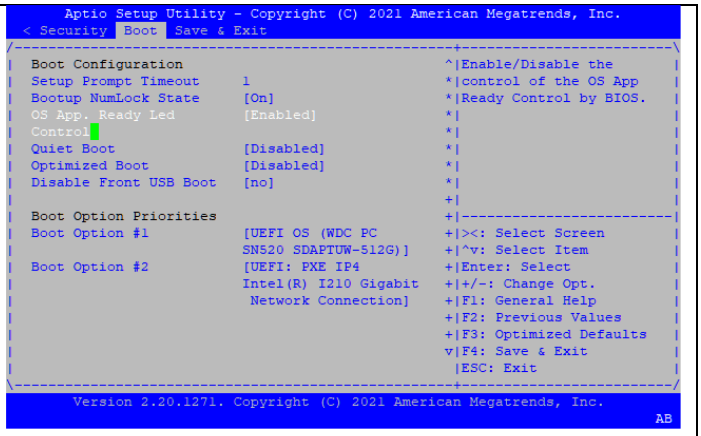
10.7.1.6 Configurer la stratégie de contrôle de l'alimentation (Power Control Policy) du serveur

Cette option permet de configurer la réponse du système à une perte d'alimentation à l'entrée du système.

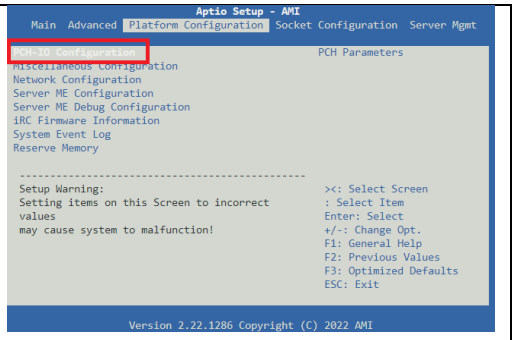
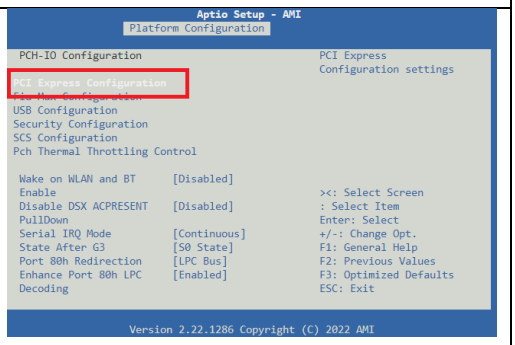
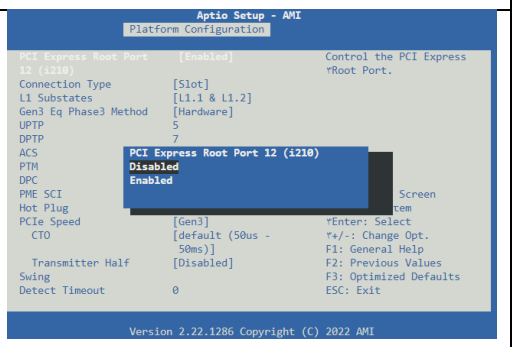
Étape_1	Naviguer jusqu'au menu **Server Mgmt**. Sélectionner **Power Control Policy** et choisir l'option en fonction de la réponse souhaitée. Valeurs possibles : [Do Not PowerUp / Last Power State / Power Restore / Unspecified] **NOTE :** Cette configuration est enregistrée dans le BMC et ne nécessite pas de réinitialisation du serveur. **NOTE :** Si la valeur choisie est Do Not PowerUp ou Last Power State, une commande doit être envoyée au BMC pour mettre sous tension et démarrer le serveur intégré puisqu'il n'y a pas de bouton d'alimentation sur l'unité.	

10.7.1.7 Configurer l'option Application Ready LED

Cette option modifie le comportement de la DEL d'alimentation verte. Voir Composants de la plateforme pour obtenir des informations sur le comportement. Voir Ressources de la plateforme destinées à l'application client pour savoir comment contrôler ce comportement à partir de votre application.

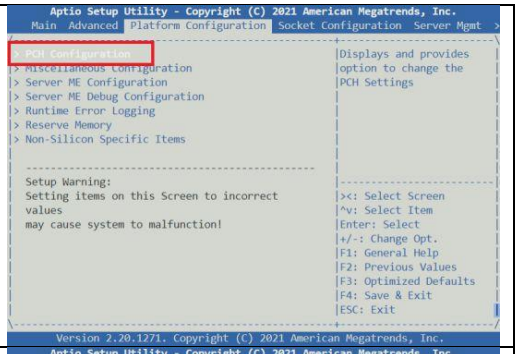
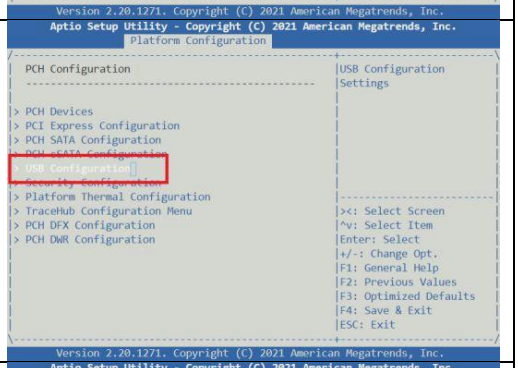
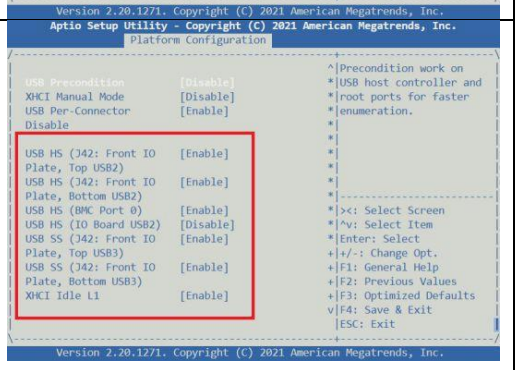
Étape_1	Naviguer jusqu'au menu **Boot** et activer ou désactiver l'option **OS App. Ready Led Control** pour enlever le contrôle à l'UEFI/BIOS.	

10.7.1.8 Désactiver de l'accès du serveur au contrôleur Ethernet I210

Étape_1	Naviguer jusqu'à l'onglet **Platform Configuration** et sélectionner **PCH-IO Configuration**.	
Étape_2	Naviguer jusqu'à **PCI Express Configuration**.	
Étape_3	Naviguer jusqu'au composant **PCI Express Root Port 12 (i210)** et sélectionner **Disabled**. Cette action déconnectera essentiellement le contrôleur Ethernet I210 du serveur.	

10.7.1.9 Désactiver des ports USB

NOTE : Activer ou désactiver des ports USB de la plateforme peut entraîner un dysfonctionnement du système. Procéder avec prudence.

Étape_1	Naviguer jusqu'à l'onglet **Platform Configuration** et sélectionner **PCH-IO Configuration** ou **PCH Configuration** en fonction de la version du micrologiciel de l'UEFI/BIOS.	
Étape_2	Sélectionner **USB Configuration**.	
Étape_3	Tous les ports USB sont identifiés dans ce menu. Activer ou désactiver les ports en fonction des considérations suivantes : 1. Il n'est pas recommandé de modifier la configuration des ports USB, à l'exception de celle des ports décrits ci-dessous. Si d'autres ports que ceux mentionnés sont reconfigurés, la plateforme risque d'être inutilisable. 2. Les ports USB du panneau avant sont étiquetés ainsi : **Front IO Plate**. La prise en charge de l'USB 3.0 et de l'USB 2.0 doit être activée/désactivée séparément. 3. Ne pas désactiver **BMC Port 0** à moins que vous ne souhaitiez désactiver la fonctionnalité Redfish pour le micrologiciel de l'UEFI/BIOS. Cela désactiverait également le port MGMTUSB du panneau avant.	

10.7.2 Configurer les options UEFI/BIOS via le BMC en utilisant Redfish

Cette option sera disponible dans une prochaine version du logiciel de la plateforme.

10.7.3 Spécifier le périphérique de démarrage suivant via le BMC en utilisant Redfish

Étape_1	Obtenir une liste des périphériques de démarrage disponibles. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/Systems/system | jq.Boot**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system
  | jq .Boot
{
    "AutomaticRetryAttempts": 3,
    "AutomaticRetryConfig": "RetryAttempts",
    "AutomaticRetryConfig@Redfish.AllowableValues": [
        "Disabled",
        "RetryAttempts"
    ],
    "BootSourceOverrideEnabled": "Continuous",
    "BootSourceOverrideTarget": "BiosSetup",
    "BootSourceOverrideTarget@Redfish.AllowableValues": [
        "None",
        "Pxe",
        "Hdd",
        "Cd",
        "Diags",
        "BiosSetup",
        "Usb"
    ],
    "TrustedModuleRequiredToBoot": "Disabled"
}
```

Étape_2

Modifier le périphérique de démarrage suivant.

Le paramètre **OVERRIDE_TYPE** peut prendre l'une des valeurs suivantes :

- Continuous
- Once
- None

InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/Systems/system --header 'Content-Type: application/json' --data '{ "Boot": { "BootSourceOverrideTarget": "[PÉRIPHÉRIQUE_DÉMARRAGE]", "BootSourceOverrideEnabled": " [TYPE_FORÇAGE] " } }' | jq**

```
$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems
/system --header 'Content-Type:application/json' --data '{"Boot": {"BootSourceOverrideTarg
et": "Hdd","BootSourceOverrideEnabled": "Continuous"}}' | jq
```

10.8 Configurer les capteurs et les paramètres thermiques

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.

Les modifications apportées aux paramètres thermiques seront perdues lors de la mise à niveau du BMC. Cependant, elles sont persistantes lorsque la BMC redémarre.

Les informations fournies dans cette section permettent de configurer les capteurs associés aux cartes d'expansion PCIe de l'utilisateur final. Seuls les capteurs suivants doivent être configurés par l'utilisateur final :

- Temp PCIe 1 mbox
- Temp PCIe 2 mbox
- Temp PCIe 1
- Temp PCIe 2
- Temp Chassis

Voir Installer une sonde thermique pour la carte d'expansion PCIe pour obtenir des informations sur l'installation et Ressources de la plateforme destinées à l'application client pour le code à intégrer dans l'application afin de communiquer des informations sur les capteurs de l'utilisateur au BMC.

Pour plus d'informations sur les capteurs, voir Liste des capteurs.

Pour les instructions d'interprétation des données d'événement, voir Interprétation des données des capteurs.

Les capteurs de la plateforme peuvent être configurés :

- En utilisant Redfish
- En utilisant IPMI

> Le seuil critique supérieur du capteur doit être supérieur au seuil non critique supérieur pour que le contrôleur des ventilateurs fonctionne correctement.

10.8.1 Configurer avec Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Voir Créer des extensions URL et Liste des capteurs pour les informations requises sur les capteurs.

10.8.1.1 Configurer les seuils des capteurs

NOTE : Les seuils des capteurs qui ne sont pas remplis par défaut ne peuvent être ni remplis ni configurés.

Étape_1	Identifier l'URL à utiliser pour modifier les seuils et le nom du capteur.
Étape_2	Modifier la valeur de seuil du capteur souhaité. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/[URL_CAPTEUR] --header 'Content- Type: application/json' --data '{ "[RESSOURCE]": [{"MemberI d": "[NOM_CAPTEUR]", "[SEUIL]":[VALEUR]}] }' | jq** Les valeurs prises en charge pour le paramètre **[SEUIL]** sont : • LowerThresholdCritical • LowerThresholdNonCritical • UpperThresholdCritical • UpperThresholdNonCritical Pour modifier les capteurs associée à la carte d'expansion PCIe de l'utilisateur final, la valeur du paramètre **[RESSOURCE]** est : • Temperatures

```
$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Chassis/ME1210_Baseboard/Thermal --header 'Content-Type:application/json' --data '{"Temperatures": [{"MemberId": "Temp_PCIe_1","UpperThresholdNonCritical": 77}]}' | jq
{
  "@odata.id": "/redfish/v1/Chassis/ME1210_Baseboard/Thermal",
  "@odata.type": "#Thermal.v1_4_0.Thermal",
  "Fans": [],
  "Id": "Thermal",
  "Name": "Thermal",
  "Temperatures": []
}
```

10.8.1.2 Configurer la vitesse minimale des ventilateurs

> La vitesse minimale des ventilateurs ne doit jamais être inférieure à 30 %.

Étape_1	Définir la vitesse minimale des ventilateurs. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/Managers/bmc --header 'Content-Type: application/json' --data '{ "Oem": { "OpenBmc": {"Fan": {"FanControllers": {"Fan_Controller": {"OutLimitMin": [VITESSE_MIN_VENTILATEURS]}}}}}}' | jq**
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc --header 'Content-Type:application/json' --data '{"Oem": {"OpenBmc": {"Fan": {"FanControllers": {"Fan_Controller": {"OutLimitMin": 30.0}}}}}}' | jq`

10.8.1.3 Configurer la vitesse maximale des ventilateurs

La vitesse maximale des ventilateurs ne peut pas dépasser 100 %.

Une valeur inférieure à 100 % peut affecter les performances du système et la plage de température de fonctionnement.

Étape_1	Définir la vitesse maximale des ventilateurs. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/Managers/bmc --header 'Content-Type: application/json' --data '{ "Oem": { "OpenBmc": {"Fan": {"FanControllers": {"Fan_Controller": {"OutLimitMin": [VITESSE_MAX_VENTILATEURS]}}}}}}' | jq**
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc --header 'Content-Type:application/json' --data '{"Oem": {"OpenBmc": {"Fan": {"FanControllers": {"Fan_Controller": {"OutLimitMax": 90.0}}}}}}' | jq`

10.8.1.4 Configurer un décalage de seuil

Un décalage de seuil est un décalage appliqué aux seuils supérieur non critique et supérieur critique en vue de démarrer les ventilateurs avant d'atteindre le seuil réel. Cela permet de s'assurer de ne pas envoyer une grande quantité d'événements lorsque les valeurs oscillent autour d'un seuil d'enclenchement.

Étape_1	Définir un décalage de seuil. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/Managers/bmc --header 'Content-Type: application/json' --data '{"Oem": {"OpenBmc": {"Fan": {"LinearControllers": {"[ID_CAPTEUR] ": {"ThresholdOffset": [VALEUR] }}}}}' | jq** **NOTE :** La valeur du paramètre ThresholdOffset doit être négative.
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc --header 'Content-Type:application/json' --data '{"Oem": {"OpenBmc": {"Fan": {"LinearControllers": {"Temp_PCIe_1": {"ThresholdOffset":-3}}}}}' | jq`

10.8.1.5 Configurer le décalage du point de départ par rapport au seuil

Le décalage du point de départ par rapport au seuil est un décalage appliqué à la valeur « supérieure non critique + décalage de seuil » pour démarrer les ventilateurs à une valeur de température inférieure. Cela permet d'obtenir une courbe plus douce à partir de la vitesse minimale des ventilateurs avant d'atteindre le seuil supérieur non critique.

Étape_1	Définir le décalage du point de départ par rapport au seuil. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/Managers/bmc --header 'Content-Type: application/json' --data '{"Oem": {"OpenBmc": {"Fan": {"LinearControllers": {"[ID_CAPTEUR]": {"StartPointOffsetFromThreshold": [VALEUR]}}}}}}'** **NOTE :** La valeur du paramètre StartPointOffsetFromThreshold doit être négative.
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc --header 'Content-Type:application/json' --data '{"Oem": {"OpenBmc": {"Fan": {"LinearControllers": {"Temp_PCIe_1": {"StartPointOffsetFromThreshold": -9}}}}}' | jq`

10.8.1.6 Configurer la température ambiante minimale

Pour plus d'informations sur les fonctionnalités liées à la température ambiante minimale, voir Refroidissement et gestion thermique de la plateforme.

La température ambiante minimale est la valeur du capteur Temp Inlet à laquelle les ventilateurs commencent à fonctionner à la vitesse minimale. En dessous de cette valeur, les ventilateurs sont arrêtés pour que le chauffage puisse faire son travail dans un environnement froid.

Étape_1	Définir la température ambiante minimale. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/ Managers/bmc --header 'Content-Type: application/json' --data '{ "Oem": {"OpenBmc": {"Fan": {"FanControllers": {"Fan_Controller":{"AmbientTempMin":[VALEUR]}}}}}}' | jq**
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc --header 'Content-Type:application/json' --data '{"Oem": {"OpenBmc": {"Fan": {"FanControllers": {"Fan_Controller": {"AmbientTempMin": 12}}}}}}' | jq`

10.8.2 Configurer avec 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] -C 17**.

10.8.2.1 Configurer les seuils

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, changer le seuil du capteur souhaité.
	InviteSE_ServeurLocal:~# **ipmitool sensor thresh "[ID_CAPTEUR]" [TYPE_SEUIL] [VALEUR]**
	Les valeurs prises en charge pour le paramètre [TYPE_SEUIL] sont :
	• unr = upper non-recoverable (supérieur irrécupérable)
	• ucr = upper critical (critique supérieur)
	• unc = upper non-critical (non critique supérieur)
	• lnc = lower non-critical (non critique inférieur)
	• lcr = lower critical (critique inférieur)
	• lnr = lower non-recoverable (inférieur irrécupérable)
		`$ ipmitool sensor thresh "Temp BMC" ucr 180`
		`Locating sensor record 'Temp BMC'...`
		`Setting sensor "Temp BMC" Upper Critical threshold to 180,000`

11/ Opération

11.1 Gestion de l'alimentation de la plateforme

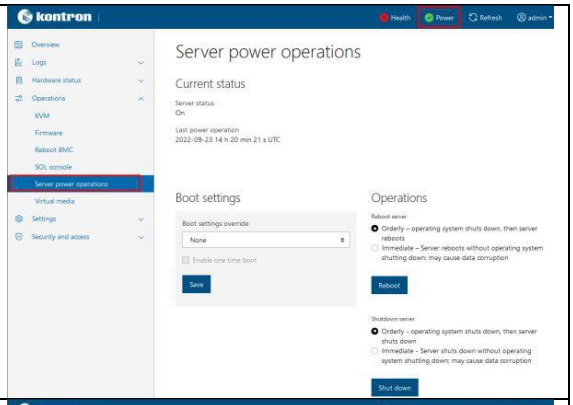
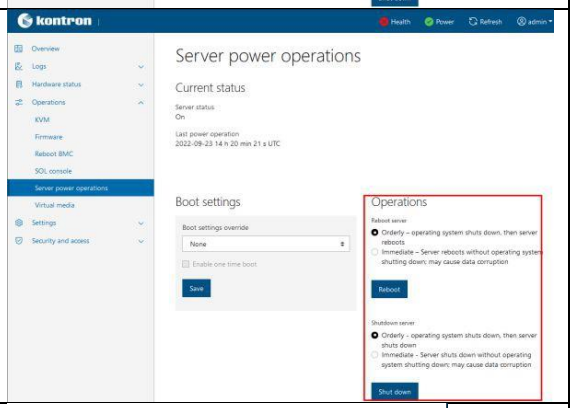
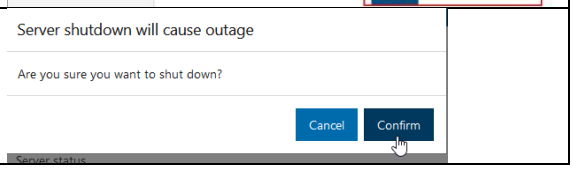
11.1.1 Gérer l'alimentation du serveur intégré

Une commande d'alimentation peut être exécutée :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish
- En utilisant IPMI sur LAN

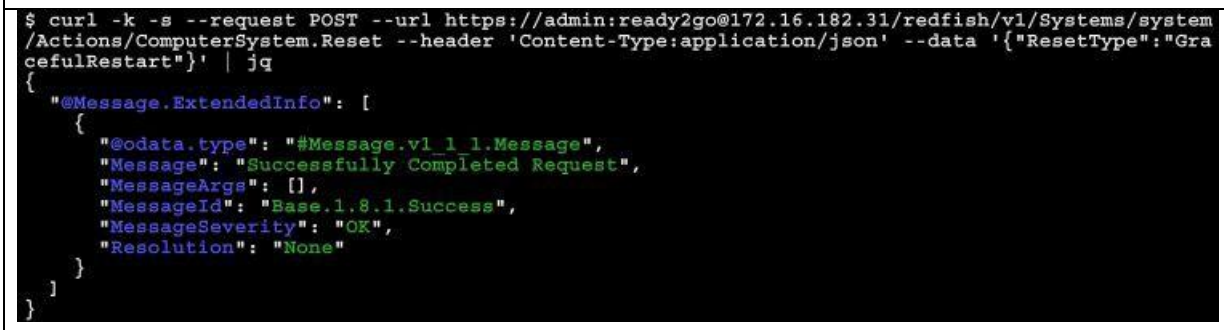
11.1.1.1 Gérer l'alimentation du serveur intégré en utilisant l'interface utilisateur Web du BMC

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

Étape_1	Dans le menu de gauche, cliquer sur **Operations**, puis sur **Server power operations** ou cliquer simplement sur l'icône d'état **Power** en haut de la page.	
Étape_2	Cliquer sur le bouton associé à l'action souhaitée.	
Étape_3	Cliquer sur le bouton **Confirm** pour continuer. La plateforme effectuera la commande d'alimentation.	

11.1.1.2 Gérer l'alimentation du serveur intégré en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

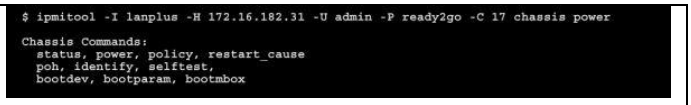
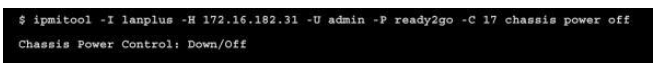
Étape_1	Exécuter la commande suivante pour gérer l'alimentation de la plateforme. InviteSE_OrdinateurDistant:~$ **curl -k -s --request POST --url [URL_RACINE]/redfish/v1/Systems/system/Actions/ComputerSystem.Reset --header 'Content-Type: application/json' - -data '{"ResetType":"[COMMANDE_ALIMENTATION]"}' | jq** Les valeurs prises en charge pour le paramètre **[COMMANDE_ALIMENTATION]** sont : • On • ForceOff • ForceOn • ForceRestart • GracefulRestart • GracefulShutdown • PowerCycle
	
Étape_2	Vérifier l'état actuel de l'alimentation. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/Systems/system | jq .PowerState**
	

11.1.1.3 Gérer l'alimentation du serveur intégré en utilisant IPMI sur LAN (IOL)

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

Les commandes d'alimentation peuvent être exécutées à partir du système d'exploitation du serveur intégré en utilisant IPMI via KCS.

NOTE : Si une commande visant à éteindre le serveur intégré est envoyée à partir du serveur intégré, il deviendra inaccessible. Si l'objectif est d'envoyer une commande pour démarrer le serveur intégré, une autre méthode d'accès au BMC doit être utilisée.

Étape_1	Afficher la liste des commandes d'alimentation. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] -C 17 chassis power**	
Étape_2	Exécuter la commande d'alimentation souhaitée parmi les commandes affichées. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] -C 17 chassis power [COMMANDE_ALIMENTATION]**	

Étape_3	Vérifier l'état de l'alimentation. InviteSE_OrdinateurDistant:~# **ipmitool -I lanplus -H [IP_GESTION_BMC] -U [NOM_UTILISATEUR_IPMI] -P [MOT_DE_PASSE_IPMI] -C 17 chassis power status**	

NOTE : La commande de réinitialisation IPMI n'entraîne pas de réinitialisation matérielle. Elle fait simplement éteindre le serveur et le redémarre automatiquement.

11.1.2 Redémarrer le BMC

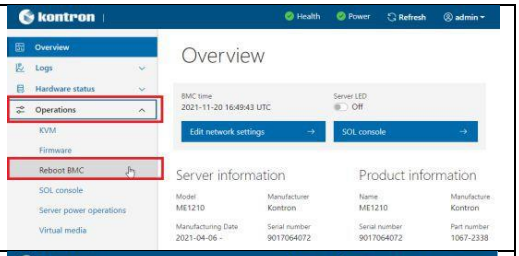
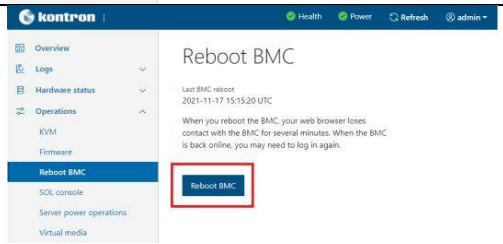
Un redémarrage du BMC peut être exécuté :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish

11.1.2.1 Redémarrer le BMC en utilisant l'interface utilisateur Web

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

NOTE : Le redémarrage du BMC avec l'interface utilisateur Web pourrait mettre fin à la session utilisateur en cours.

Étape_1	Dans le menu de gauche, cliquer sur **Operations**, puis **Reboot BMC**.	
Étape_2	Cliquer sur le bouton **Reboot BMC**, puis confirmer.	
Étape_3	Attendre que le BMC redémarre. Cela peut prendre un certain temps.	

11.1.2.2 Redémarrer le BMC en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Exécuter la commande suivante pour redémarrer le BMC. InviteSE_OrdinateurDistant:~$ **curl -k -s --request POST --url [URL_RACINE] /redfish/v1/ Managers /bmc/Actions/Manager.Reset --header 'Content-Type: application/json' --data '{"ResetType":"GracefulRestart"}' | jq**


```
$ curl -k -s --request POST --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/Actions/Manager.Reset --header 'Content-Type:application/json' --data '{"ResetType":"GracefulRestart"}' | jq
{
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "Message": "Successfully Completed Request",
      "MessageArgs": [],
      "MessageId": "Base.1.8.1.Success",
      "MessageSeverity": "OK",
      "Resolution": "None"
    }
  ]
}
```

Étape_2	Attendre que le BMC redémarre. Cela peut prendre un certain temps.

11.1.3 Redémarrer le NOS

Un redémarrage du NOS peut être exécuté :

- En utilisant le CLI du NOS
- En utilisant l'interface utilisateur Web du NOS

11.1.3.1 Redémarrer le NOS en utilisant le CLI du NOS

NOTE : Cette procédure s'applique uniquement aux plateformes équipées du module d'E/S de commutation Ethernet.

NOTE : S'assure que toutes les modifications apportées à la configuration sont enregistrées avant de redémarrer le NOS. Voir Configuration du commutateur.

Voir Accéder au NOS pour les instructions d'accès.

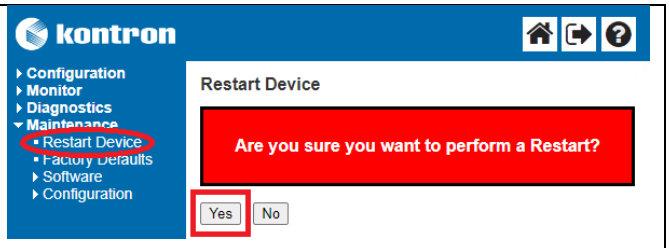
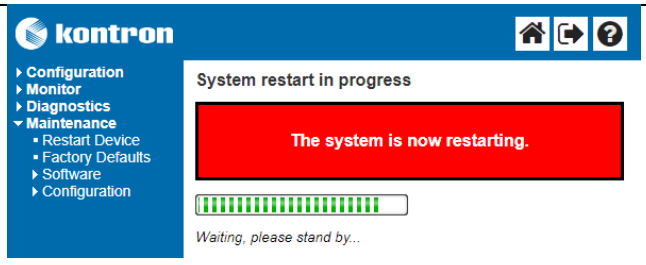
Étape_1	InviteCLI_NOSLocal:~# **reload cold** **NOTE :** Le redémarrage du NOS peut prendre plusieurs secondes.

11.1.3.2 Redémarrer le NOS en utilisant l'interface utilisateur Web du NOS

NOTE : Cette procédure s'applique uniquement aux plateformes équipées du module d'E/S de commutation Ethernet.

NOTE : S'assure que toutes les modifications apportées à la configuration sont enregistrées avant de redémarrer le NOS. Voir Configuration du commutateur.

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

Étape_1	Dans le menu de gauche, sélectionner **Maintenance**, puis **Restart Device**.	
Étape_2	Cliquer sur le bouton **Yes** pour lancer la procédure de redémarrage.	
Étape_3	Attendre que le commutateur soit à nouveau disponible. **NOTE :** Le redémarrage du NOS peut prendre plusieurs secondes.	

11.2 Gestion des sessions BMC

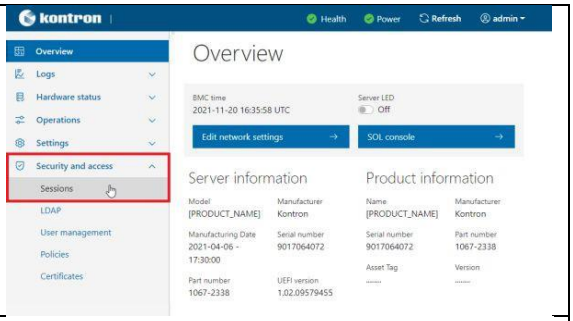
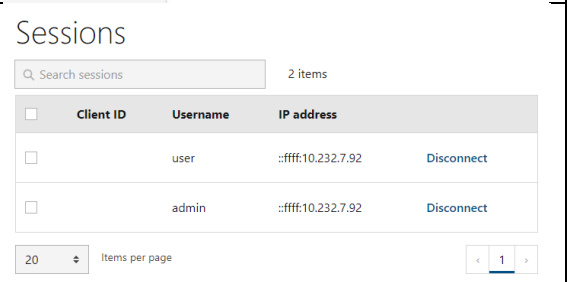
11.2.1 Afficher les sessions BMC

Il est possible d'accéder aux sessions BMC :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish

11.2.1.1 Afficher les sessions BMC 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	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Security and access**, puis sur **Sessions**.	
Étape_2	La liste des sessions s'affiche.	

11.2.1.2 Afficher les sessions BMC en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Afficher la liste des sessions actives avec la commande suivante. Noter l'URL de la session. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET –url [URL_RACINE]/redfish/v1/SessionService/Sessions | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/SessionService/
Sessions | jq
{
  "@odata.id": "/redfish/v1/SessionService/Sessions/",
  "@odata.type": "#SessionCollection.SessionCollection",
  "Description": "Session Collection",
  "Members": [
    {
      "@odata.id": "/redfish/v1/SessionService/Sessions/TzsDHTSiJk"
    },
    {
      "@odata.id": "/redfish/v1/SessionService/Sessions/ppt1YBKbx7"
    }
  ],
  "Members@odata.count": 2,
  "Name": "Session Collection"
}
```

Étape_2	Accéder aux informations d'une session particulière avec de la commande suivante. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/SessionService/Sessions/[URL_SESSION] | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/SessionService/
Sessions/TzsDHTSiJk | jq
{
  "@odata.id": "/redfish/v1/SessionService/Sessions/TzsDHTSiJk",
  "@odata.type": "#Session.v1_3_0.Session",
  "ClientOriginIPAddress": "::ffff:10.232.7.92",
  "Description": "Manager User Session",
  "Id": "TzsDHTSiJk",
  "Name": "User Session",
  "UserName": "user"
}
```

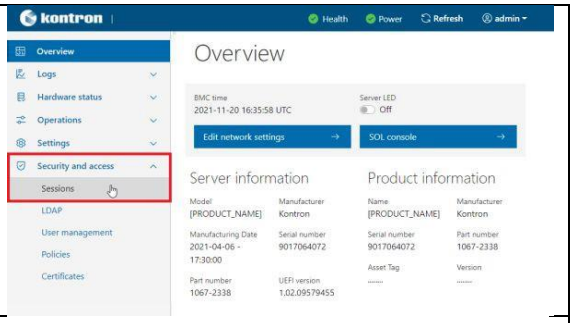
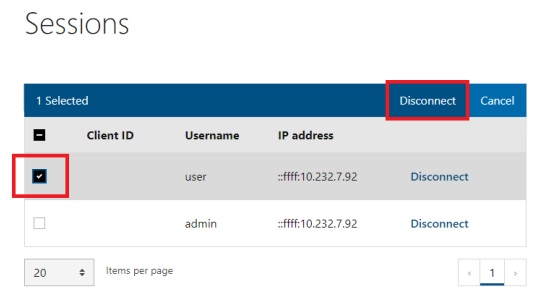
11.2.2 Déconnecter des sessions BMC

Il est possible d'accéder aux sessions BMC :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish

11.2.2.1 Déconnecter des sessions BMC 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	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Security and access**, puis sur **Sessions**.	
Étape_2	Sélectionner la ou les sessions à déconnecter à l'aide des cases à cocher, puis cliquer sur **Disconnect**. **NOTE :** Cette procédure pourrait mettre fin à la session BMC en cours.	

11.2.2.2 Déconnecter une session BMC en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Afficher la liste des sessions actives avec la commande suivante. Noter l'URL de la session à déconnecter. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/SessionService/Sessions | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/SessionService/
Sessions | jq
{
  "@odata.id": "/redfish/v1/SessionService/Sessions/",
  "@odata.type": "#SessionCollection.SessionCollection",
  "Description": "Session Collection",
  "Members": [
    {
      "@odata.id": "/redfish/v1/SessionService/Sessions/TzsDHTSiJk"
    },
    {
      "@odata.id": "/redfish/v1/SessionService/Sessions/ppt1YBKbx7"
    }
  ],
  "Members@odata.count": 2,
  "Name": "Session Collection"
}
```

Étape_2	Effacer la session avec la commande suivante. InviteSE_OrdinateurDistant:~# **curl -k -s --request DELETE --url [URL_RACINE]/redfish/v1/SessionService/Sessions/[URL_SESSION] | jq**

```
$ curl -k -s --request DELETE --url https://admin:ready2go@172.16.182.31/redfish/v1/SessionServi
ce/Sessions/TzsDHTSiJk | jq
{
  "@odata.id": "/redfish/v1/SessionService/Sessions/TzsDHTSiJk",
  "@odata.type": "#Session.v1_3_0.Session",
  "ClientOriginIPAddress": "::ffff:10.232.7.92",
  "Description": "Manager User Session",
  "Id": "TzsDHTSiJk",
  "Name": "User Session",
  "UserName": "user"
}
```

11.2.3 Configurer le délai d'expiration des sessions BMC

Une session BMC sera automatiquement déconnectée une fois le délai d'expiration atteint. Cette valeur peut être modifiée si nécessaire. Le délai d'expiration des sessions BMC par défaut est de 1800 secondes.

Le délai d'expiration des sessions BMC peut seulement être configuré en utilisant Redfish.

11.2.3.1 Configurer le délai d'expiration des sessions BMC en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Afficher la valeur actuelle du délai d'expiration des sessions BMC. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE] /redfish/v1/SessionService | jq.SessionTimeout**
	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/SessionService | jq .SessionTimeout` `1800`
Étape_2	Changer le délai d'expiration des sessions BMC par la nouvelle valeur souhaitée. InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE] /redfish/v1/SessionService --header 'Content- Type:application/json' --data '{"SessionTimeout": [DÉLAI_EXPIRATION]}'| jq**

	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/SessionServic e --header 'Content-Type:application/json' --data '{"SessionTimeout": 3600}' | jq`
	`{`
	`  "SessionTimeOut@Message.ExtendedInfo": [`
	`  {`
	`  "@odata.type": "#Message.v1_1_1.Message",`
	`  "Message": "The property SessionTimeOut was assigned the value 3600 due to modification by the service.",`
	`  "MessageArgs": [`
	`  "SessionTimeOut",`
	`  "3600"`
	`  ],`
	`  "MessageId": "Base.1.8.1.PropertyValueModified",`
	`  "MessageSeverity": "Warning",`
	`  "Resolution": "No resolution is required."`
	`  }`
	`  ]`
	`}`

11.2.4 Authentification Redfish basée sur des jetons

Cette section décrit comment un client HTTPS peut obtenir un jeton d'authentification via l'API Redfish. Dans le guide d'utilisation, l'authentification de base est utilisée afin de simplifier la documentation. Cependant, le codage en dur des noms d'utilisateur et des mots de passe peut devenir un obstacle à la sécurité. Afin d'améliorer la sécurité de la plateforme, il est possible d'utiliser une authentification basée sur un jeton.

L'authentification Redfish basée sur des jetons peut également réduire le temps de réponse du BMC.

11.2.4.1 Préalables

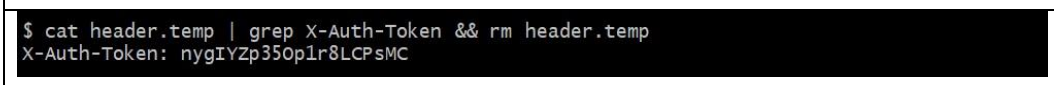
1	L'adresse IP du BMC est connue.
2	Un outil client HTTP est installé sur l'ordinateur distant.

11.2.4.2 Créer un jeton de session

Section pertinente :

Noms d'utilisateur et mots de passe par défaut

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Demander un jeton de session au service de session. L'ID de la session nouvellement créée devrait être affiché. InviteSE_OrdinateurDistant:~$ **curl -k -s --insecure --request POST --url https:// [IP_GESTION_BMC] /redfish/v1/SessionService/Sessions --header 'Content-Type: application/json' --data '{'UserName": "[NOM_UTILISATEUR_BMC]", "Password": "[MOT_DE_PASSE_BMC]"}' --dump-header [NOM_FICHIER] | jq**
	
Étape_2	Extraire le jeton de l'en-tête de réponse du fichier temporaire et le supprimer. InviteSE_OrdinateurDistant:~$ **cat [NOM_FICHIER] | grep X-Auth-Token && rm [NOM_FICHIER]**
	
Étape_3	Vérifier que le jeton est valide en accédant à une ressource Redfish. Ajouter le jeton en tant qu'en-tête supplémentaire. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url https:// [IP_GESTION_BMC] /redfish/v1/UpdateService --header 'X- Auth-Token: [JETON] ' | jq**
	

11.3 Inventaire du système

Voici les informations qui peuvent être collectées pour créer un inventaire du système :

- Données FRU
- Version du micrologiciel du FPGA, de l’UEFI et du BMC
- Type de bloc d'alimentation
- Informations sur le module d’E/S du produit
- Informations sur le processeur
- Configuration des modules de mémoire
- Configuration de l'UEFI/BIOS
- Configuration actuelle du commutateur Ethernet
- Version du commutateur Ethernet

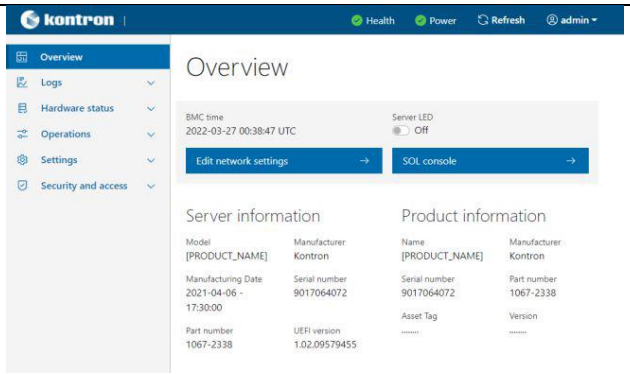
11.3.1 Recueillir les données FRU

Les données FRU peuvent être recueillies :

- En utilisant l’interface utilisateur Web du BMC
- En utilisant Redfish
- En utilisant IPMI

11.3.1.1 Recueillir les données FRU en utilisant l’interface utilisateur Web du BMC

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

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Overview**. Les données FRU s’affichent.	

11.3.1.2 Recueillir les données FRU en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur.

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

Étape_1	Utiliser la commande suivante pour recueillir les données FRU. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/Systems/system | jq ".Manufacturer, .ManufactureDate,.Model,.PartNumber,.ProductManufacturer,.ProductName,.ProductPartNumber,.ProductSerialNumber"**

	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system | jq ".Manufacturer, .ManufactureDate, .Model, .PartNumber, .ProductManufacturer, .ProductName, .ProductPartNumber, .ProductSerialNumber"`
	
	`"Kontron"`
	`"2021-04-06 - 17:30:00"`
	`"ME1310"`
	`"1067-2338"`
	`"Kontron"`
	`"ME1310"`
	`"1067-2338"`
	`"9017064072"`

11.3.1.3 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. 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] -C 17**.

Étape_1	Utiliser la commande suivante pour recueillir les données FRU.
	
	InviteSE_ServeurLocal:~# **ipmitool fru print**
	
	NOTE : Cette commande renvoie tous les périphériques FRU détectés, y compris les cartes d'expansion PCIe avec EEPROM FRU.
		`# ipmitool fru print`
		`FRU Device Description : Builtin FRU Device (ID 0)`
		`Chassis Type : Main Server Chassis`
		`Chassis Part Number : XXXX-XXXX`
		`Chassis Serial : XXXXXXXXXX`
		`Chassis Extra : ME1310`
		`Board Mfg Date : Wed Apr 7 13:30:00 2021`
		`Board Mfg : Kontron`
		`Board Product : ME1310`
		`Board Serial : 9017064072`
		`Board Part Number : 1067-2338`
		`Board Extra : MAC=00:A0:A5:E1:0E:20/07`
		`Product Manufacturer : Kontron`
		`Product Name : ME1310`
		`Product Part Number : 1067-2338`
		`Product Version : ........`
		`Product Serial : 9017064072`
		`Product Asset Tag : ........`
		
		`FRU Device Description : ME1310-PSU-DC (ID 74)`
		`Board Mfg Date : Mon Jun 1 04:00:00 2020`
		`Board Mfg : Kontron`
		`Board Product : ME1310-PSU-DC`
		`Board Serial : 9017067765`
		`Board Part Number : 1067-4309`
		
		`FRU Device Description : ME1310-SW-X (ID 212)`
		`Board Mfg Date : Mon Aug 12 11:55:00 2019`
		`Board Mfg : Kontron`
		`Board Product : ME1310-SW-X`
		`Board Serial : XXXXXXXXXX`
		`Board Part Number : ........`
		`Board Extra : MAC=CC:CC:CC:CC:CC:CC/DD`

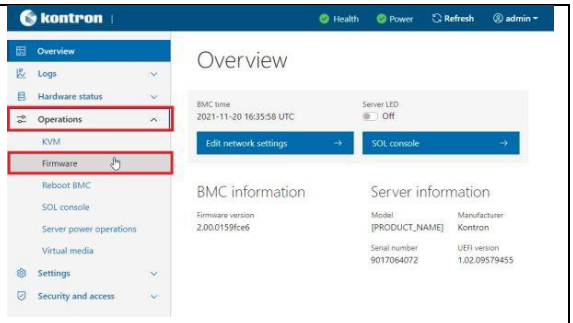
11.3.2 Recueillir la version du micrologiciel du BMC, de l'UEFI et du FPGA

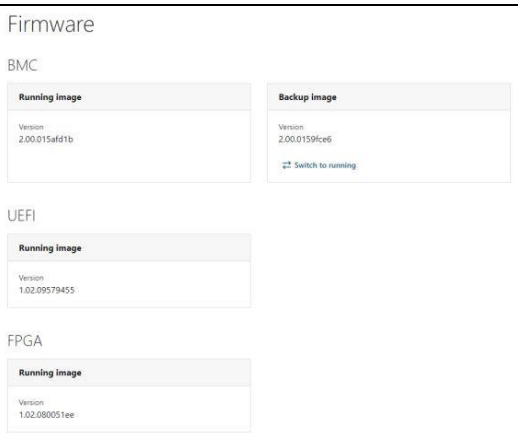
La version du micrologiciel du BMC, de l'UEFI et du FPGA peut être recueillie :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish

11.3.2.1 Recueillir la version du micrologiciel du BMC, de l'UEFI et du FPGA en utilisant l'interface utilisateur Web du BMC

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

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Operations**, puis sur **Firmware**.	

Étape_2	La version du micrologiciel du BMC, de l'UEFI/BIOS et du FPGA sera affichée.	

11.3.2.2 Recueillir la version du micrologiciel du BMC, de l'UEFI et du FPGA en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Recueillir la version actuelle du micrologiciel du BMC avec la commande suivante. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/Managers/bmc | jq.FirmwareVersion**
	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc | jq .FirmwareVersion` `"2.00.0159fce6"`
Étape_2	Obtenir via Redfish la liste des micrologiciels qui se trouvent dans l'inventaire du BMC. Les URL indiqués par la commande ci-dessous seront utilisés à l'étape 3. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE] /redfish/v1/UpdateService/FirmwareInventory | jq**

	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService/FirmwareInventory | jq`
	`{`
	`  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory",`
	`  "@odata.type": "#SoftwareInventoryCollection.SoftwareInventoryCollection",`
	`  "Members": [`
	`  {`
	`  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/8c50fd55"`
	`  },`
	`  {`
	`  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/c172d3d8"`
	`  },`
	`  {`
	`  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/d6bcd2a6"`
	`  },`
	`  {`
	`  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/ebbd5d7b"`
	`  }`
	`  ],`
	`  "Members@odata.count": 4,`
	`  "Name": "Software Inventory Collection"`
	`}`

Étape_3	Pour chaque URL de la liste générée à l'étape 2, exécuter cette commande pour obtenir plus d'informations sur les images du micrologiciel. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE] /redfish/v1/ [URL_DE_ÉTAPE_2] | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService/F
irmwareInventory/d6bcd2a6  | jq
{
  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/d6bcd2a6",
  "@odata.type": "#SoftwareInventory.v1_1_0.SoftwareInventory",
  "Description": "Host image",
  "Id": "d6bcd2a6",
  "Members@odata.count": 1,
  "Name": "Software Inventory",
  "RelatedItem": [
    {
      "@odata.id": "/redfish/v1/Systems/system/Bios"
    }
  ],
  "Status": {
    "Health": "OK",
    "HealthRollup": "OK",
    "State": "Enabled"
  },
  "Updateable": true,
  "Version": "1.02.09579455"
}
```

11.3.3 Recueillir de l'information sur la configuration matérielle

Des informations sur la configuration matérielle peuvent être nécessaires afin d'établir un bon diagnostic de l'état de la carte. La liste suivante contient des exemples d'informations de base qui pourraient aider l'équipe de soutien de Kontron.

- Type de bloc d'alimentation (CA ou CC)
- Configuration de la carte d'E/S de la carte
- Informations sur le processeur
- Configuration des modules de mémoire

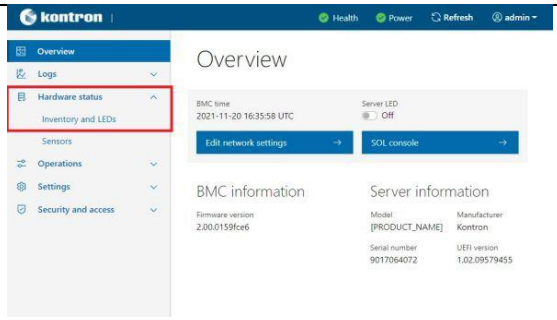
11.3.3.1 Recueillir le type de bloc d'alimentation (CA ou CC)

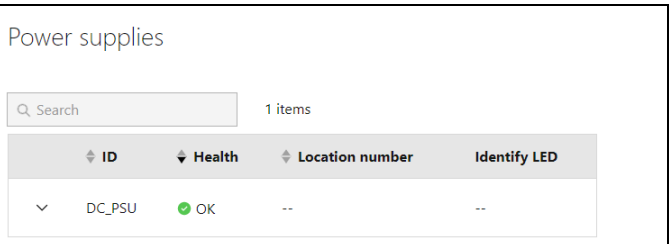
Le type de bloc d'alimentation peut être recueilli :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish
- En utilisant IPMI

11.3.3.1.1 Recueillir le type de bloc d'alimentation en utilisant l'interface utilisateur Web du BMC

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

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Hardware status**, puis sur **Inventory and LEDs**.	

Étape_2	Dans la section **Power supplies**, recueillir le type de bloc d'alimentation.	

11.3.3.1.2 Recueillir le type de bloc d'alimentation en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Recueillir le type de bloc d'alimentation avec la commande suivante. Le type de bloc d'alimentation peut être : DC (CC) ou AC (CA). InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE] /redfish/v1/Chassis/ME1310_Baseboard/Power | jq .PowerSupplies**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Chassis/M
E1310_Baseboard/Power | jq .PowerSupplies
[
  {
    "@odata.id": "/redfish/v1/Chassis/ME1310_Baseboard/Power#/PowerSupplies/0",
    "EfficiencyPercent": 90,
    "Manufacturer": "Kontron",
    "MemberId": "MERS_DC_PSU",
    "Model": "ME1310-PSU-DC",
    "Name": "MERS DC PSU",
    "PartNumber": "1067-4309",
    "PowerOutputWatts": 62,
    "SerialNumber": "9017067765",
    "Status": {
      "Health": "OK",
      "State": "Enabled"
    }
  }
]
```

11.3.3.1.3 Recueillir le type de bloc d'alimentation 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] -C 17**.

Étape_1	Utiliser la commande suivante pour recueillir les données FRU. Le bloc d'alimentation sera dans la liste des périphériques répertoriés par la commande. InviteSE_ServeurLocal:~# **ipmitool fru print** **Types de bloc d'alimentation :** CA : M1877 CC : ME1310-PSU-DC	

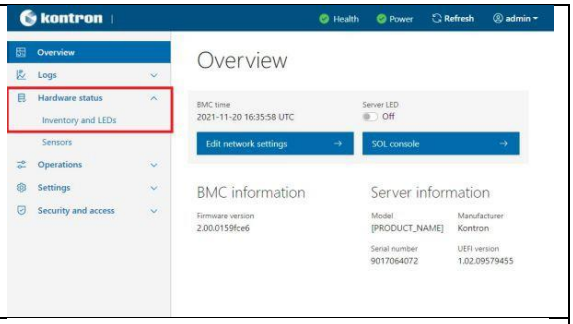
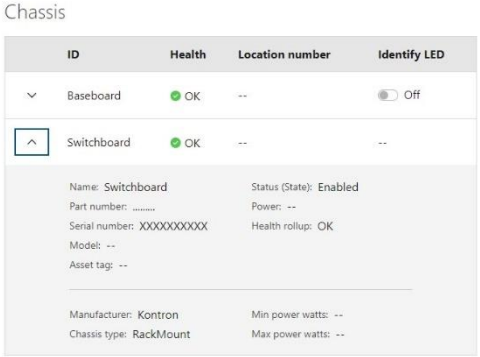
11.3.3.2 Recueillir les informations sur le module d'E/S du produit

Les informations sur le module d'E/S du produit peuvent être recueillies :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish
- En utilisant IPMI

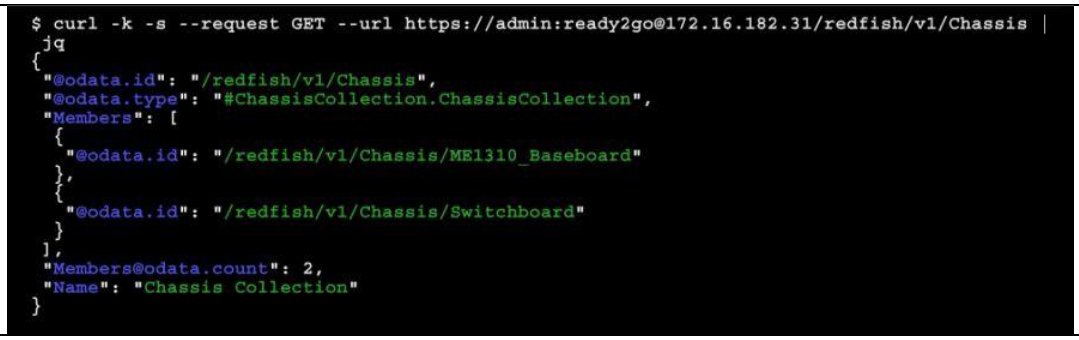
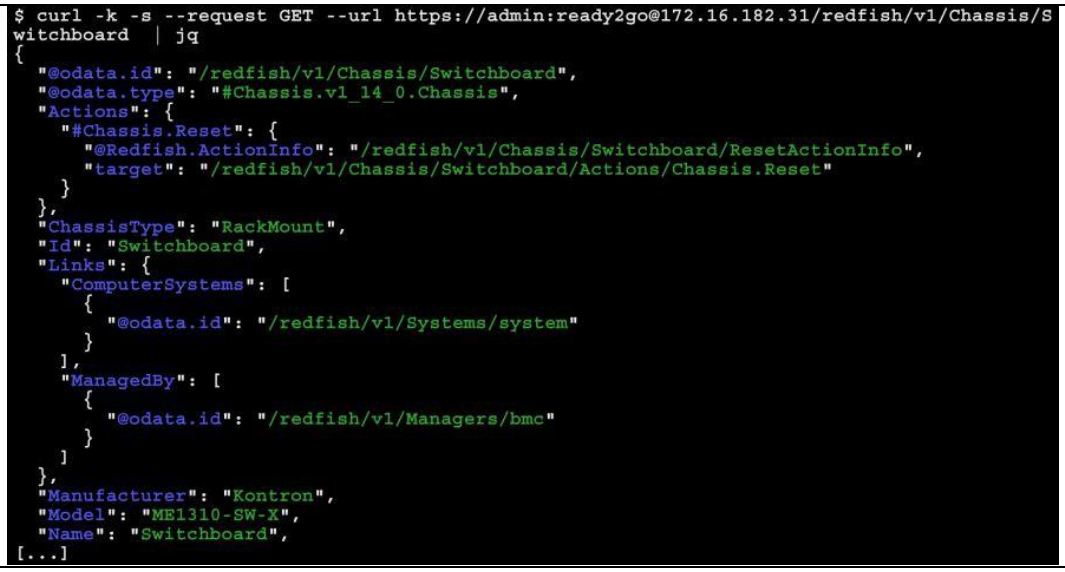
11.3.3.2.1 Recueillir les informations sur le module d'E/S en utilisant l'interface utilisateur Web du BMC

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

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Hardware status**, puis sur **Inventory and LEDs**.	
Étape_2	Dans la section **Chassis**, recueillir les informations sur le module d'E/S. Si nécessaire, développer les informations relatives au module d'E/S en cliquant sur la flèche de gauche.	

11.3.3.2.2 Recueillir les informations sur le module d'E/S du produit en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Afficher le type de module d'E/S avec la commande suivante. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE] /redfish/v1/Chassis | jq**
	
Étape_2	Recueillir les informations sur le module d'E/S avec la commande suivante et l'URL obtenue à l'étape précédente. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE] /redfish/v1/Chassis/[URL_MODULE_ES] | jq**
	

11.3.3.2.3 Recueillir les informations sur le module d'E/S du produit 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] -C 17**.

Étape_1	Utiliser la commande suivante pour recueillir les données FRU. InviteSE_ServeurLocal:~# **ipmitool fru print** **Type de module d'E/S :** Module de commutation Ethernet = ME1310-SW-X Module de connexion directe = ME1310-IOS	

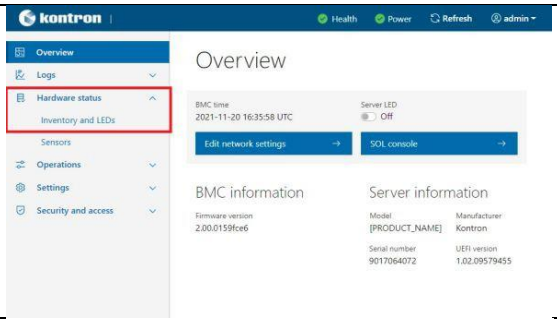
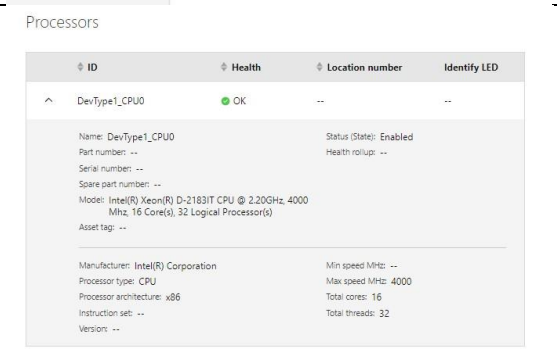
11.3.3.3 Recueillir les informations sur le processeur

Les informations sur le processeur peuvent être recueillies :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish

11.3.3.3.1 Recueillir les informations sur le processeur en utilisant l'interface utilisateur Web du BMC

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

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Hardware status**, puis sur **Inventory and LEDs**.	
Étape_2	Dans la section **Processors**, recueillir les informations sur la configuration du processeur.	

11.3.3.3.2 Recueillir les informations sur le processeur en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Afficher les processeurs avec la commande suivante. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE] /redfish/v1/Systems/system/Processors | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system/
Processors | jq
{
 "@odata.id": "/redfish/v1/Systems/system/Processors",
 "@odata.type": "#ProcessorCollection.ProcessorCollection",
 "Members": [
  {
   "@odata.id": "/redfish/v1/Systems/system/Processors/DevType1_CPU0"
  }
 ],
 "Members@odata.count": 1,
 "Name": "Processor Collection"
}
```

Étape_2	Recueillir les informations sur le processeur avec la commande suivante. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE] /redfish/v1/Systems/system/Processors/[URL_PÉRIPHÉRIQUE] | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system/
Processors/DevType1_CPU0 | jq
{
 "@odata.context": "/redfish/v1/$metadata#Processor.Processor",
 "@odata.id": "/redfish/v1/Systems/system/Processors/DevType1_CPU0",
 "@odata.type": "#Processor.v1_1_0.Processor",
 "CurrentFrequency": 2200,
 "Id": "DevType1_CPU0",
 "Manufacturer": "Intel(R) Corporation",
 "MaxSpeedMHz": 4000,
 "Model": "Intel(R) Xeon(R) D-2183IT CPU @ 2.20GHz, 4000 Mhz, 16 Core(s), 32 Logical Processor(s
)",
 "Name": "DevType1_CPU0",
 "ProcessorArchitecture": "x86",
 "ProcessorId": {
  "EffectiveFamily": "Intel(R) Xeon(R) D-2183IT CPU @ 2.20GHz"
 },
 "ProcessorType": "CPU",
 "Socket": "CPU0",
 "Status": {
  "Health": "OK",
  "State": "Enabled"
 },
[...]
```

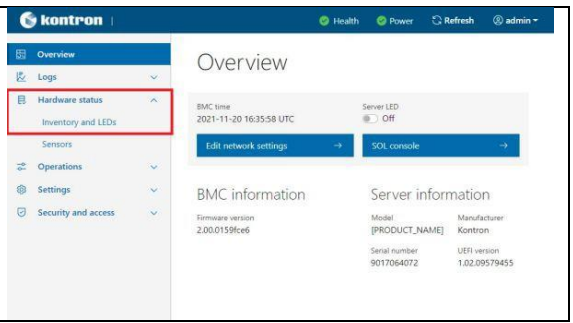
11.3.3.4 Recueillir la configuration des modules de mémoire

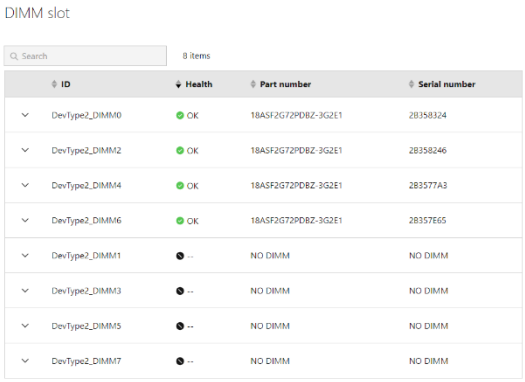
La configuration des modules de mémoire peut être recueillie :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish

11.3.3.4.1 Recueillir la configuration des modules de mémoire en utilisant l'interface utilisateur Web du BMC

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

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Hardware status**, puis sur **Inventory and LEDs**.	

Étape_2	Dans la section **DIMM slot**, recueillir la configuration des modules de mémoire.	

11.3.3.4.2 Recueillir la configuration des modules de mémoire en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Afficher les modules de mémoire avec la commande suivante. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE] /redfish/v1/Systems/system/Memory | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system/Memory | jq
{
 "@odata.context": "/redfish/v1/$metadata#MemoryCollection.MemoryCollection",
 "@odata.id": "/redfish/v1/Systems/system/Memory/",
 "@odata.type": "#MemoryCollection.MemoryCollection",
 "Members": [
  {
   "@odata.id": "/redfish/v1/Systems/system/Memory/DevType2_DIMM0"
  },
  {
   "@odata.id": "/redfish/v1/Systems/system/Memory/DevType2_DIMM1"
  },
  {
   "@odata.id": "/redfish/v1/Systems/system/Memory/DevType2_DIMM2"
  },
  {
   "@odata.id": "/redfish/v1/Systems/system/Memory/DevType2_DIMM3"
  },
  {
   "@odata.id": "/redfish/v1/Systems/system/Memory/DevType2_DIMM4"
  },
  {
   "@odata.id": "/redfish/v1/Systems/system/Memory/DevType2_DIMM5"
  },
  {
   "@odata.id": "/redfish/v1/Systems/system/Memory/DevType2_DIMM6"
  },
  {
   "@odata.id": "/redfish/v1/Systems/system/Memory/DevType2_DIMM7"
  }
 ],
 "Members@odata.count": 8,
 "Name": "Memory Module Collection"
}
```

Étape_2	Recueillir les informations sur les modules de mémoire avec la commande suivante. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE] /redfish/v1/Systems/system/Memory/[URL_PÉRIPHÉRIQUE] | jq**

11.3.4 Recueillir la configuration de l'UEFI/BIOS

La configuration de l'UEFI/BIOS peut seulement être recueillie en utilisant Redfish. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur.

À chaque démarrage, le micrologiciel de l'UEFI/BIOS envoie sa configuration UEFI/BIOS actuelle au BMC. Si l'UEFI/BIOS est configuré à partir d'une autre source (ex. le menu UEFI/BIOS), les options UEFI/BIOS mises à jour sont envoyées automatiquement au BMC.

Étape_1	Obtenir les paramètres actuels de l'UEFI/BIOS. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE] /redfish/v1/Systems/system/Bios | jq.Attributes** **NOTE :** Le résultat de cette commande est assez gros et il peut être plus utile de l'envoyer dans un fichier local. L'option curl **-o, --output [NOM_FICHIER]** peut être utilisée à cet effet.

11.3.5 Recueillir la configuration actuelle du commutateur Ethernet

La configuration actuelle du commutateur Ethernet peut être recueillie :

- En utilisant le CLI du NOS
- En utilisant l'interface utilisateur Web du NOS

11.3.5.1 Recueillir la configuration actuelle du commutateur Ethernet en utilisant le CLI du NOS

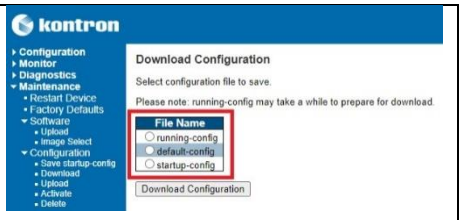
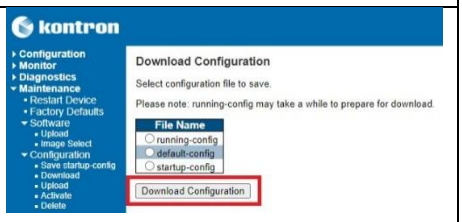
Voir Accéder au NOS pour les instructions d'accès.

Étape_1	Accéder au système d'exploitation réseau du commutateur en utilisant SSH ou une connexion série.
Étape_2	Copier la configuration souhaitée sur le serveur distant. • **running-config** : configuration actuellement active (peut différer de startup-config si des modifications ont été apportées depuis le dernier démarrage, mais n'ont pas été sauvegardées). • **startup-config** : configuration sauvegardée appliquée au démarrage du commutateur. InviteCLI_NOSLocal:~# **copy <running-config|startup-config> scp://<NOM_UTILISATEUR_SERVEUR>:<MOT_DE_PASSE_SERVEUR>@<IP_SERVEUR>/<CHEMIN_ACCÈS_FICHIER> save-host-key**

```
# copy startup-config scp://user:password@192.168.0.10/
startup-config save-host-key
% Saving 1506 bytes to server 192.168.0.10: startup-config
```

11.3.5.2 Recueillir la configuration actuelle du commutateur Ethernet en utilisant l'Interface utilisateur Web du NOS

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

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du NOS, cliquer sur **Maintenance**, sur **Configuration**, puis sur **Download**. Choisir la configuration à sauvegarder : • **running-config** : configuration actuellement active (peut différer de startup-config si des modifications ont été apportées depuis le dernier démarrage, mais n'ont pas été sauvegardées). • **default-config** : configuration appliquée lorsque la configuration par défaut est rechargée. • **startup-config** : configuration sauvegardée appliquée au démarrage du commutateur.	
Étape_2	Cliquer sur **Download Configuration**, puis sélectionner l'endroit où enregistrer le fichier de configuration.	

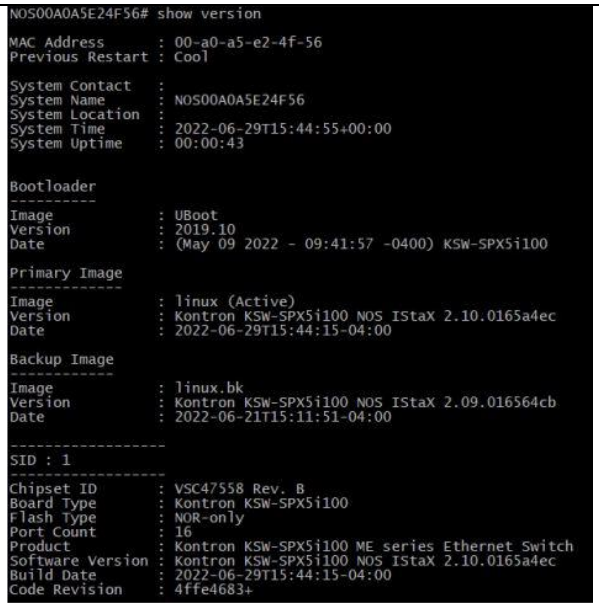
11.3.6 Recueillir la version du micrologiciel du commutateur Ethernet

La version du micrologiciel du commutateur Ethernet peut être recueillie :

- En utilisant le CLI du NOS
- En utilisant l'interface utilisateur Web du NOS

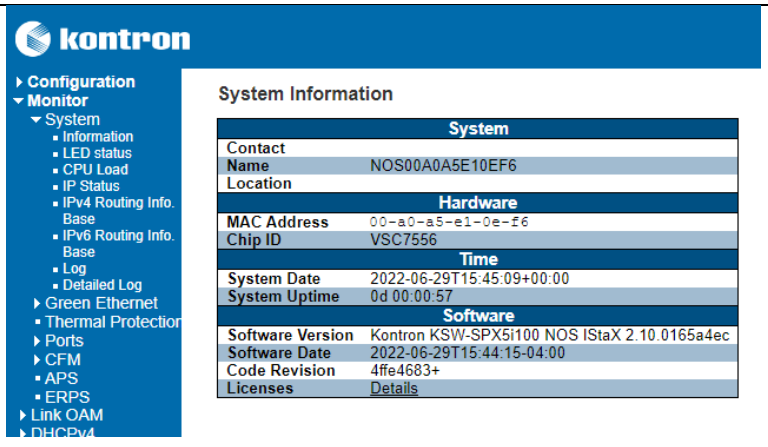
11.3.6.1 Recueillir la version du micrologiciel du commutateur Ethernet en utilisant le CLI du NOS

Voir Accéder au NOS pour les instructions d'accès.

Étape_1	Afficher les versions. InviteCLI_NOSLocal:~# **show version**	

11.3.6.2 Recueillir la version du micrologiciel du commutateur Ethernet en utilisant l'interface utilisateur Web du NOS

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

Étape_1	Dans le menu de gauche, sélectionner **Monitor**, **System**, puis **Information**.	

11.4 Surveillance

11.4.1 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 peuvent être classés en deux catégories et les deux types sont décrits dans la liste des capteurs :

- Capteurs associés à une unité de mesure – utiliser la procédure de surveillance générale
- Capteurs discrets – utiliser la procédure de surveillance des capteurs discrets

11.4.1.1 Procédure de surveillance générale pour les capteurs associés à une unité de mesure

Les capteurs de la plateforme peuvent être surveillés :

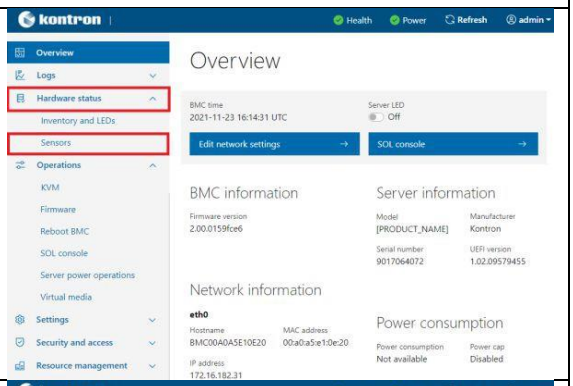
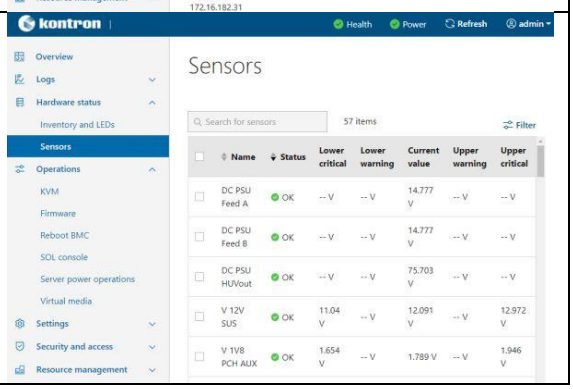
- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish
- En utilisant IPMI

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.

11.4.1.1.1 Surveiller les capteurs 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.	
Étape_2	Dans le menu de gauche, cliquer sur **Hardware status**, puis sur **Sensors**.	
Étape_3	La liste des capteurs s'affiche. Faire défiler vers le bas pour voir la liste des capteurs ou utiliser la barre de recherche dédiée pour filtrer les capteurs.	

11.4.1.1.2 Surveiller les capteurs en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

11.4.1.1.2.1 Créer des extensions URL

Pour une liste de toutes les extensions URL, voir Liste des capteurs. Ce tableau présente les principales catégories de capteurs et leur emplacement.

Type	**Extensions URL**	**Arguments de l'analyseur**
Capteurs des ventilateurs	Chassis/ ME1310_Baseboard /Thermal	| jq ".Fans"
Capteurs de température (y compris les capteurs du bloc d'alimentation)	Chassis/ ME1310_Baseboard /Thermal	| jq ".Temperatures"
Capteurs de tension (y compris les capteurs du bloc d'alimentation)	Chassis/ ME1310_Baseboard /Power	| jq ".Voltages"

Type	Extensions URL	Arguments de l'analyseur
Capteurs d'alimentation (y compris les capteurs du bloc d'alimentation)	Chassis/ ME1310_Baseboard /Sensors	| jq
Autres capteurs associés à une unité de mesure	Chassis/ ME1310_Baseboard /Sensors	| jq
Capteurs discrets	Managers/bmc	| jq ".Oem.Kontron.Discrete"
Capteurs du module d'E/S de connexion directe	Chassis/IOBoard/Thermal	| jq ".Temperatures"
Capteurs du module d'E/S de commutation Ethernet	Chassis/Switchboard/Thermal	| jq ".Temperatures"

11.4.1.1.2.2 Afficher les détails 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 --request GET --url [URL_RACINE]/redfish/v1/[EXTENSION_URL] [ARGUMENT_ANALYSEUR]**

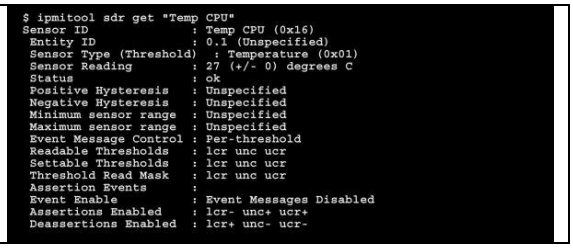
```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Chassis/ME1310_
Baseboard/Thermal | jq ".Fans"

  "Fans": [
    {
      "@odata.id": "/redfish/v1/Chassis/ME1210_Baseboard/Thermal#/Fans/0",
      "@odata.type": "#Thermal.v1_3_0.Fan",
      "MaxReadingRange": 27000,
      "MemberId": "Fan_1",
      "MinReadingRange": 0,
      "Name": "Fan 1",
      "Oem": {
        "RunningTime": 8387014.545065252
      },
      "Reading": 12321,
      "ReadingUnits": "RPM",
      "Status": {
        "Health": "OK",
        "State": "Enabled"
      }
    },
    {
      "@odata.id": "/redfish/v1/Chassis/ME1210_Baseboard/Thermal#/Fans/1",
      "@odata.type": "#Thermal.v1_3_0.Fan",
      "MaxReadingRange": 27000,
      "MemberId": "Fan_2",
      "MinReadingRange": 0,
      "Name": "Fan 2",
      "Oem": {
        "RunningTime": 8387016.783241839
      },
      "Reading": 12321,
      "ReadingUnits": "RPM",
      "Status": {
        "Health": "OK",
        "State": "Enabled"
      }
    }
    [...]
```

11.4.1.1.3 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. 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] -C 17**.

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**	

```
$ ipmitool sensor
Fan 1             | 10600.000  | RPM         | ok  | na  | na          | na
Fan 2             | 10494.000  | RPM         | ok  | na  | na          | na
Fan 3             | 10918.000  | RPM         | ok  | na  | na          | na
Fan 4             | 11130.000  | RPM         | ok  | na  | na          | na
Fan 5             | 10918.000  | RPM         | ok  | na  | na          | na
Fan 6             | 10494.000  | RPM         | ok  | na  | na          | na
Fan 7             | 10918.000  | RPM         | ok  | na  | na          | na
Fan 8             | 10600.000  | RPM         | ok  | na  | na          | na
Temp BMC          | 27.000     | degrees C   | ok  | na  | -41.000     | na
Temp CPU          | 28.000     | degrees C   | ok  | na  | -41.000     | na
Temp CPU Area     | 30.000     | degrees C   | ok  | na  | -41.000     | na
[...]
```

Étape_2	Utiliser la commande sdr pour obtenir plus de détails sur un capteur particulier. InviteSE_ServeurLocal:~# **ipmitool sdr get [ID_CAPTEUR]**	

11.4.1.2 Procédure de surveillance des capteurs discrets

Cette section décrit les comportements spécifiques et les méthodes de surveillance des capteurs discrets de la plateforme. La plateforme est équipée des capteurs discrets suivants :

- Board Reset
- Heater CPU, Heater PCIe1, Heater PCIe2
- Intrusion
- IPMIWatchdog
- Jumpers Status
- TelcoAlarm1-7

11.4.1.2.1 Capteur Board Reset

Le capteur Board Reset consigne la cause de la dernière réinitialisation dans le journal des événements système.

Sections pertinentes :

Liste des capteurs

Journal des événements système

11.4.1.2.1.1 Valeurs possibles (IPMI uniquement)

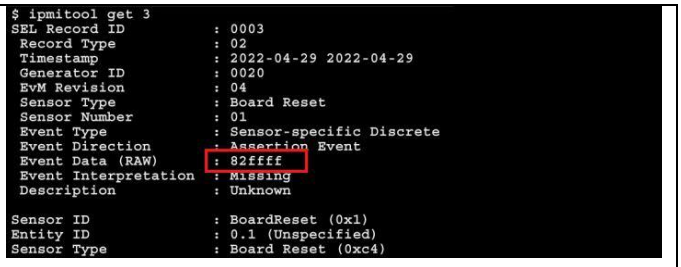
La cause de la dernière réinitialisation de la carte peut seulement être trouvée dans les entrées du journal des événements système.

Décalage de l'événement (event offset)	Description
0x01	Perte d'alimentation inattendue
0x02	Cycle d'alimentation ou réinitialisation du port série
0x06	Réinitialisation à froid
0x07	Réinitialisation de l'alimentation à partir d'une commande IPMI

11.4.1.2.1.2 Surveiller la réinitialisation de la carte 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] -C 17**.

Étape_1	Accéder au journal des événements système et identifier l'ID de l'événement souhaité dans la première colonne. InviteSE_ServeurLocal:~# **ipmitool sel list**	

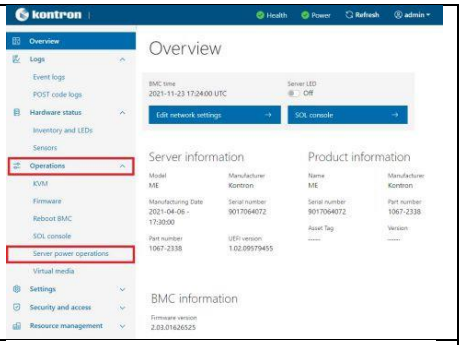
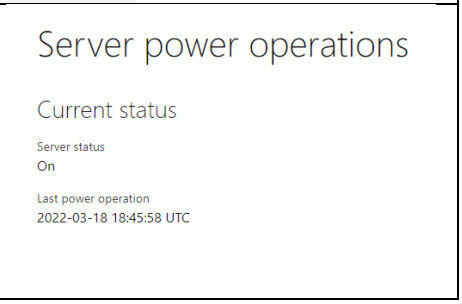
Étape_2	Afficher les détails de l'entrée du journal des événements système. InviteSE_ServeurLocal:~# **ipmitool get [ID]** La valeur est représentée par l'octet de plus fort poids de la valeur du paramètre **Event Data (RAW)**. Noter que le bit 7 de l'octet de plus fort poids est réservé et toujours égal à 1 (ou 0x8 en hexadécimal). Consulter la liste des valeurs possibles.	

11.4.1.2.1.3 Surveiller la date et l'heure de la dernière réinitialisation

La date et l'heure de la dernière réinitialisation peuvent être trouvées en utilisant l'interface utilisateur Web du BMC et Redfish.

11.4.1.2.1.3.1 Surveiller la date et l'heure de la dernière réinitialisation 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	Dans le menu de gauche, cliquer sur **Operations**, puis sur **Server power operations** ou cliquer simplement sur l'icône d'état **Power** en haut de la page.	
Étape_2	La date et l'heure de la dernière action liée à l'alimentation s'affichent.	

11.4.1.2.1.3.2 Surveiller la date et l'heure de la dernière réinitialisation en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/ Systems/system | jq.LastResetTime**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1
/Systems/system | jq .LastResetTime
"2022-03-18T18:45:58+00:00"
```

11.4.1.2.2 Capteurs de chauffage

Le BMC enregistre les événements indiquant un changement d'état du chauffage. Trois capteurs de chauffage sont présents dans la plateforme :

- Heater CPU
- Heater PCIe1 (optionnel)
- Heater PCIe2 (optionnel)

Pour plus d'informations sur le chauffage PCIe, contacter l'équipe de soutien de Kontron. Voir Obtenir du soutien.

Sections pertinentes :

Refroidissement et gestion thermique de la plateforme – Comportement au démarrage à des températures inférieures à 0 degré Celsius

Liste des capteurs

11.4.1.2.2.1 Valeurs possibles

Valeur	Description
0	Périphérique désactivé
1	Périphérique activé

11.4.1.2.2.2 Surveiller les périphériques de chauffage en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

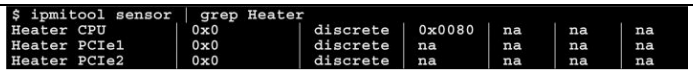
NOTE : Redfish ne rapporte pas la présence de périphériques de chauffage.

Étape_1	Afficher les états des périphériques de chauffage avec la commande suivante. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/ Managers/bmc | jq.Oem.Kontron.Discrete**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1
/Managers/bmc | jq .Oem.Kontron.Discrete
{
    "Heater_CPU": "0",
    "Heater_PCIe1": "0",
    "Heater_PCIe2": "0",
    "Jumpers_Status": {
        "JMP1 (JPx p1-2)": "?",
        "JMP2 (JPx p3-4)": "OUT",
        "JMP3 (JPx p5-6)": "OUT",
        "JMP4 (JPx p7-8)": "OUT",
        "JMP5 (JPx p9-10)": "OUT",
        "JMP6 (JPx p11-12)": "OUT",
        "JMP7 (JPx p13-14)": "OUT"
    },
    "TelcoAlarm1": "1",
    "TelcoAlarm2": "1",
    "TelcoAlarm3": "1",
    "TelcoAlarm4": "1"
}
```

11.4.1.2.2.3 Surveiller les périphériques de chauffage 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] -C 17**.

Étape_1	Afficher les états des périphériques de chauffage avec la commande suivante. InviteSE_ServeurLocal:~# **ipmitool sensor | grep Heater** La valeur est représentée par le deuxième octet en partant de la gauche dans la quatrième colonne. Valeurs possibles : • 0x0080 si le périphérique de chauffage est désactivé • 0x0180 si le périphérique de chauffage est activé • na si aucun périphérique de chauffage n'est présent	

11.4.1.2.3 Capteur Intrusion

Le capteur d'intrusion du châssis consigne un événement si le châssis est ouvert. Ce capteur doit être désenclenché manuellement.

Sections pertinentes :

Liste des capteurs

Journal des événements système

11.4.1.2.3.1 Enclenchement d'un événement

Le capteur d'intrusion du châssis consigne un événement dans les circonstances suivantes :

- Lorsque le châssis est ouvert – le BMC consigne un événement critique d'intrusion dans le châssis dans le journal des événements système.
- Lorsque le capteur d'intrusion du châssis est désenclenché manuellement – le BMC consigne un événement de réinitialisation de l'intrusion dans le châssis dans le journal des événements système.

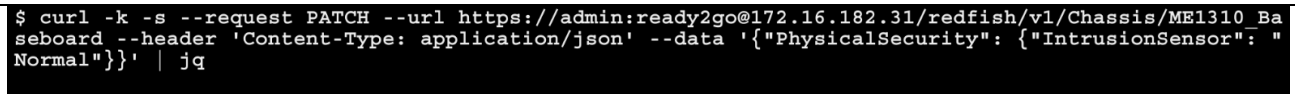
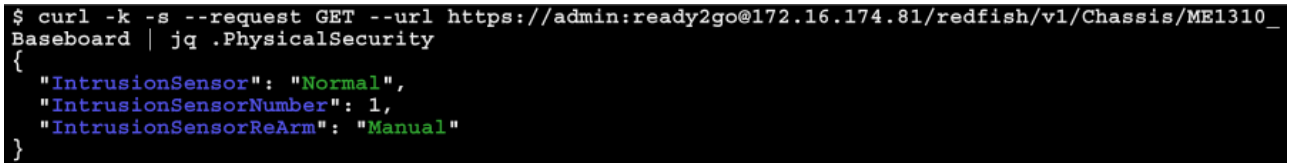
11.4.1.2.3.2 Désenclenchement d'un événement

Ce capteur doit être désenclenché manuellement. En cas d'intrusion dans le châssis, l'état du capteur doit être réinitialisé manuellement. Redfish est le seul moyen pris en charge pour le désenclenchement d'un événement.

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur.

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

Étape_1	Modifier manuellement la valeur du capteur avec la commande suivante : InviteSE_OrdinateurDistant:~# **curl -k -s --request PATCH --url [URL_RACINE]/redfish/v1/Chassis/ME1310_Baseboard --header 'Content-Type: application/json' --data '{"PhysicalSecurity": {"I ntrusionSensor": "Normal"}}' | jq**

	
Étape_2	Vérifiez l'état du capteur en utilisant la commande suivante. S'il montre toujours « HardwareIntrusion », cela signifie qu'une des portes n'est toujours pas correctement fermée et il faut effectuer l'Étape_3. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Chassis/RS1310_Baseboard | jq .PhysicalSecurity** 
Étape_3	Assurez-vous que les deux portes sont correctement fermées et effectuez l'Étape_1 puis l'Étape_2 à nouveau jusqu'à ce que le statut soit **normal**.

NOTE : À partir de la version actuelle du micrologiciel du BMC, l'état de santé du BMC sera critique tant que des événements critiques sont enregistrés dans le journal des événements système. Actuellement, le seul moyen de restaurer l'état de santé du BMC consiste à vider le journal des événements système. Voir Journal des événements système pour des instructions. Il est recommandé d'exporter au préalable toutes les entrées du journal des événements système.

11.4.1.2.4 Capteur IPMIWatchdog

Le capteur IPMIWatchdog consigne un événement critique dans le journal des événements système lorsqu'il expire parce qu'une erreur empêche la plateforme de démarrer correctement.

Sections pertinentes :

Liste des capteurs

Journal des événements système

11.4.1.2.5 Capteur Jumpers Status

> Les valeurs du capteur Jumpers Status sont réservées et ne doivent jamais différer des valeurs par défaut indiquées ci-dessous. Si ce n'est pas le cas, la plateforme pourrait être inutilisable.

Section pertinente :

Liste des capteurs

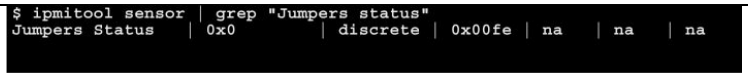
11.4.1.2.5.1 Surveiller le capteur Jumpers Status en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Afficher les valeurs du capteur Jumpers Status avec la commande suivante. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/ Managers/bmc | jq.Oem.Kontron.Discrete**

11.4.1.2.5.2 Surveiller le capteur Jumpers Status 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] -C 17**.

Étape_1	Afficher la valeur du capteur Jumpers Status avec la commande suivante. InviteSE_ServeurLocal:~# **ipmitool sensor | grep "Jumpers Status"** La valeur est représentée par les octets dans la quatrième colonne. La valeur doit toujours être **0x00fe**.	

11.4.1.2.6 Capteurs TelcoAlarm

Les capteurs TelcoAlarm sont des contacts secs normalement fermés entre un signal d'entrée d'alarme et le signal commun d'alarme. Ces signaux sont situés sur le connecteur du port d'alarme. Le BMC consignera un événement indiquant un changement d'état. Voir Brochage et caractéristiques électriques des connecteurs.

NOTE : Si aucun contact normalement fermé n'est connecté au panneau avant, le BMC consignera un événement critique dans le journal des événements système à chaque redémarrage, car il supposera qu'il détecte du matériel défectueux ou un fil coupé. Voir Journal des événements système pour une description de ce qui se passe dans le SEL au redémarrage pour les alarmes TelcoAlarm.

Sept capteurs TelcoAlarm sont présents dans la plateforme :

- TelcoAlarm1
- TelcoAlarm2
- TelcoAlarm3
- TelcoAlarm4
- TelcoAlarm5
- TelcoAlarm6
- TelcoAlarm7

Sections pertinentes :

Liste des capteurs

Journal des événements système

11.4.1.2.6.1 Surveiller les capteurs TelcoAlarm en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Afficher les états des capteurs TelcoAlarm avec la commande suivante. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/ Managers/bmc | jq.Oem.Kontron.Discrete** Valeurs possibles : • 0 pour un contact fermé • 1 pour un contact ouvert

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1
/Managers/bmc | jq .Oem.Kontron.Discrete
{
    "Heater_CPU": "0",
    "Heater_PCIe1": "0",
    "Heater_PCIe2": "0",
    "Jumpers_Status": {
        "JMP1 (JPx p1-2)": "?",
        "JMP2 (JPx p3-4)": "OUT",
        "JMP3 (JPx p5-6)": "OUT",
        "JMP4 (JPx p7-8)": "OUT",
        "JMP5 (JPx p9-10)": "OUT",
        "JMP6 (JPx p11-12)": "OUT",
        "JMP7 (JPx p13-14)": "OUT"
    },
    "TelcoAlarm1": "1",
    "TelcoAlarm2": "1",
    "TelcoAlarm3": "1",
    "TelcoAlarm4": "1",
    "TelcoAlarm5": "1",
    "TelcoAlarm6": "1",
    "TelcoAlarm7": "1"
}
```

11.4.1.2.6.2 Surveiller les capteurs TelcoAlarm 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] -C 17**.

Étape_1	Afficher les états des capteurs TelcoAlarm avec la commande suivante. InviteSE_ServeurLocal:~# **ipmitool sensor | grep TelcoAlarm** La valeur est représentée par le deuxième octet en partant de la gauche dans la quatrième colonne. Valeurs possibles : • 0x0080 pour un contact fermé • 0x0180 pour un contact ouvert	

```
$ ipmitool sensor | grep TelcoAlarm
TelcoAlarm1      | 0x0   | discrete | 0x0180 | na | na | na
TelcoAlarm2      | 0x0   | discrete | 0x0180 | na | na | na
TelcoAlarm3      | 0x0   | discrete | 0x0180 | na | na | na
TelcoAlarm4      | 0x0   | discrete | 0x0180 | na | na | na
TelcoAlarm5      | 0x0   | discrete | 0x0180 | na | na | na
TelcoAlarm6      | 0x0   | discrete | 0x0180 | na | na | na
TelcoAlarm7      | 0x0   | discrete | 0x0180 | na | na | na
```

11.4.1.2.6.3 Enclenchement d'un événement

Le capteur TelcoAlarm consigne un événement dans les circonstances suivantes :

- Lorsqu'une entrée TelcoAlarm passe de fermée à ouverte – le BMC consigne un événement TelcoAlarm critique dans le journal des événements système.
- Lorsqu'une entrée TelcoAlarm passe d'ouverte à fermée – le BMC consigne un événement de restauration TelcoAlarm dans le journal des événements système, mais il est important de noter qu'un événement de restauration ne désenclenche pas un événement TelcoAlarm critique.

11.4.1.2.6.4 Désenclenchement d'un événement

Cet événement ne peut pas être désenclenché.

NOTE : À partir de la version actuelle du micrologiciel du BMC, l'état de santé du BMC sera critique tant que des événements critiques sont enregistrés dans le journal des événements système. Actuellement, le seul moyen de restaurer l'état de santé du BMC consiste à vider le journal des événements système. Voir Journal des événements système pour des instructions. Il est recommandé d'exporter au préalable toutes les entrées du journal des événements système.

11.4.2 Liste des capteurs

Voir Surveillance des capteurs pour des instructions de surveillance.

Pour les extensions URL Redfish, voir Surveiller des capteurs en utilisant Redfish – Créer des extensions URL.

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.

11.4.2.1 Capteurs du ME1310

Les capteurs du ME1310 sont toujours présents, quelle que soit la configuration matérielle de la plateforme.

11.4.2.1.1 Capteurs associés à une unité de mesure

11.4.2.1.1.1 Capteurs des ventilateurs

Nom du capteur [ID_CAPTEUR]	Description	Code de type de capteur	Code de type d'événement/de lecture
Fan 1	Vitesse du ventilateur 1 (tr/min)	Fan (0x04)	0x01 (Threshold Based)
Fan 2	Vitesse du ventilateur 2 (tr/min)	Fan (0x04)	0x01 (Threshold Based)
Fan 3	Vitesse du ventilateur 3 (tr/min)	Fan (0x04)	0x01 (Threshold Based)
Fan 4	Vitesse du ventilateur 4 (tr/min)	Fan (0x04)	0x01 (Threshold Based)
Fan 5	Vitesse du ventilateur 5 (tr/min)	Fan (0x04)	0x01 (Threshold Based)
Fan 6	Vitesse du ventilateur 6 (tr/min)	Fan (0x04)	0x01 (Threshold Based)
Fan 7	Vitesse du ventilateur 7 (tr/min)	Fan (0x04)	0x01 (Threshold Based)
Fan 8	Vitesse du ventilateur 8 (tr/min)	Fan (0x04)	0x01 (Threshold Based)

11.4.2.1.1.2 Capteurs de température

Nom du capteur [ID_CAPTEUR]	Description	Code de type de capteur	Code de type d'événement/de lecture
Temp CPU	Température interne du CPU	Temperature (0x01)	0x01 (Threshold Based)
Temp BMC	Température sous le BMC	Temperature (0x01)	0x01 (Threshold Based)

Nom du capteur [ID_CAPTEUR]	Description	Code de type de capteur	Code de type d'événement/de lecture
Temp CPU Area	Température sous le CPU	Temperature (0x01)	0x01 (Threshold Based)
Temp Chassis	Température de la thermistance du châssis Voir Installer une sonde thermique pour la carte d'expansion PCIe pour l'emplacement de la sonde thermique.	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMA1	Température du module DIMM 1 sur le canal A	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMA2	Température du module DIMM 2 sur le canal A	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMB1	Température du module DIMM 1 sur le canal B	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMC1	Température du module DIMM 1 sur le canal C	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMC2	Température du module DIMM 2 sur le canal C	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMD1	Température du module DIMM 1 sur le canal D	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMD2	Température du module DIMM 2 sur le canal D	Temperature (0x01)	0x01 (Threshold Based)
Temp FPGA	Température sous le FPGA	Temperature (0x01)	0x01 (Threshold Based)
Temp Inlet	Température à l'entrée d'air frais	Temperature (0x01)	0x01 (Threshold Based)
Temp M2 Area	Température près de M.2 J8 et J9	Temperature (0x01)	0x01 (Threshold Based)
Temp PCIe 1	Température de la thermistance de l'emplacement PCIe 1 Voir Installer une sonde thermique pour la carte d'expansion PCIe pour l'emplacement de la sonde thermique.	Temperature (0x01)	0x01 (Threshold Based)
Temp PCIe 1 mbox	Température de l'emplacement PCIe 1 rapportée via un registre (mailbox) Voir Ressources de la plateforme destinées à l'application client – Capteurs de température propres aux clients pour les instructions relatives à la consignation de températures.	Temperature (0x01)	0x01 (Threshold Based)
Temp PCIe 2	Température de la thermistance de l'emplacement PCIe 2 Voir Installer une sonde thermique pour la carte d'expansion PCIe pour l'emplacement de la sonde thermique.	Temperature (0x01)	0x01 (Threshold Based)
Temp PCIe 2 mbox	Température de l'emplacement PCIe 2 rapportée via un registre (mailbox) Voir Ressources de la plateforme destinées à l'application client – Capteurs de température propres aux clients pour les instructions relatives à la consignation de températures.	Temperature (0x01)	0x01 (Threshold Based)
Temp PSU Outlet	Température à la sortie du bloc d'alimentation du système	Temperature (0x01)	0x01 (Threshold Based)
Temp VCCIN	Température près du régulateur VCCIN	Temperature (0x01)	0x01 (Threshold Based)

Nom du capteur [ID_CAPTEUR]	Description	Code de type de capteur	Code de type d'événement/de lecture
Temp VDDQ_AB	Température près du régulateur VDDQ_AB	Temperature (0x01)	0x01 (Threshold Based)
Temp VDDQ_CD	Température près du régulateur VDDQ_CD	Temperature (0x01)	0x01 (Threshold Based)
Temp V_3V3_SUS	Température près du régulateur V_3V3_SUS	Temperature (0x01)	0x01 (Threshold Based)

11.4.2.1.1.3 Capteurs de tension

Nom du capteur [ID_CAPTEUR]	Description	Code de type de capteur	Code de type d'événement/de lecture
VBAT	Tension de la pile de l'horloge temps réel	Voltage (0x02)	0x01 (Threshold Based)
V_3V3_M2	Tension V_3V3_M2	Voltage (0x02)	0x01 (Threshold Based)
V_3V3_PCH_AUX	Tension V_3V3_PCH_AUX	Voltage (0x02)	0x01 (Threshold Based)
V_3V3_RGM_BMC	Tension V_3V3_RGM_BMC	Voltage (0x02)	0x01 (Threshold Based)
V_3V3_SLOT	Tension V_3V3_SLOT	Voltage (0x02)	0x01 (Threshold Based)
V_12V_SLOT1	Tension V_12V_SLOT1	Voltage (0x02)	0x01 (Threshold Based)
V_12V_SLOT2	Tension V_12V_SLOT2	Voltage (0x02)	0x01 (Threshold Based)
V_12V_SUS	Tension V_12V_SUS	Voltage (0x02)	0x01 (Threshold Based)
V_VTT_AB	Tension V_VTT_AB	Voltage (0x02)	0x01 (Threshold Based)
V_VTT_CD	Tension V_VTT_CD	Voltage (0x02)	0x01 (Threshold Based)

11.4.2.1.1.4 Capteurs d'alimentation

Nom du capteur [ID_CAPTEUR]	Description	Code de type de capteur	Code de type d'événement/de lecture
P_12V_SLOT1	Puissance consommée V_12V_SLOT1	Power Supply (0x08)	0x01 (Threshold Based)
P_12V_SLOT2	Puissance consommée V_12V_SLOT2	Power Supply (0x08)	0x01 (Threshold Based)

11.4.2.1.1.5 Autres capteurs associés à une unité de mesure

Nom du capteur [ID_CAPTEUR]	Description	Code de type de capteur	Code de type d'événement/de lecture
Humidité	Humidité relative à l'entrée d'air	Other Units-based sensor (0x0B)	0x01 (Threshold Based)

11.4.2.1.2 Capteurs discrets

Pour plus d'information sur les capteurs discrets, voir Procédure de surveillance des capteurs discrets.

Nom du capteur [ID_CAPTEUR]	Description	Code de type de capteur	Code de type d'événement/de lecture
Heater CPU	Indicateur d'état du chauffage pour le CPU	Chassis (0x18)	0x9 ('digital' Discrete - Device Disabled/Device Enabled)
Heater PCIe1	Indicateur d'état du chauffage pour PCIe1	Chassis (0x18)	0x9 ('digital' Discrete - Device Disabled/Device Enabled)
Heater PCIe2	Indicateur d'état du chauffage pour PCIe2	Chassis (0x18)	0x9 ('digital' Discrete - Device Disabled/Device Enabled)
Intrusion	État de l'alarme du connecteur du panneau avant	Platform Alert (0x24)	0x3 (‘digital’ Discrete - Assert/Deassert)
TelcoAlarm1	État du connecteur d'alarme du panneau avant	Platform Alert (0x24)	0x3 (‘digital’ Discrete - Assert/Deassert)
TelcoAlarm2	État du connecteur d'alarme du panneau avant	Platform Alert (0x24)	0x3 (‘digital’ Discrete - Assert/Deassert)
TelcoAlarm3	État du connecteur d'alarme du panneau avant	Platform Alert (0x24)	0x3 (‘digital’ Discrete - Assert/Deassert)
TelcoAlarm4	État du connecteur d'alarme du panneau avant	Platform Alert (0x24)	0x3 (‘digital’ Discrete - Assert/Deassert)
TelcoAlarm5	État du connecteur d'alarme du panneau avant	Platform Alert (0x24)	0x3 (‘digital’ Discrete - Assert/Deassert)
TelcoAlarm6	État du connecteur d'alarme du panneau avant	Platform Alert (0x24)	0x3 (‘digital’ Discrete - Assert/Deassert)
TelcoAlarm7	État du connecteur d'alarme du panneau avant	Platform Alert (0x24)	0x3 (‘digital’ Discrete - Assert/Deassert)
IPMIWatchdog	Consignation d’action du IPMI Watchdog	Watchdog 2 (0x23)	0x6f (Sensor Specific)
Board Reset	Signale la dernière source de réinitialisation	Board Reset (Kontron OEM) (0xC4)	0x6f (Sensor Specific)
Jumpers Status	Réservé – capteur basé sur un événement	Jumpers Status - Kontron OEM (0xD3)	0x6f (Sensor Specific)

11.4.2.2 Capteurs du bloc d'alimentation

Les capteurs du bloc d'alimentation diffèrent selon la configuration de l'alimentation électrique de la plateforme. Le ME1310 est équipé d'un bloc d'alimentation CC ou CA.

11.4.2.2.1 Capteurs du bloc d'alimentation CC

NOTE : Les capteurs du bloc d'alimentation CC sont présents uniquement lorsqu'un bloc d'alimentation CC est connecté.

Nom du capteur [ID_CAPTEUR]	Description	Code de type de capteur	Code de type d'événement/de lecture
DC PSU Pout	Puissance de sortie du bloc d'alimentation	Power Supply (0x08)	0x01 (Threshold Based)
DC PSU Vout	Tension de sortie du régulateur 48V à 12V du bloc d'alimentation CC	Voltage (0x02)	0x01 (Threshold Based)
DC PSU Iout	Courant de sortie du régulateur 48V à 12V du bloc d'alimentation CC	Current (0x03)	0x01 (Threshold Based)
DC PSU Regulator	Température dans le régulateur 48V à 12V du bloc d'alimentation CC	Temperature (0x01)	0x01 (Threshold Based)
DC PSU HoldUp	Température dans le régulateur de maintien (HoldUp) du bloc d'alimentation CC	Temperature (0x01)	0x01 (Threshold Based)
DC PSU Inlet	Température dans le circuit ORing de l’entrée d'alimentation du bloc d'alimentation CC	Temperature (0x01)	0x01 (Threshold Based)

DC PSU HUVout	Tension de maintien du bloc d'alimentation CC	Voltage (0x02)	0x01 (Threshold Based)
DC PSU Vin	Tension d'entrée QBrick du bloc d'alimentation CC	Voltage (0x02)	0x01 (Threshold Based)
DC PSU Feed A	Lecture de l'entrée A d'alimentation du bloc d'alimentation CC	Voltage (0x02)	0x01 (Threshold Based)
DC PSU Feed B	Lecture de l'entrée B d'alimentation du bloc d'alimentation CC	Voltage (0x02)	0x01 (Threshold Based)

11.4.2.2.2 Capteurs du bloc d'alimentation CA

NOTE : Les capteurs du bloc d'alimentation CA sont présents uniquement lorsqu'un bloc d'alimentation CA est connecté.

Nom du capteur [ID_CAPTEUR]	Description	Code de type de capteur	Code de type d'événement/de lecture
AC PSU Vout	Tension de sortie du bloc d'alimentation	Voltage (0x02)	0x01 (Threshold Based)
AC PSU Pout	Puissance de sortie du bloc d'alimentation	Power Supply (0x08)	0x01 (Threshold Based)
AC PSU Vin	Tension d'entrée du bloc d'alimentation	Voltage (0x02)	0x01 (Threshold Based)
AC PSU Pin	Puissance d'entrée du bloc d'alimentation	Power Supply (0x08)	0x01 (Threshold Based)
AC PSU Temp1	Température du bloc d'alimentation	Temperature (0x01)	0x01 (Threshold Based)

11.4.2.3 Capteurs du module d'E/S

Les capteurs du module d'E/S diffèrent selon la configuration du module d'E/S de la plateforme.

11.4.2.3.1 Capteurs du module d'E/S de commutation Ethernet

NOTE : Les capteurs du module d'E/S de commutation Ethernet sont présents seulement si la plateforme est équipée d'un module d'E/S de commutation Ethernet.

Nom du capteur [ID_CAPTEUR]	Description	Code de type de capteur	Code de type d'événement/de lecture
Temp SWB Clk	Température sous la DPLL ZL30772 sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB Inlet	Température à l'entrée d'air sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB OCXO	Température sous l'OCXO sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP1	Température du module SFP1 sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP2	Température du module SFP2 sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP3	Température du module SFP3 sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP4	Température du module SFP4 sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP5	Température du module SFP5 sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)

Nom du capteur [ID_CAPTEUR]	Description	Code de type de capteur	Code de type d'événement/de lecture
Temp SWB SFP6	Température du module SFP6 sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP7	Température du module SFP7 sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP8	Température du module SFP8 sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP9	Température du module SFP9 sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP10	Température du module SFP10 sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP11	Température du module SFP11 sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP12	Température du module SFP12 sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB Switch	Température de la puce du commutateur sur le module d'E/S de commutation Ethernet	Temperature (0x01)	0x01 (Threshold Based)

11.4.2.3.2 Capteurs du module d'E/S de connexion directe

NOTE : Les capteurs du module d'E/S de connexion directe sont présents seulement si la plateforme est équipée d'un module d'E/S de connexion directe. Le développement de cette option est envisagé. Veuillez contacter le service des ventes de Kontron.

11.4.2.4 Capteurs propres à l'application

11.4.2.4.1 Capteurs Silicom P3iMB

Les capteurs Silicom P3iMB sont présents seulement lorsque le périphérique FRU virtuel PCIe est configuré pour une carte d'expansion PCIe P3iMB.

Nom du capteur [ID_CAPTEUR]	Description	Code de type de capteur	Code de type d'événement/de lecture
T P3iMB Local S<X>	Température locale pour la carte d'expansion PCIe Silicom P3iMB Où <X> est l'ID de l'emplacement PCIe.	Temperature (0x01)	0x01 (Threshold Based)
T ACC100 TSDE S<X>	Température TSDE East de l'accélérateur FEC Intel ACC100 de la carte d'expansion PCIe Silicom P3iMB Où <X> est l'ID de l'emplacement PCIe.	Temperature (0x01)	0x01 (Threshold Based)
T ACC100 TSDW S<X>	Température TSDW West de l'accélérateur FEC Intel ACC100 de la carte d'expansion PCIe Silicom P3iMB Où <X> est l'ID de l'emplacement PCIe.	Temperature (0x01)	0x01 (Threshold Based)

11.5 Maintenance

11.5.1 Journal des événements système

11.5.1.1 Journal des événements système du BMC

Le journal des événements système du BMC est accessible :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish
- En utilisant IPMI

11.5.1.1.1 Liens entre les journaux des événements système du BMC

Les journaux des événements système accessibles via l'interface utilisateur Web du BMC et Redfish sont gérés indépendamment. Cela a deux conséquences :

- Les journaux visualisés dans l'interface utilisateur Web et Redfish peuvent afficher des événements qui ne sont pas pris en charge par le journal des événements IPMI.
- L'utilisation des méthodes décrites ci-dessous pour vider les journaux avec l'interface utilisateur Web ou Redfish aura pour résultat de vider complètement le journal pour ces deux interfaces. Toutefois, pour vider le journal des événements IPMI, la commande IPMI appropriée doit être utilisée.

11.5.1.1.2 Événements TelcoAlarm enregistrés dans le SEL au redémarrage du BMC

Les capteurs TelcoAlarm sont utilisés pour détecter les états des entrées du connecteur d'alarme du panneau avant. Si rien n'est connecté au port d'alarmes, des événements TelcoAlarm seront enregistrés dans le SEL lorsque le BMC redémarre. Cela se produit parce que pour détecter un câblage défectueux (un câble coupé, etc.), le système considère une boucle ouverte comme un événement – et un port d'alarmes vide crée une boucle ouverte.

Si le port d'alarmes n'est pas utilisé, une solution consisterait à installer un connecteur RJ45 de bouclage dans le port d'alarmes.

Les événements TelcoAlarm générés mettront l'état de santé du BMC dans un état critique. Actuellement, le seul moyen de restaurer l'état de santé du BMC consiste à vider le journal des événements système. Kontron recommande d'exporter le SEL avant de le vider.

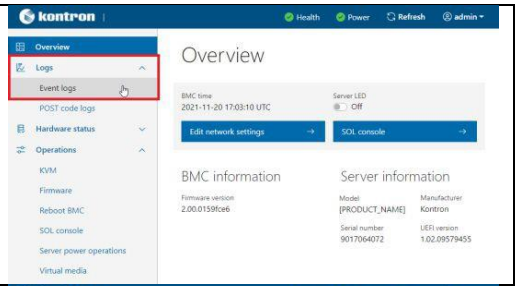
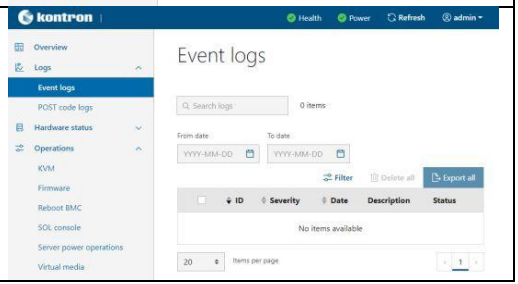
Section pertinente :

Composants de la plateforme

11.5.1.1.3 Accéder au SEL du BMC en utilisant l'interface utilisateur Web du BMC

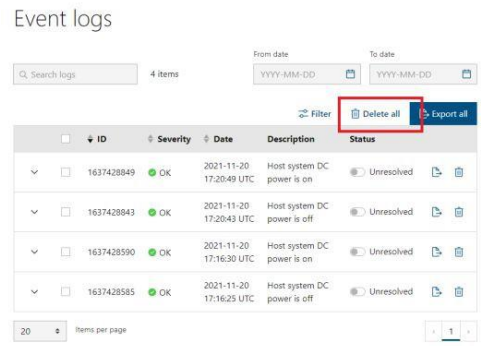
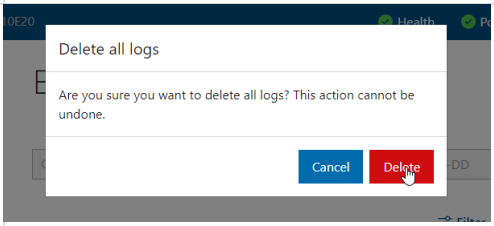
Voir Accéder au BMC en utilisant l'interface utilisateur Web pour les instructions d'accès.

11.5.1.1.3.1 Accéder au journal des événements système du BMC

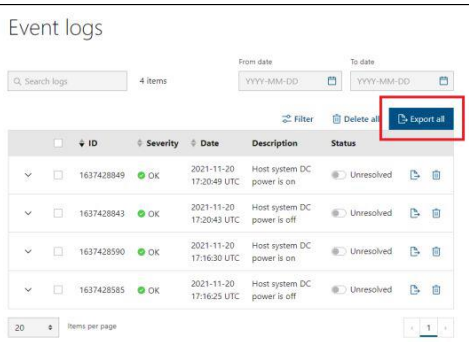
Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Logs**, puis sur **Event Logs**.	
Étape_2	Le journal des événements système s'affiche. L'information suivante peut être recueillie : 1. ID (ID de l'événement) 2. Severity (gravité) 3. Date (date) 4. Description (description) 5. Status (état)	

11.5.1.1.3.2 Vider le journal des événements système du BMC

NOTE : Cette méthode effacera les événements visibles via l'interface utilisateur Web et Redfish. Le journal des événements IPMI doit être vidé séparément.

Étape_1	Cliquer sur le bouton **Delete all**.	
Étape_2	Confirmer l'action en cliquant sur le bouton **Delete**.	

11.5.1.1.3.3 Exporter le journal des événements système du BMC

Étape_1	Cliquer sur le bouton **Export all** pour télécharger le journal des événements système.	

11.5.1.1.4 Accéder au SEL du BMC en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

11.5.1.1.4.1 Accéder au journal des événements système du BMC

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.

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 --request GET --url [URL_RACINE]/redfish/v1/Systems/system/LogServices/EventLog/Entries | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system/
LogServices/EventLog/Entries  | jq
{
  "@odata.id": "/redfish/v1/Systems/system/LogServices/EventLog/Entries",
  "@odata.type": "#LogEntryCollection.LogEntryCollection",
  "Description": "Collection of System Event Log Entries",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Systems/system/LogServices/EventLog/Entries/1647629153",
      "@odata.type": "#LogEntry.v1_4_0.LogEntry",
      "Created": "2022-03-18T18:45:53+00:00",
      "EntryType": "Event",
      "Id": "1647629153",
      "Message": "Host system DC power is off",
      "MessageArgs": [],
      "MessageId": "OpenBMC.0.1.DCPowerOff",
      "Name": "System Event Log Entry",
      "Severity": "OK"
    },
    {
      "@odata.id": "/redfish/v1/Systems/system/LogServices/EventLog/Entries/1647629154",
      "@odata.type": "#LogEntry.v1_4_0.LogEntry",
      "Created": "2022-03-18T18:45:54+00:00",
      "EntryType": "Event",
      "Id": "1647629154",
      "Message": "System Restart : Normal power down",
      "MessageArgs": [
        "Normal power down"
      ],
      "MessageId": "OpenBMC.0.1.BoardReset",
      "Name": "System Event Log Entry",
      "Severity": "OK"
    },
[...]
```

11.5.1.1.4.2 Vider le journal des événements système du BMC

NOTE : Cette méthode effacera les événements visibles via l'interface utilisateur Web et Redfish. Le journal des événements IPMI doit être vidé séparément.

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 --request POST --url [URL_RACINE] /redfish/v1/Systems/system/LogServices/EventLog/Actions/LogService.ClearLog | jq**

	`$ curl -k -s --request POST --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system/LogServices/EventLog/Actions/LogService.ClearLog  | jq`
	`{`
	`  "@Message.ExtendedInfo": [`
	`    {`
	`      "@odata.type": "#Message.v1_1_1.Message",`
	`      "Message": "Successfully Completed Request",`
	`      "MessageArgs": [],`
	`      "MessageId": "Base.1.8.1.Success",`
	`      "MessageSeverity": "OK",`
	`      "Resolution": "None"`
	`    }`
	`  ]`
	`}`

Étape_2	Vérifier que le journal des événements système a été correctement vidé. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE] /redfish/v1/Systems/system/LogServices/EventLog/Entries | jq**

	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system/LogServices/EventLog/Entries  | jq`
	`{`
	`  "@odata.id": "/redfish/v1/Systems/system/LogServices/EventLog/Entries",`
	`  "@odata.type": "#LogEntryCollection.LogEntryCollection",`
	`  "Description": "Collection of System Event Log Entries",`
	`  "Members": [],`
	`  "Members@odata.count": 0,`
	`  "Name": "System Event Log Entries"`
	`}`

11.5.1.1.4.3 Types d'événements pris en charge par Redfish

Le format de l'événement est composé de la version du schéma d'événement OpenBMC suivie du type d'événement [SCHEMA VERSION].[EVENT TYPE]. La version actuelle du schéma [SCHEMA VERSION] est **OpenBMC.0.1**.

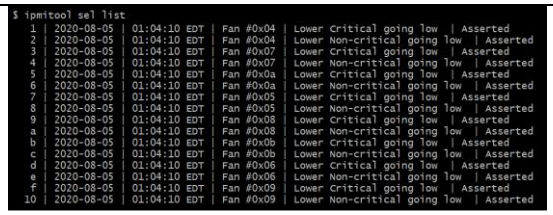
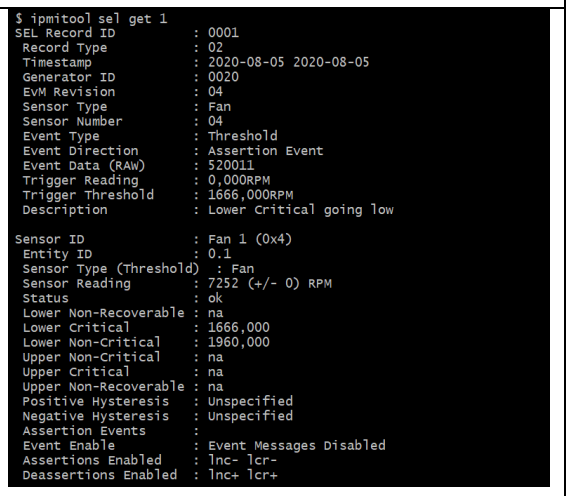
Type d'événement [EVENT TYPE]	**Description**
InventoryAdded	Indique qu'un article d'inventaire avec le modèle, le type et le numéro de série spécifiés a été installé
InventoryRemoved	Indique qu'un article d'inventaire avec le modèle, le type et le numéro de série spécifiés a été retiré
BoardReset	Indique que la charge utile a été réinitialisée
DCPowerOn	Indique que l'alimentation CC du système est activée
DCPowerOff	Indique que l'alimentation CC du système est éteinte

Type d'événement [EVENT TYPE]	Description
SensorThresholdCriticalLowGoingLow	Indique qu'un capteur de seuil a franchi un seuil critique bas avec un franchissement à la baisse
SensorThresholdCriticalLowGoingHigh	Indique qu'un capteur de seuil a franchi un seuil critique bas avec un franchissement à la hausse
SensorThresholdCriticalHighGoingLow	Indique qu'un capteur de seuil a franchi un seuil critique haut avec un franchissement à la baisse
SensorThresholdCriticalHighGoingHigh	Indique qu'un capteur de seuil a franchi un seuil critique haut avec un franchissement à la hausse
SensorThresholdWarningLowGoingLow	Indique qu'un capteur de seuil a franchi un seuil d'avertissement bas avec un franchissement à la baisse
SensorThresholdWarningLowGoingHigh	Indique qu'un capteur de seuil a franchi un seuil d'avertissement bas avec un franchissement à la hausse
SensorThresholdWarningHighGoingLow	Indique qu'un capteur de seuil a franchi un seuil d'avertissement haut avec un franchissement à la baisse
SensorThresholdWarningHighGoingHigh	Indique qu'un capteur de seuil a franchi un seuil d'avertissement haut avec un franchissement à la hausse
FanRedundancyLost	Indique que la redondance des ventilateurs du système a été perdue
FanRedundancyRegained	Indique que la redondance des ventilateurs du système a été rétablie
FanSpeedDeviated	Indique que la vitesse des ventilateurs s'est écartée de la valeur cible, ce qui pourrait indiquer un ventilateur défectueux
FanSpeedRestored	Indique que la vitesse des ventilateurs est revenue à la normale
IPMIWatchdog	Indique que la durée prévue pour le IPMI Watchdog a expiré

11.5.1.1.5 Accéder au SEL du BMC 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] -C 17**.

11.5.1.1.5.1 Accéder au journal des événements système du BMC

Étape_1	Afficher la liste de tous les événements. InviteSE_ServeurLocal:~# **ipmitool sel list**	
Étape_2	Pour obtenir plus de détails sur un événement particulier, utiliser la commande suivante. InviteSE_ServeurLocal:~# **ipmitool sel get [ID_ÉVÉNEMENT]**	

11.5.1.1.5.2 Vider le journal des événements système du BMC

NOTE : Cette méthode efface seulement le journal des événements IPMI. Les journaux des événements accessibles via l'interface utilisateur Web et Redfish doivent être vidés séparément.

Étape_1	Utiliser la commande suivante pour vider le journal des événements système. InviteSE_ServeurLocal:~# **ipmitool sel clear**	`$ ipmitool sel clear` `Clearing SEL.  Please allow a few seconds to erase.`

11.5.1.1.5.3 Exporter le journal des événements système du BMC

Étape_1	Utiliser la commande suivante pour enregistrer le journal des événements système dans un fichier.
	
	InviteSE_ServeurLocal:~# **ipmitool sel save [NOM_FICHIER]**
		`$ ipmitool sel save file`
		`1 | 2020-08-05 | 01:04:10 EDT | Fan #0x04 | Lower Critical going low  | Asserted`
		`2 | 2020-08-05 | 01:04:10 EDT | Fan #0x04 | Lower Non-critical going low  | Asserted`
		`3 | 2020-08-05 | 01:04:10 EDT | Fan #0x07 | Lower Critical going low  | Asserted`
		`4 | 2020-08-05 | 01:04:10 EDT | Fan #0x07 | Lower Non-critical going low  | Asserted`
		`5 | 2020-08-05 | 01:04:10 EDT | Fan #0x0a | Lower Critical going low  | Asserted`
		`6 | 2020-08-05 | 01:04:10 EDT | Fan #0x0a | Lower Non-critical going low  | Asserted`
		`7 | 2020-08-05 | 01:04:10 EDT | Fan #0x05 | Lower Critical going low  | Asserted`
		`8 | 2020-08-05 | 01:04:10 EDT | Fan #0x05 | Lower Non-critical going low  | Asserted`
		`9 | 2020-08-05 | 01:04:10 EDT | Fan #0x08 | Lower Critical going low  | Asserted`
		`a | 2020-08-05 | 01:04:10 EDT | Fan #0x08 | Lower Non-critical going low  | Asserted`
		`b | 2020-08-05 | 01:04:10 EDT | Fan #0x0b | Lower Critical going low  | Asserted`
		`c | 2020-08-05 | 01:04:10 EDT | Fan #0x0b | Lower Non-critical going low  | Asserted`
		`d | 2020-08-05 | 01:04:10 EDT | Fan #0x06 | Lower Critical going low  | Asserted`
		`e | 2020-08-05 | 01:04:10 EDT | Fan #0x06 | Lower Non-critical going low  | Asserted`

11.5.1.2 Journal des événements système du NOS

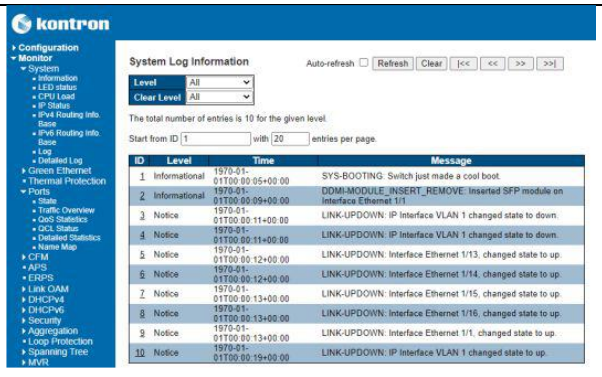
Le journal des événements système du NOS est accessible :

- En utilisant l'interface utilisateur Web du NOS
- En utilisant le CLI du NOS

11.5.1.2.1 Accéder au SEL du NOS en utilisant l'interface utilisateur Web du NOS

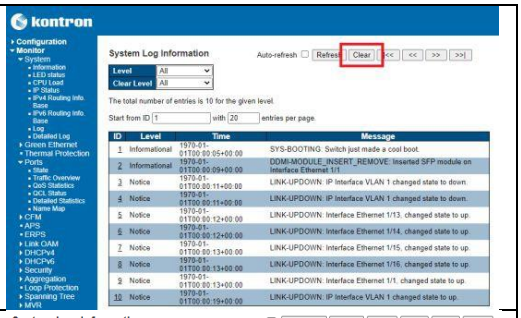
Voir Accéder au NOS en utilisant l'interface utilisateur Web du NOS pour les instructions d'accès.

11.5.1.2.1.1 Accéder au journal des événements système du NOS

Étape_1	Dans le menu de gauche, sélectionner **Monitoring**, **System**, puis **Log**. Le journal des événements système du NOS devrait être affiché.	

11.5.1.2.1.2 Vider le journal des événements système du NOS

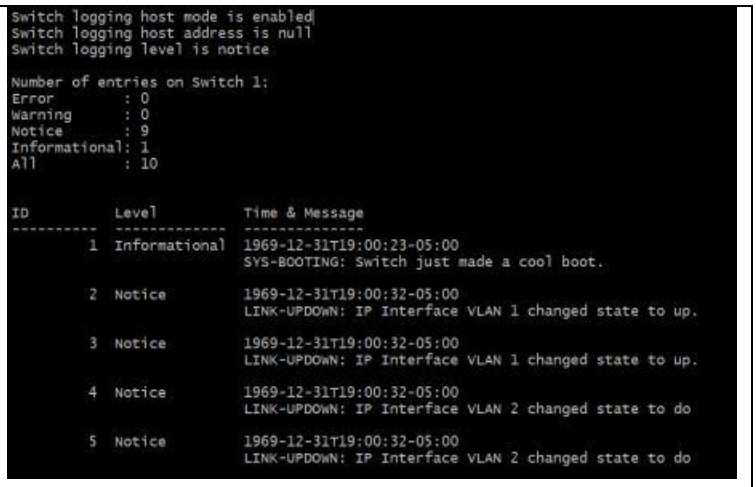
Étape_1	Dans le menu de gauche, sélectionner **Monitoring**, **System**, puis **Log**. Le journal des événements système du NOS devrait être affiché.	

Étape_2	Cliquer sur le bouton **Clear**.	
Étape_3	Le journal des événements système du NOS devrait être vide.	

11.5.1.2.2 Accéder au SEL du NOS en utilisant le CLI du NOS

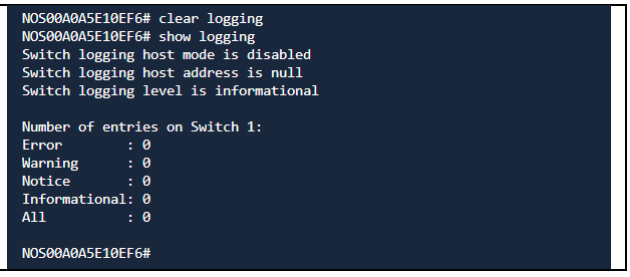
Voir Accéder au NOS pour les instructions d'accès.

11.5.1.2.2.1 Accéder au journal des événements système du NOS

Étape_1	Afficher le journal des événements du NOS. InviteCLI_NOSLocal:~# **show logging**	

```
Switch logging host mode is enabled
Switch logging host address is null
Switch logging level is notice

Number of entries on Switch 1:
Error        : 0
Warning      : 0
Notice       : 9
Informational: 1
All          : 10


ID          Level          Time & Message
----------  -------------  --------------
         1  Informational  1969-12-31T19:00:23-05:00
                           SYS-BOOTING: Switch just made a cool boot.

         2  Notice         1969-12-31T19:00:32-05:00
                           LINK-UPDOWN: IP Interface VLAN 1 changed state to up.

         3  Notice         1969-12-31T19:00:32-05:00
                           LINK-UPDOWN: IP Interface VLAN 1 changed state to up.

         4  Notice         1969-12-31T19:00:32-05:00
                           LINK-UPDOWN: IP Interface VLAN 2 changed state to do

         5  Notice         1969-12-31T19:00:32-05:00
                           LINK-UPDOWN: IP Interface VLAN 2 changed state to do
```

11.5.1.2.2.2 Vider le journal des événements système du NOS

Étape_1	Afficher le journal des événements du NOS. InviteCLI_NOSLocal:~# **clear logging**	
Étape_2	Le journal des événements système du NOS devrait être vide. InviteCLI_NOSLocal:~# **show logging**	

```
NOS00A0A5E10EF6# clear logging
NOS00A0A5E10EF6# show logging
Switch logging host mode is disabled
Switch logging host address is null
Switch logging level is informational

Number of entries on Switch 1:
Error        : 0
Warning      : 0
Notice       : 0
Informational: 0
All          : 0

NOS00A0A5E10EF6#
```

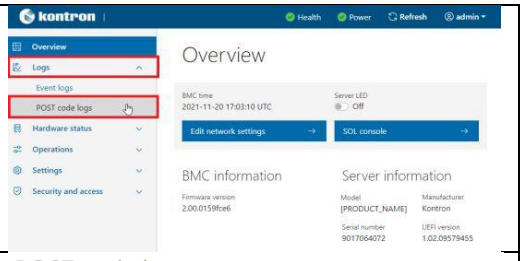
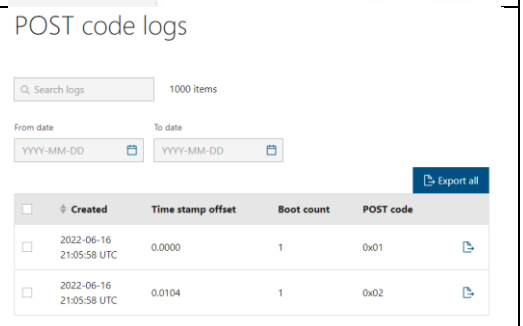
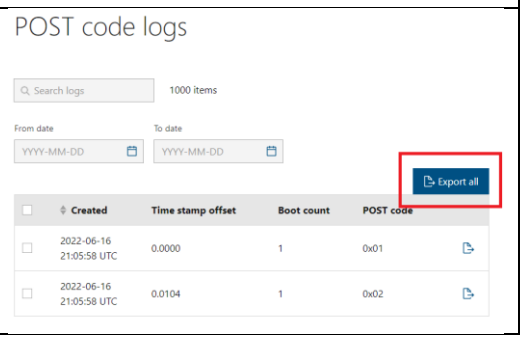
11.5.2 Journaux des codes POST

Les codes POST sont accessibles :

- En utilisant l'interface utilisateur Web du BMC
- En utilisant Redfish

11.5.2.1 Accéder aux journaux des codes POST 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	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Logs**, puis sur **POST code logs**.	
Étape_2	Le journal des événements système s'affiche. L'information suivante peut être recueillie : 1. ID (ID de l'événement) 2. Time stamp offset (décalage de l'estampille temporelle) 3. Boot count (nombre d'amorçages) 4. POST code (code POST) 5. Status (état)	
Étape_3	Cliquer sur le bouton **Export all** pour télécharger les journaux des codes POST.	

11.5.2.2 Accéder aux journaux des codes POST en utilisant Redfish

Les procédures suivantes seront exécutées en utilisant l'URL racine Redfish requise pour une connexion réseau externe. Elles peuvent également être exécutées à l'aide de l'URL racine Redfish requise pour l'interface hôte Redfish interne si les commandes sont lancées localement à partir du système d'exploitation du serveur. Voir Accéder au BMC en utilisant Redfish pour les instructions d'accès.

Étape_1	Accédez aux journaux des codes POST avec la commande suivante. InviteSE_OrdinateurDistant:~# **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/Systems/system/LogServices/PostCodes/Entries | jq**

11.5.3 Interprétation des données des capteurs

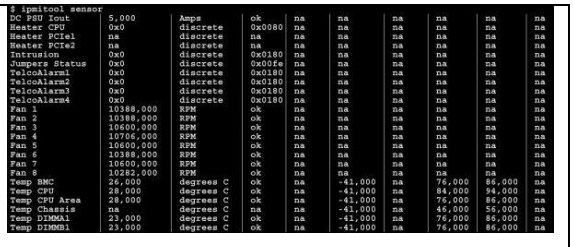
11.5.3.1 Procédure d'interprétation

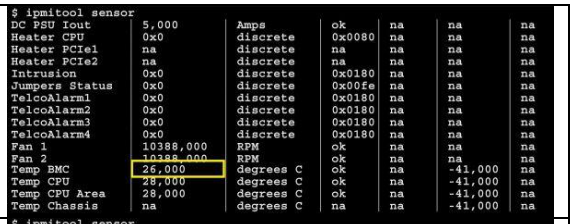
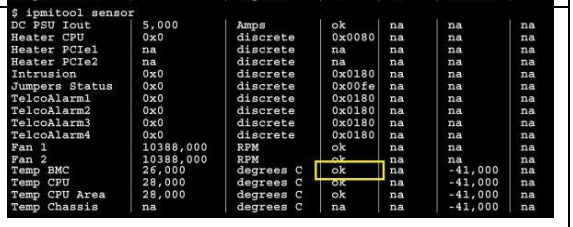
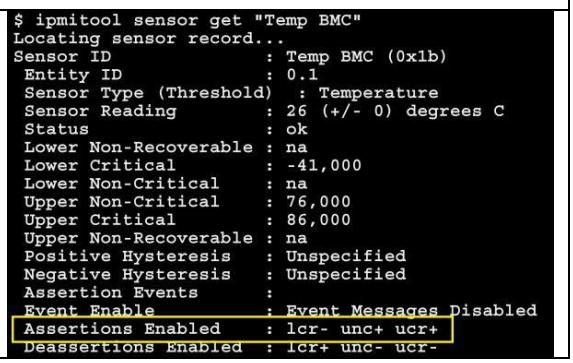
Avant de commencer la procédure d'interprétation, recueillir les informations suivantes sur l'événement :

- 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. InviteSE_ServeurLocal:~# **ipmitool sensor** Les colonnes du tableau sont les suivantes : • Name (nom) • Numerical reading (lecture numérique) • Event/reading type/unit (type d'événement/de lecture/unité) • Unit-based sensors status/discrete sensors reading (état des capteurs associés à une unité de mesure/lecture des capteurs discrets) • 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	La valeur de la lecture numérique est indiquée dans la deuxième colonne. InviteSE_ServeurLocal:~# **ipmitool sensor**	
Étape_3	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_4	Un événement sera créé en fonction du type d'enclenchement activé pour le capteur spécifié. InviteSE_ServeurLocal:~# **ipmitool sensor get "[ID_CAPTEUR]"**	

11.5.3.2 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). Pour plus d'informations sur les capteurs IPMI, voir la documentation IPMI.

11.5.3.2.1 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)	Rapporte la température d'un composant de la plateforme.
02h (Voltage)	Rapporte la présence d'une tension sur le bloc d'alimentation ou sur la plateforme.
03h (Current)	Rapporte le courant de sortie d'un composant de la plateforme.
04h (Fan)	Information générale sur le ou les ventilateurs de la plateforme (ex. vitesse, présence, défaillance).
08h (Power supply)	Information générale sur le bloc d'alimentation (ex. présence, défaillance, état de santé).
0Bh (Other Unit-based sensor)	Rapporte une unité propre au capteur.
18h (Chassis)	Rapporte la présence d'un élément dans le châssis.
C4h (Board Reset - Kontron OEM)	Indique la dernière source de redémarrage.
D3h (Jumpers status - Kontron OEM)	Réservé.
23h (Watchdog 2)	Information générale sur le mécanisme de surveillance (watchdog) IPMI.
24h (Platform alert)	Rapporte de l'information sur les alertes générées par le BMC.

11.5.3.2.2 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. 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	Capteurs associés à une unité de mesure, ce qui signifie qu'ils disposent 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.

11.5.3.2.2.1 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, la vitesse d'un ventilateur ou un état discret.

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	

11.5.4 Remplacement des composants

Voir Installation et assemblage des composants pour obtenir les procédures de remplacement des composants.

11.5.5 Sauvegarde et récupération

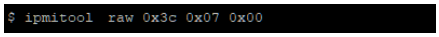
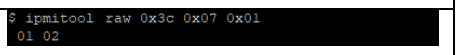
Sur une plateforme ME1310, les configurations de l'UEFI/BIOS et du NOS peuvent être sauvegardées et récupérées.

11.5.5.1 UEFI/BIOS

Cette section décrit comment faire une sauvegarde de l'UEFI/BIOS qui inclut les paramètres utilisateur actuels de l'UEFI/BIOS et une récupération à partir de la sauvegarde créée. 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] -C 17**.

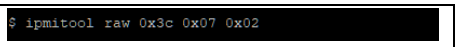
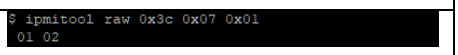
11.5.5.1.1 Sauvegarder l'UEFI/BIOS

Pour de l'information sur [OCTET1], voir Description des étapes de création et de récupération.

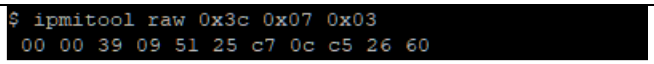
Étape_1	Sauvegarder l'UEFI/BIOS. Cette action permet de sauvegarder l'UEFI/BIOS et la configuration. InviteSE_ServeurLocal: ~# **ipmitool raw 0x3c 0x07 0x00** Code d'exécution : • 0x00 : Le processus de récupération a démarré avec succès • 0xd5 : Le processus de récupération ne peut pas être lancé	
Étape_2	Vérifier l'état de la sauvegarde de l'UEFI/BIOS. InviteSE_ServeurLocal: ~# **ipmitool raw 0x3c 0x07 0x01** Le code d'exécution est toujours 0x00. [OCTET0] État : • 0x00 : Succès/inactif • 0x01 : En cours • 0x02 : Échec [OCTET1] Étape actuelle : • Voir le tableau dans la section Description des étapes de création et de récupération. Dans l'image de droite, l'état de la création de la sauvegarde est **En cours** et l'étape actuelle est **Set Server to Power Off state** (mise hors tension du serveur).	

11.5.5.1.2 Récupérer l'UEFI/BIOS

Pour de l'information sur [OCTET1], voir Description des étapes de création et de récupération.

Étape_1	Récupérer l'UEFI/BIOS. Cette action permet de récupérer l'UEFI/BIOS et la configuration. InviteSE_ServeurLocal: ~# **ipmitool raw 0x3c 0x07 0x02** Code d'exécution : • 0x00 : Le processus de récupération a démarré avec succès • 0xd5 : Le processus de récupération ne peut pas être lancé	
Étape_2	Vérifier l'état de la récupération. InviteSE_ServeurLocal: ~# **ipmitool raw 0x3c 0x07 0x01** Le code d'exécution est toujours 0x00. [OCTET0] État : • 0x00 : Succès/inactif • 0x01 : En cours • 0x02 : Échec [OCTET1] Étape actuelle : • Voir le tableau dans la section Description des étapes de création et de récupération. Dans l'image de droite, l'état de la récupération est **En cours** et l'étape actuelle est **Set Server to Power Off state** (mise hors tension du serveur).	

11.5.5.1.3 Obtenir de l'information sur la dernière sauvegarde de l'UEFI/BIOS

Étape_1	Obtenir de l'information sur l'UEFI/BIOS sauvegardé. InviteSE_ServeurLocal: ~# **ipmitool raw 0x3c 0x07 0x03** Code d'exécution : 0x00 : La sauvegarde est valide 0xff : La sauvegarde n'est pas valide [OCTET0-OCTET5] Version : [1B] Majeure [1B] Mineure [4B] Aux [OCTET6] État [OCTET7-OCTET10] Estampille temporelle Unix Dans l'image de droite, la version est 0.57.095125C7, l'état est 0x00 et l'estampille temporelle est 1613153548.	

11.5.5.1.4 Description des étapes de création et de récupération

Description de l'étape	**Valeur de l'étape (OCTET1)**	**Détails**
No step	0x00	Rien ne se passe actuellement, aucune défaillance n'est à signaler.
Get UEFI/BIOS version	0x01	Récupérer la version de l'UEFI/BIOS via DBUS.
Server Power Off	0x02	Mise hors tension du serveur.
Force Intel ME Recovery mode	0x03	Force Intel ME à passer en mode rétablissement.
MTD partition detect	0x04	Vérification à savoir si le périphérique flash et la partition sont détectés.
MTD Flash erase	0x05	Périphérique flash en cours d'effacement. La cible dépend de la nature de l'action (création ou récupération).
MTD Flash write	0x06	Écriture en cours sur le périphérique flash. La cible dépend de la nature de l'action (création ou récupération).
MTD Flash verify	0x07	Périphérique flash en cours de vérification. La cible dépend de la nature de l'action (création ou récupération).
Reset Intel ME to Normal mode	0x08	Réinitialiser Intel ME pour revenir au mode normal.
Server Power On	0x09	Démarrage du serveur.

11.5.5.2 Configuration du NOS

Cette section décrit comment sauvegarder et récupérer la configuration du NOS. Ces opérations peuvent être réalisées :

- En utilisant SCP
- En utilisant l'interface utilisateur Web du NOS

11.5.5.2.1 Sauvegarder et récupérer la configuration du NOS en utilisant SCP

11.5.5.2.1.1 Préalables

1	Un serveur configuré pour le protocole souhaité est disponible et accessible à partir du NOS.
2	En cas de récupération d'une configuration, le fichier de configuration correspondant est présent sur le serveur.

L'URL qui suit l'adresse IP du serveur est un chemin relatif au dossier personnel de l'utilisateur ("~/"). Pour spécifier un chemin d'accès absolu, utiliser une double barre oblique après l'adresse IP (ex. scp://[NOM_UTILISATEUR_SERVEUR]:[MOT_DE_PASSE_SERVEUR]@[IP_SERVEUR]//[path/to/configfile]).

Voir Accéder au NOS pour les instructions d'accès.

11.5.5.2.1.2 Sauvegarder la configuration du NOS

Étape_1	Accéder au système d'exploitation réseau du commutateur en utilisant SSH ou une connexion série.
Étape_2	Copier la configuration souhaitée sur le serveur distant. • **running-config** : configuration actuellement active (peut différer de startup-config si des modifications ont été apportées depuis le dernier démarrage, mais n'ont pas été sauvegardées). • **startup-config** : configuration sauvegardée appliquée au démarrage du commutateur. InviteCLI_NOSLocal:~# **copy [running-config|startup-config] scp://[NOM_UTILISATEUR_SERVEUR]:[MOT_DE_PASSE_SERVEUR]@[IP_SERVEUR]/[CHEMIN_ACCÈS_FICHIER] save-host-key**
	`# copy startup-config scp://user:password@192.168.0.10/ startup-config save-host-key` `% Saving 1506 bytes to server 192.168.0.10: startup-config`

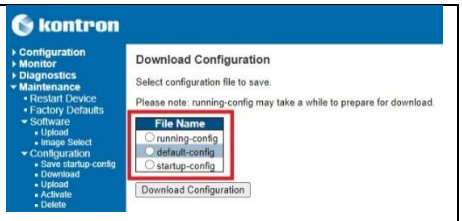
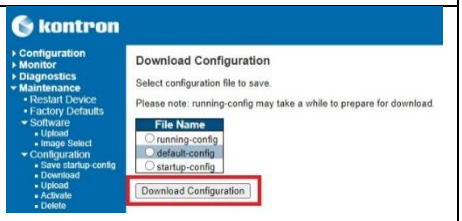
11.5.5.2.1.3 Récupérer la configuration du NOS

Étape_1	Accéder au système d'exploitation réseau du commutateur en utilisant SSH ou une connexion série.	
Étape_2	Copier le fichier de configuration du serveur distant sous l'une des formes suivantes : • **Running-config** : configuration actuellement active (volatile jusqu'à ce qu'elle soit sauvegardée en tant que startup-config). • **startup-config** : configuration sauvegardée appliquée au démarrage du commutateur. InviteCLI_NOSLocal:~# **copy scp://[NOM_UTILISATEUR_SERVEUR]:[MOT_DE_PASSE_SERVEUR] @ [IP_SERVEUR]/[CHEMIN_ACCÈS_FICHIER] [running-config|startup- config] save-host-key**	`# copy scp://user:password@192.168.0.10/startup-config startup-config save-host-key` `% Saving 1506 bytes to flash:startup-config`
Étape_3	Si la configuration a été écrite dans startup-config, le NOS doit être redémarré pour que les changements prennent effet. InviteCLI_NOSLocal:~# **reload cold**	`# reload cold` `% Cold reload in progress, please stand by.`

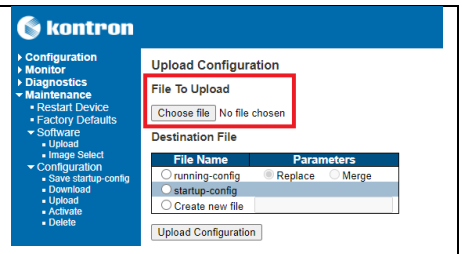
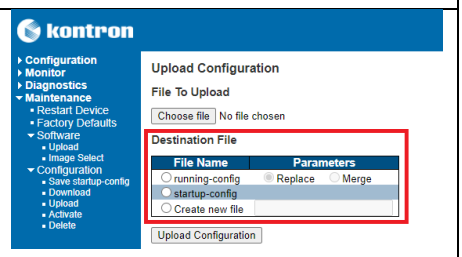
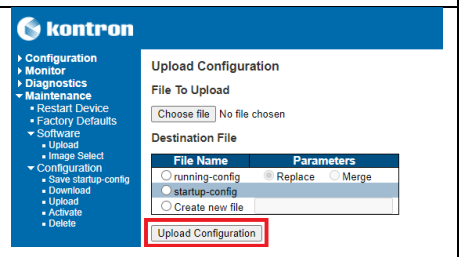
11.5.5.2.2 Sauvegarder et récupérer la configuration du NOS en utilisant l'interface utilisateur Web du NOS

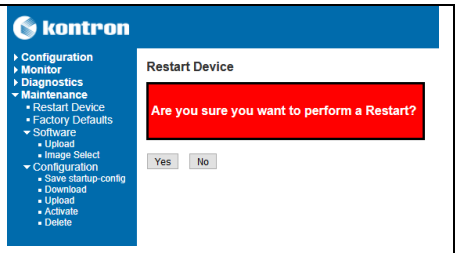
Accéder à l'interface utilisateur Web du NOS. Voir Accéder au NOS pour les instructions d'accès.

11.5.5.2.2.1 Sauvegarder la configuration du NOS

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du NOS, cliquer sur **Maintenance**, sur **Configuration**, puis sur **Download**. Choisir la configuration à sauvegarder : • **running-config** : configuration actuellement active (peut différer de startup-config si des modifications ont été apportées depuis le dernier démarrage, mais n'ont pas été sauvegardées). • **default-config** : configuration appliquée lorsque la configuration par défaut est rechargée. • **startup-config** : configuration sauvegardée appliquée au démarrage du commutateur.	
Étape_2	Cliquer sur **Download Configuration**, puis sélectionner l'endroit où enregistrer le fichier de configuration.	

11.5.5.2.2.2 Récupérer la configuration du NOS

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du NOS, cliquer sur **Maintenance**, sur **Configuration**, puis sur **Upload**. Cliquer sur **Choose file**. Ensuite, à l'aide du navigateur de fichiers, sélectionner le fichier de configuration à récupérer.	
Étape_2	Choisir la configuration à récupérer : • **running-config** : configuration actuellement active (volatile jusqu'à ce qu'elle soit sauvegardée en tant que startup-config). Cette sélection permet de remplacer complètement la configuration actuelle ou de fusionner la nouvelle configuration avec l'actuelle. • **startup-config** : configuration sauvegardée appliquée au démarrage du commutateur. • **Create new file** : crée une nouvelle entrée de configuration qui peut être activée ultérieurement dans le menu (Maintenance → Configuration → Activate). **NOTE :** Il n'est pas possible d'écrire dans default-config, mais il est possible d'écrire dans une configuration par défaut précédemment sauvegardée en utilisant l'une de ces options.	
Étape_3	Cliquer sur **Upload Configuration**.	

Étape_4	Si la configuration a été écrite dans startup-config, le NOS doit être redémarré pour que les changements prennent effet. Pour ce faire, sélectionner **Maintenance**, puis **Restart Device** dans le menu de gauche. Ensuite, confirmer qu'un redémarrage doit être effectué en cliquant sur **Yes**.	

11.5.6 Mise à niveau

11.5.6.1 Mise à niveau le micrologiciel du BMC

NOTE : Pour que la mise à niveau fonctionne, la version du fichier image de mise à niveau doit être différente de celle qui s'exécute sur le BMC. En d'autres termes, il n'est pas possible d'effectuer une mise à niveau avec la même version.

Sections pertinentes :

Description des méthodes d'accès au système

Accéder au BMC

Le micrologiciel du BMC peut être mis à niveau :

- En utilisant Redfish
- En utilisant l'interface utilisateur Web

11.5.6.1.1 Mettre à niveau le micrologiciel du BMC en utilisant Redfish

Redfish est l'interface privilégiée pour la mise à niveau du micrologiciel du BMC.

11.5.6.1.1.1 Préalables

1	Le fichier **.tar** fourni par Kontron a été téléchargé sur l'ordinateur distant.
2	L'accès à l'interface Redfish du BMC est nécessaire.

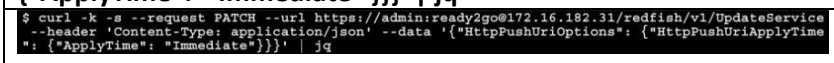
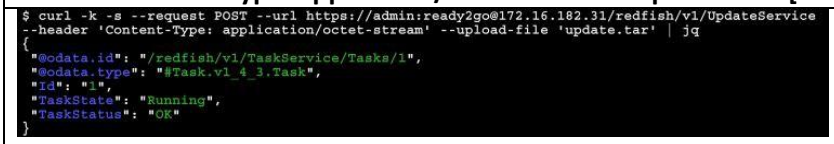
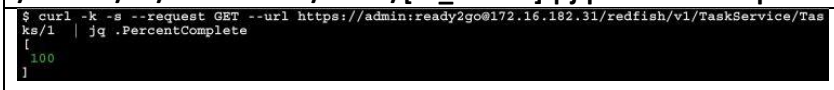
Section pertinente :

Accéder au BMC en utilisant Redfish

11.5.6.1.1.2 Procédure

Étape_1	À partir de l'interface Redfish du BMC, vérifier la version actuelle du micrologiciel du BMC.
	InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/Managers/bmc | jq.FirmwareVersion**
	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc | jq .FirmwareVersion`
	`"2.00.0159fce6"`

Étape_2	Recueillir la liste des identifiants de tous les micrologiciels présents sur la plateforme.
	InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/UpdateService/FirmwareInventory |jq.Members**
	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService/FirmwareInventory | jq .Members`
	`[`
	`{`
	`"@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/8c50fd55"`
	`},`

Étape_3	Vérifier que le nouveau micrologiciel n'est pas déjà présent sur la plateforme. Répéter la commande suivante pour chaque micrologiciel découvert à l'étape précédente. Le champ **Description** décrit le composant visé par ce micrologiciel. Le champ **Version** décrit la version du micrologiciel de ce composant. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/UpdateService/FirmwareInventory/ [ID_MICROLOGICIEL] | jq ".Description,.Version"**
	
Étape_4	Régler l'heure d'application (apply time) à **Immediate**. InviteSE_OrdinateurDistant:~$ **curl -k -s --request PATCH --url [URL_RACINE] /redfish/v1/UpdateService --header 'Content-Type:application/json' --data '{"HttpPushUriOptions": {"HttpPushUriApplyTime": {"ApplyTime": " Immediate "}}}' | jq**
	
Étape_5	Télécharger le micrologiciel en exécutant la commande suivante. Le BMC devrait retourner un **ID** de TaskService. InviteSE_OrdinateurDistant:~$ **curl -k -s --request POST --url [URL_RACINE] /redfish/v1/UpdateService --header 'Content-Type: application/octet-stream' --upload-file ' [CHEMIN_ACCÈS_FICHIER]' | jq**
	
Étape_6	En utilisant l'**ID** retourné à l'étape précédente, s'assurer que la tâche est terminée. La valeur du paramètre **PercentComplete** doit être de 100 avant de passer aux étapes suivantes. Cela peut prendre plusieurs secondes. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE] /redfish/v1/TaskService/Tasks/[ID_TÂCHE] | jq .PercentComplete**
	
Étape_7	Une fois le BMC à nouveau disponible, vérifier que la version du micrologiciel a changé. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/Managers/bmc | jq.FirmwareVersion**
	

11.5.6.1.2 Mettre à niveau le micrologiciel du BMC en utilisant l'interface utilisateur Web

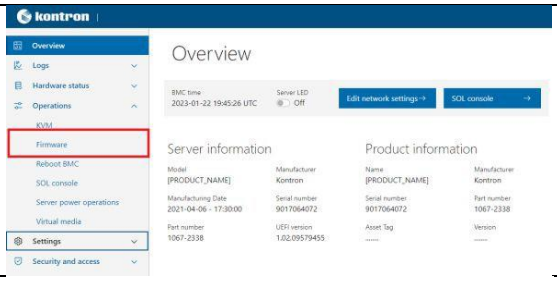
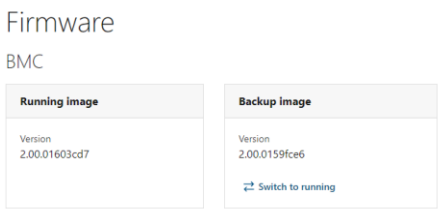
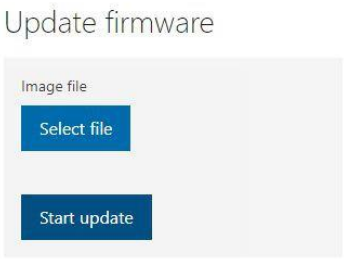
11.5.6.1.2.1 Préalables

1	Le fichier **.tar** fourni par Kontron a été téléchargé sur l'ordinateur distant.
2	L'accès à l'interface utilisateur Web du BMC est nécessaire.

Section pertinente :

Accéder au BMC en utilisant l'interface utilisateur Web

11.5.6.1.2.2 Procédure

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Operations**, puis sur **Firmware**.	
Étape_2	Vérifier la version actuelle du micrologiciel. S'assurer que le nouveau micrologiciel est plus récent.	
Étape_3	Dans la section **Update firmware**, choisir un fichier **.tar** à télécharger pour le BMC en cliquant sur **Select file**.	
Étape_4	Cliquer sur **Start update**.	
Étape_5	Lorsque le fichier a été téléchargé avec succès, un message de réussite apparaît dans le coin supérieur droit.	
Étape_6	Attendre que le BMC se mette à niveau. La page devrait se rafraîchir automatiquement si la mise à niveau est réussie.	
Étape_7	Une fois le BMC à nouveau disponible, vérifier que la version du micrologiciel a changé.	

11.5.6.2 Mettre à niveau le micrologiciel du FPGA

NOTE : Pour que la mise à niveau fonctionne, la version du fichier image de mise à niveau doit être différente de celle qui s'exécute sur le BMC. En d'autres termes, il n'est pas possible d'effectuer une mise à niveau avec la même version.

Sections pertinentes :

Description des méthodes d'accès au système

Accéder au BMC

Le micrologiciel du FPGA peut être mis à niveau :

- En utilisant Redfish
- En utilisant l'interface utilisateur Web

11.5.6.2.1 Mettre à niveau le micrologiciel du FPGA en utilisant Redfish

Redfish est l'interface privilégiée pour la mise à niveau du micrologiciel du FPGA.

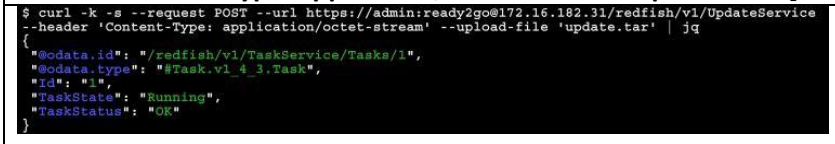
11.5.6.2.1.1 Préalables

1	Le fichier **.tar** fourni par Kontron a été téléchargé sur l'ordinateur distant.
2	L'accès à l'interface Redfish du BMC est nécessaire.

Section pertinente :

Accéder au BMC en utilisant Redfish

11.5.6.2.1.2 Procédure

Étape_1	À partir de l'interface Redfish du BMC, vérifier la version actuelle du micrologiciel du FPGA. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/Systems/system | jq.FpgaVersion** 
Étape_2	Recueillir la liste des identifiants de tous les micrologiciels présents sur la plateforme. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/UpdateService/FirmwareInventory |jq.Members** 
Étape_3	Vérifier que le nouveau micrologiciel n'est pas déjà présent sur la plateforme. Répéter la commande suivante pour chaque micrologiciel découvert à l'étape précédente. Le champ **Description** décrit le composant visé par ce micrologiciel. Le champ **Version** décrit la version du micrologiciel de ce composant. InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/UpdateService/FirmwareInventory/ [ID_MICROLOGICIEL] | jq ".Description,.Version"** 
Étape_4	Régler l'heure d'application (apply time) à **Immediate**. InviteSE_OrdinateurDistant:~$ **curl -k -s --request PATCH --url [URL_RACINE] /redfish/v1/UpdateService --header 'Content-Type:application/json' --data '{"HttpPushUriOptions": {"HttpPushUriApplyTime": {"ApplyTime": " Immediate "}}}' | jq** 
Étape_5	Télécharger le micrologiciel en exécutant la commande suivante. Le BMC arrêtera temporairement. InviteSE_OrdinateurDistant:~$ **curl -k -s --request POST --url [URL_RACINE] /redfish/v1/UpdateService --header 'Content-Type: application/octet-stream' --upload-file ' [CHEMIN_ACCÈS_FICHIER]' | jq** 

Étape_6	Une fois le BMC à nouveau disponible, vérifier que la version du micrologiciel a changé.
	InviteSE_OrdinateurDistant:~$ **curl -k -s --request GET --url [URL_RACINE]/redfish/v1/Systems/system | jq.FpgaVersion**
	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/System`
	`  | jq .FpgaVersion`
	`"1.00.0159fce6"`

11.5.6.2.2 Mettre à niveau le micrologiciel du FPGA en utilisant l'interface utilisateur Web

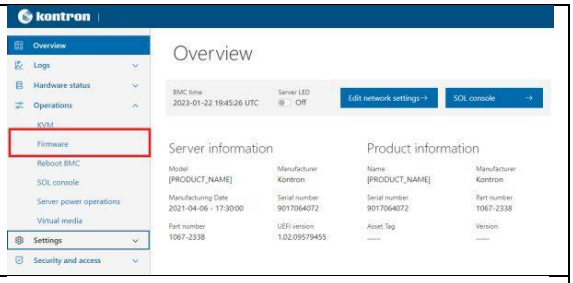
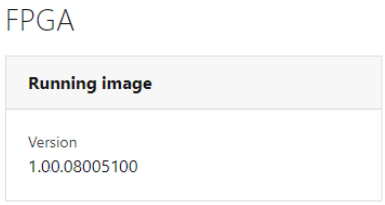
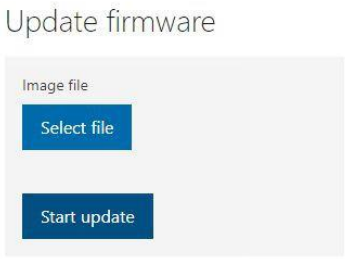
11.5.6.2.2.1 Préalables

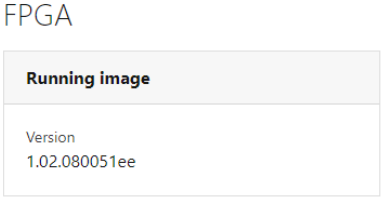
1	Le fichier **.tar** fourni par Kontron a été téléchargé sur l'ordinateur distant.
2	L'accès à l'interface utilisateur Web du BMC est nécessaire.

Section pertinente :

Accéder au BMC en utilisant l'interface utilisateur Web

11.5.6.2.2.2 Procédure

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Operations**, puis sur **Firmware**.	
Étape_2	Vérifier la version actuelle du micrologiciel. S'assurer que le nouveau micrologiciel est plus récent.	
Étape_3	Dans la section **Update firmware**, choisir un fichier **.tar** à télécharger pour le FPGA en cliquant sur **Select file**.	
Étape_4	Cliquer sur **Start update**.	
Étape_5	Lorsque le fichier a été téléchargé avec succès, un message de réussite apparaît dans le coin supérieur droit.	
Étape_6	Attendre que le FPGA se mette à niveau. La page devrait se rafraîchir automatiquement si la mise à niveau est réussie.	

Étape_7	Une fois le FPGA à nouveau disponible, vérifier que la version du micrologiciel a changé.	

11.5.6.3 Mettre à niveau le micrologiciel de l'UEFI/BIOS

Le micrologiciel de l'UEFI/BIOS peut être mis à niveau :

- En utilisant un support virtuel et le shell UEFI intégré

11.5.6.3.1 Mettre à niveau le micrologiciel de l'UEFI/BIOS en utilisant un support virtuel et le shell UEFI intégré

11.5.6.3.1.1 Préalables

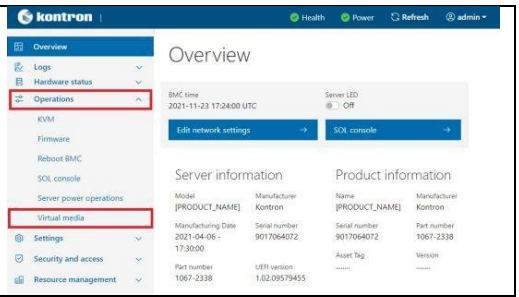
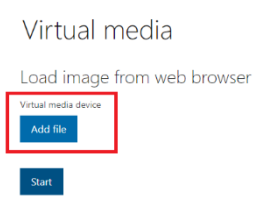
1	Un fichier de média virtuel **.bin** a été fourni par Kontron.
2	L'accès à l'interface utilisateur Web du BMC est nécessaire.
3	Le démarrage sécurisé (Secure Boot) doit être désactivé.

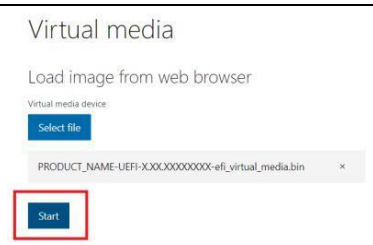
Sections pertinentes :

Accéder à l'UEFI/BIOS

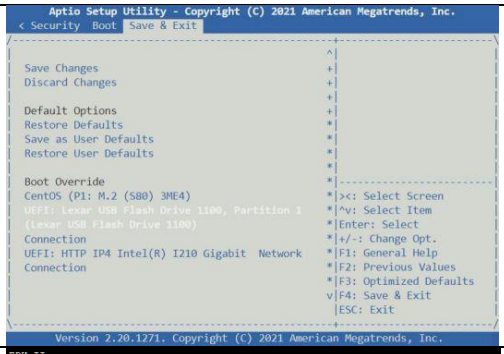
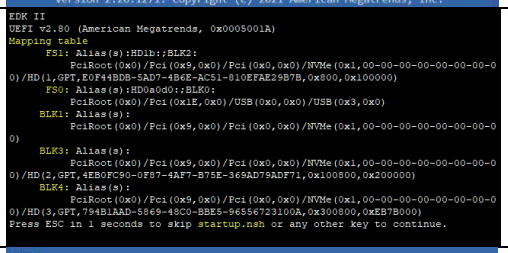
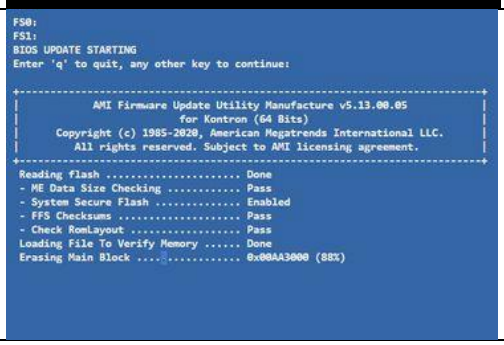
Accéder au BMC en utilisant l'interface utilisateur Web

11.5.6.3.1.2 Monter le support virtuel pour la mise à niveau de l'UEFI/BIOS

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du BMC, cliquer sur **Operations**, puis sur **Virtual media**.	
Étape_2	Cliquer sur **Add file** pour naviguer afin de sélectionner le fichier **.bin** fourni par Kontron.	

Étape_3	Cliquer sur **Start**.	

11.5.6.3.1.3 Mettre à niveau l'UEFI/BIOS

Étape_1	Accéder au menu de configuration de l'UEFI/BIOS.	
Étape_2	Dans le menu de configuration de l'UEFI/BIOS, naviguer jusqu'au menu **Save & Exit**.	
Étape_3	Sélectionner l'option UEFI (shell UEFI intégré) dans le menu **Boot Override**.	
Étape_4	Le shell EFI intégré devrait être lancé. Ne pas appuyer sur aucune touche. Attendre le message "BIOS UPDATE STARTING".	
Étape_5	Lorsque l'invite le demande, appuyer sur n'importe quelle touche autre que "q" pour continuer. La mise à niveau de l'UEFI/BIOS devrait commencer.	
Étape_6	À la fin du processus de mise à niveau, appuyer sur la touche Entrée pour terminer la mise à niveau de l'UEFI/BIOS.	
Étape_7	Une fois cette opération terminée, le BMC et la plateforme se réinitialisent automatiquement. L'exécution du cycle d'alimentation peut prendre plusieurs secondes, et la connexion à distance pourrait être perdue.	

11.5.6.4 Mettre à niveau le micrologiciel du commutateur

NOTE : La configuration de démarrage du commutateur ne sera pas affectée par une mise à niveau du micrologiciel du commutateur.

Le micrologiciel du commutateur peut être mis à niveau :

- En utilisant SCP
- En utilisant l'interface utilisateur Web du NOS

11.5.6.4.1 Mettre à niveau le micrologiciel du commutateur en utilisant SCP

11.5.6.4.1.1 Préalables

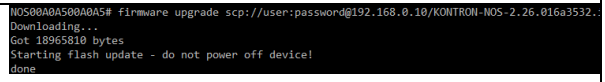
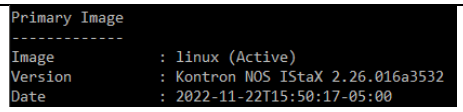
1	Un serveur configuré pour le protocole souhaité est disponible et accessible à partir du NOS.
2	Le fichier **.itb** de mise à niveau fourni par Kontron a été téléchargé sur le serveur.

Section pertinente :

Accéder au NOS

11.5.6.4.1.2 Procédure

L'URL qui suit l'adresse IP du serveur est un chemin relatif au dossier personnel de l'utilisateur ("~/"). Pour spécifier un chemin d'accès absolu, utiliser une double barre oblique après l'adresse IP (ex. scp://[NOM_UTILISATEUR_SERVEUR]:[MOT_DE_PASSE_SERVEUR]@[IP_SERVEUR]//[path/to/filename.itb]).

Étape_1	Accéder au NOS en utilisant SSH ou une connexion série.	
Étape_2	Lancer le téléchargement et la mise à niveau du micrologiciel. InviteCLI_NOSLocal:~# **firmware upgrade scp://[NOM_UTILISATEUR_SERVEUR]:[MOT_DE_PASSE_SERVEUR]@[IP_SERVEUR]/[CHEMIN_ACCÈS_FICHIER] save-host-key**	
Étape_3	Attendre que le commutateur redémarre une fois la mise à niveau terminée.	
Étape_4	Confirmer la réussite de la mise à niveau en vérifiant la version du micrologiciel. InviteCLI_NOSLocal:~# **show version** Dans les résultats, rechercher la version dans la section **Primary Image**. Dans l'image, la version est 2.26.016a3532.	

11.5.6.4.2 Mettre à niveau le micrologiciel du commutateur en utilisant l'interface utilisateur Web du NOS

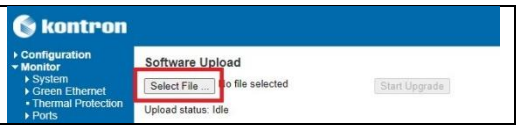
11.5.6.4.2.1 Préalables

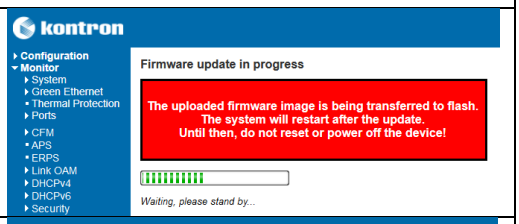
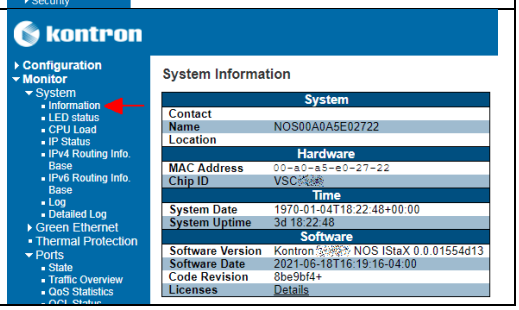
1	L'accès à l'interface utilisateur Web du NOS est nécessaire.
2	Le fichier **.itb** de mise à niveau fourni par Kontron a été téléchargé sur l'ordinateur distant.

Section pertinente :

Accéder au NOS en utilisant l'interface utilisateur Web du NOS

11.5.6.4.2.2 Procédure

Étape_1	Dans le menu de gauche de l'interface utilisateur Web du NOS, cliquer sur **Maintenance**, sur **Software**, puis sur **Upload**.	
Étape_2	Cliquer sur le bouton **Select File** et choisir le fichier **.itb** désiré.	

Étape_3	Après avoir sélectionné le fichier pour la mise à niveau, cliquer sur **Start Upgrade**.	
Étape_4	Attendre la fin du téléchargement et de la mise à niveau.	
Étape_5	Une fois la mise à niveau effectuée, dans le menu de gauche, sélectionner **Monitor**, **System**, puis **Information**. Confirmer que le paramètre **Software Version** correspond à la version du fichier **.itb**.	

11.6 Refroidissement et gestion thermique de la plateforme

Sections pertinentes :

Considérations environnementales

Liste des capteurs

Configurer les capteurs et les paramètres thermiques

La plateforme ME1310 peut fonctionner dans une plage de température ambiante de :

- -40 °C à +65 °C lorsqu'un bloc d'alimentation CC est utilisé
- -5 °C à +50 °C lorsqu'un bloc d'alimentation CA est utilisé

Les ventilateurs pourraient ne pas fonctionner lorsque la température ambiante est inférieure à 10 °C.

11.6.1 Comportement au démarrage à des températures inférieures à 0 degré Celsius

Le système est conçu pour fonctionner dans un environnement froid, mais pour que tous les composants fonctionnent dans leur plage de température spécifiée, le système doit être chauffé avant son démarrage. Des éléments chauffants sont intégrés pour le CPU et, en option, pour les cartes d'expansion PCIe.

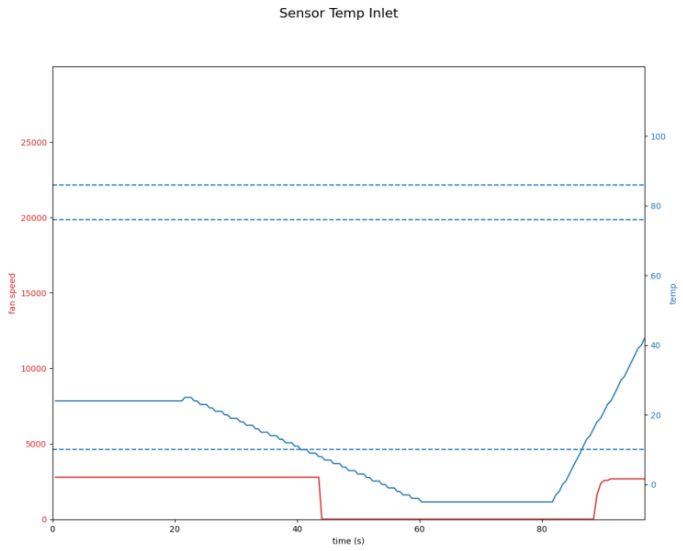
- Lorsque la plateforme est mise sous tension à des températures inférieures à 0 °C, un élément chauffant interne préchauffe les composants sensibles au froid avant le démarrage de la carte.
- Lorsque la température de ces composants dépasse 0 °C, le serveur démarre.

Ce comportement est communiqué au moyen des DEL de la plateforme. Pour plus d'information, voir DEL générales de la plateforme.

11.6.2 Comportement à des températures inférieures ou supérieures à 10 degrés Celsius

La température ambiante est mesurée par le capteur Temp Inlet.

- Lorsque la **température ambiante est inférieure à 10 °C** et qu'aucun capteur n'a dépassé ses seuils de température, les ventilateurs sont en veille (ils ne fonctionnent pas et n'émettent aucun son).
- Lorsque la **température ambiante est supérieure à 10 °C**, les ventilateurs se mettent en marche et fonctionnent à 8 % de leur capacité maximale.
- Si, à n'importe quelle température ambiante, il est détecté qu'un capteur atteint son seuil non critique supérieur, le refroidissement produit par les ventilateurs s'enclenche pour s'assurer qu'aucun composant ne surchauffe.



11.6.3 Gestion du refroidissement

La gestion du refroidissement de la plateforme est assurée par un BMC intégré.

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. Pour chaque capteur, la lecture de température est comparée aux seuils configurés correspondants afin de déterminer la vitesse de ventilation requise. Le cycle de service qui en résulte est basé sur les paramètres de refroidissement, tels que la vitesse minimale et maximale du ventilateur, et augmente de façon linéaire lorsqu'une température se situe entre les seuils non critique supérieur et critique supérieur pour ce capteur. Le contrôle du comportement des ventilateurs peut être ajusté en configurant ces seuils afin qu'ils s'harmonisent à l'environnement cible.

Outre les capteurs lus par le BMC, d'autres capteurs peuvent être lus par une application client installée et fonctionnant sous le système d'exploitation du serveur. L'information sur ces capteurs est ensuite transmise au BMC. Ainsi, les températures des cartes d'expansion PCIe, ainsi que les températures des disques de stockage M.2 et des modules SFP, peuvent être communiquées au BMC par l'application client et prises en compte par le régulateur de vitesse des ventilateurs dans son calcul pour la fonction de gestion thermique.

Les seuils de ces capteurs peuvent également être configurés.

11.6.3.1 Caractéristiques de la gestion du refroidissement

- La vitesse minimale des ventilateurs est fixée à 8 %.
- La température ambiante minimale est fixée à 10 °C. Au-delà de cette température, les ventilateurs fonctionnent. En dessous de cette température, les ventilateurs sont arrêtés, mais prêts à démarrer si un composant a besoin d'être refroidi.
- Les ventilateurs sont démarrés avant d'atteindre leur valeur seuil à l'aide d'un paramètre de décalage du seuil.
- L'écart de vitesse des ventilateurs est surveillé pour détecter toute défaillance.

- Une horloge de surveillance règle les ventilateurs à 100 % si le BMC n'émet pas de commandes de contrôle. Cela se produit normalement lorsque le BMC redémarre, par exemple lors d'une mise à jour du micrologiciel.
- Un processus de mise à niveau sans échec du BMC règle la vitesse des ventilateurs à 100 % pendant un redémarrage ou une mise à niveau du micrologiciel du BMC.
- Une petite réduction de la valeur de la commande de vitesse est appliquée à la vitesse des ventilateurs pour assurer une diminution lente de la vitesse des ventilateurs et empêcher l'oscillation des ventilateurs.
- Réponse rapide à une augmentation de la température.
- Redondance des ventilateurs.

11.6.3.2 Méthode de détection de défaillance des ventilateurs

Pour détecter les ventilateurs défectueux, la vitesse de chaque ventilateur est surveillée en permanence et comparée à la valeur cible envoyée par le contrôleur des ventilateurs. Si la vitesse d'un ventilateur est hors de sa plage de ±15 % pendant 30 secondes, le ventilateur est considéré comme défectueux et un événement Redfish est envoyé. L'état du ventilateur peut être rétabli ultérieurement si la vitesse revient dans sa plage pendant une période stable de 5 secondes.

Tous les ventilateurs sont redondants. Cela signifie que lorsqu'un ventilateur est défectueux, tous les autres ventilateurs sains sont réglés sur la vitesse maximale.


```
{
    "@odata.context": "/redfish/v1/$metadata#LogEntry.LogEntry",
    "@odata.id": "/redfish/v1/Systems/system/LogServices/EventLog/Entries/#1614699759_4",
    "@odata.type": "#LogEntry.v1_4_0.LogEntry",
    "Created": "2021-03-02T15:42:39+00:00",
    "EntryType": "Event",
    "Id": "1614699759_4",
    "Message": "Fan_1 speed deviated.",
    "MessageArgs": [
        "Fan_1"
    ],
    "MessageId": "OpenBMC.0.1.FanSpeedDeviated",
    "Name": "System Event Log Entry",
    "Severity": "OK"
},
 {
    "@odata.context": "/redfish/v1/$metadata#LogEntry.LogEntry",
    "@odata.id": "/redfish/v1/Systems/system/LogServices/EventLog/Entries/#1614699764_4",
    "@odata.type": "#LogEntry.v1_4_0.LogEntry",
    "Created": "2021-03-02T15:42:44+00:00",
    "EntryType": "Event",
    "Id": "1614699764_4",
    "Message": "Fan_1 speed restored.",
    "MessageArgs": [
        "Fan_1"
    ],
    "MessageId": "OpenBMC.0.1.FanSpeedRestored",
    "Name": "System Event Log Entry",
    "Severity": "OK"
},
```


Pour accéder au SEL en utilisant Redfish afin de voir les événements, voir Journal des événements système.

11.6.4 Seuils de température par défaut

Pour connaître les seuils de température, voir les instructions fournies dans les sections Surveillance des capteurs et Configurer les capteurs et les paramètres thermiques.

12/ Dépannage

12.1 Collecte des diagnostics

Les informations suivantes pourraient être nécessaires lorsque vous communiquez avec l'équipe du soutien afin d'établir un bon diagnostic de l'état de la carte. Toutefois, si la plateforme est non fonctionnelle, certaines informations peuvent être récupérées à l'aide du code QR.

12.1.1 Recueillir l'inventaire du système

Les informations suivantes pourraient être utilisées afin d'établir un bon diagnostic de l'état de la carte. Voir Inventaire du système.

- Données FRU
- Version du micrologiciel du FPGA, de l'UEFI et du BMC
- Type de bloc d'alimentation
- Informations sur le module d'E/S du produit
- Informations sur le processeur
- Configuration des modules de mémoire
- Unités de stockage
- Configuration de l'UEFI/BIOS
- Configuration actuelle du commutateur Ethernet
- Versions du commutateur Ethernet

12.1.2 Recueillir les journaux des événements

Plusieurs journaux des événements pourraient être utilisés afin d'établir un bon diagnostic de l'état de la carte.

- Journal des événements du BMC Voir Journal des événements système du BMC.
- Journal des événements du NOS. Voir Journal des événements système du NOS.
- Codes POST de l'UEFI/BIOS (optionnel). Voir Journaux des codes POST.

12.1.3 Recueillir de l'information sur le système avec le code QR

Section pertinente :

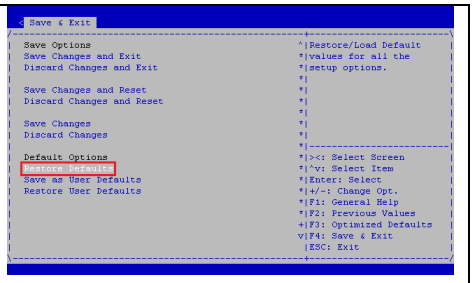
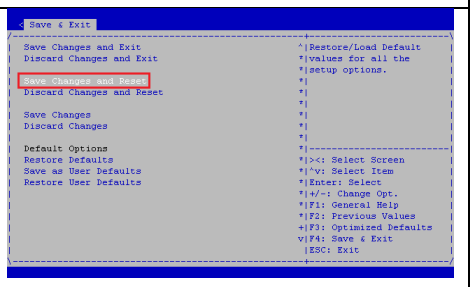
Adresses MAC

Étape_1	À l'aide d'une application de code QR, scanner le code QR de la plateforme. Enregistrer les informations obtenues dans votre appareil (par exemple en faisant une capture d'écran). S/N:9017020001 = Numéro de série de la plateforme P/N:1065-2823 = Numéro de pièce de la plateforme BATCH:0A00000001 = Numéro de lot de production de la plateforme MAC : 00A0A5D6402A = Première adresse MAC attribuée au BMC/serveur. Valeur à utiliser pour remplacer MAC_BASE. 00A0A5E1B934 = Première adresse MAC attribuée au commutateur Ethernet intégré. Valeur à utiliser pour remplacer SW_MAC_BASE. Cette information n'est présente que pour une plateforme configurée avec le module d'E/S de commutation Ethernet.	S/N:9017020001 P/N:1065-2823 BATCH:0A00000001 MAC: 00A0A5D6402A 00A0A5E1B934

12.2 Configurations par défaut

12.2.1 Rétablir les paramètres par défaut de l'UEFI/BIOS

Voir Accéder à l'UEFI/BIOS pour les instructions d'accès.

Étape_1	Dans le menu de configuration de l'UEFI/BIOS, naviguer jusqu'au menu **Save & Exit** et sélectionner **Restore Defaults**.	
Étape_2	Sélectionner **Save Changes and Reset**.	
Étape_3	Attendre que le système se réinitialise. Les paramètres du UEFI/BIOS devraient avoir été réinitialisés aux configurations par défaut.	

12.2.2 Rétablir les paramètres par défaut du NOS

Faire preuve de prudence lors du rétablissement des paramètres par défaut. Votre accès aux composants du système pourrait être interrompu en raison de modifications de la configuration du réseau. Voir Description des méthodes d'accès au système pour sélectionner une méthode appropriée pour accéder aux composants de la plateforme.

12.2.2.1 Rétablir les paramètres par défaut du NOS en utilisant le CLI

Voir Accéder au NOS pour les instructions d'accès.

NOTE : Cette procédure équivaut à réinitialiser les configurations par défaut du commutateur. Toutes les modifications apportées à la configuration seront perdues.

Étape_1	Rétablir la configuration par défaut. InviteCLI_NOSLocal:~# **reload defaults**	`# reload defaults` `% Reloading defaults. Please stand by.`

Étape_2	Pour rendre le retour aux valeurs par défaut permanent, utiliser la commande suivante.
	InviteCLI_NOSLocal:~# **copy running-config startup-config**
		`# copy running-config startup-config`
		`Building configuration...`
		`% Saving 1555 bytes to flash:startup-config`

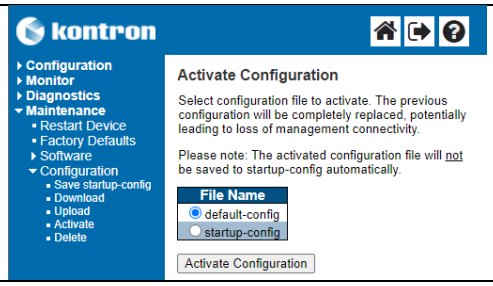
12.2.2.2 Rétablir les paramètres par défaut du NOS en utilisant l'interface utilisateur Web

Voir Accéder au NOS pour les instructions d'accès.

Pour préserver les configurations, la configuration actuelle doit être sauvegardée dans startup-config. Voir Sauvegarder la configuration actuelle en utilisant l'interface utilisateur Web.

NOTE : Cette procédure équivaut à réinitialiser les configurations par défaut du commutateur. Toutes les modifications apportées à la configuration seront perdues.

Étape_1	Dans le menu de gauche, sélectionner **Maintenance**, **Configuration** puis **Activate**.	
Étape_2	Cliquer sur le bouton radio **default-config**.	

Étape_3	Appuyer sur le bouton **Activate Configuration** pour confirmer.	
Étape_4	(Optionnel) Pour rendre la modification persistante, enregistrer la configuration actuelle (running-config) dans la configuration de démarrage (startup-config).	

12.2.3 Rétablir un mot de passe du BMC

Le mot de passe de l'administrateur du BMC peut être rétabli en utilisant la méthode Accéder au BMC en utilisant IPMI (KCS).

Étape_1	Identifier l'ID de l'utilisateur avec le mot de passe à rétablir.
	InviteSE_ServeurLocal:~# **ipmitool user list [CANAL]**
		`# ipmitool user list 1`
		`ID  Name             Callin  Link Auth  IPMI Msg   Channel Priv Limit`
		`1   admin            false   true       true        ADMINISTRATOR`
		`2   mynewuser        false   true       true        ADMINISTRATOR`
		`3                    true    false      false       NO ACCESS`
		`4                    true    false      false       NO ACCESS`

Étape_2	Réinitialiser le mot de passe. InviteSE_ServeurLocal:~# **ipmitool user set password [ID_UTILISATEUR] [NOUVEAU_MOT_DE_PASSE]**	`# ipmitool user set password 1 "newpassword123456"`

12.3 Obtenir du soutien

Pour assurer un traitement rapide de votre demande de soutien, Kontron recommande de recueillir l'inventaire du système et les diagnostics pertinents. L'équipe du soutien technique de Kontron peut être jointe par les moyens suivants :

- Par téléphone : 1-888-835-5575
- Par courriel : support-na@kontron.com
- Via le site Web : www.kontron.com

Pour obtenir des informations sur les ventes, y compris sur les options de produits actuelles et futures, veuillez contacter le soutien des ventes de Kontron au Canada par les moyens suivants :

- Par téléphone : 1-800-3 87-4222
- Par courriel : gss-com@kontron.com

13/ Base de connaissances

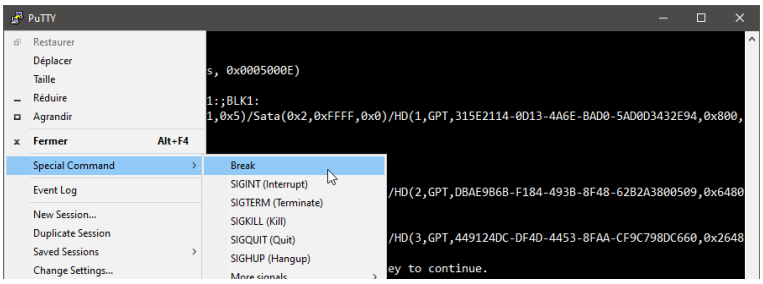
13.1 Envoi d'une commande BREAK sur une connexion série

La documentation fait référence à la possibilité de réinitialiser un serveur Kontron en utilisant un signal spécial appelé commande BREAK.

Voici des méthodes pour envoyer une commande BREAK avec divers émulateurs de terminal et d'autres types de connexions série.

13.1.1 PuTTY

PuTTY accepte la combinaison de touches Ctrl et Pause/Break (les claviers modernes indiquent souvent uniquement Pause). Le signal peut également être envoyé via le menu de l'application. Un exemple est présenté dans l'image ci-dessous.



13.1.2 Minicom

Un signal **BREAK** peut être envoyé à partir de l'aide de l'utilitaire minicom de Linux.

```
|          Minicom Command Summary    |
| Commands can be called by CTRL-A <key> |
|          Main Functions  |
...
| send break.........F       |
```

13.1.3 Picocom

Un signal **BREAK** peut être envoyé à partir de l'aide de l'utilitaire picocom de Linux.

```
*** Picocom commands (all prefixed by [C-a])
...
*** [C-|]: Send break
```

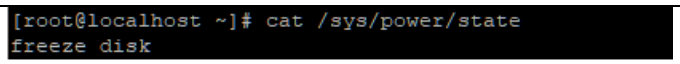
13.1.4 Serveurs de console série

Il existe également des serveurs dédiés qui mettent en œuvre de nombreuses connexions série physiques qui sont ensuite accessibles via un réseau en utilisant des clients Telnet ou SSH, par exemple. Ces serveurs de console série permettent généralement de configurer une combinaison ou une séquence de touches pour chaque port qui enverra une commande BREAK à l'équipement connecté. Reportez-vous au manuel de votre équipement pour plus d'informations.

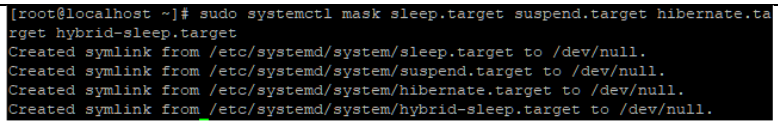
13.1.5 Désactiver les états de veille sous Linux

Sous Linux, les états de veille ne sont pas contrôlés exclusivement par les définitions des tables ACPI. Ils sont également contrôlés par le système d'exploitation. Voir Accéder au système d'exploitation d'un serveur pour les instructions d'accès.

13.1.6 Vérifier les états de veille activés

Étape_1	Vérifier les états de veille activés InviteSE_ServeurLocal:~# **cat /sys/power/state**	

13.1.7 Désactiver les états de veille

Étape_1	Désactiver les états de veille avec systemd. InviteSE_ServeurLocal:~# **sudo systemctl mask sleep.target suspend.target hibernate.target hybrid- sleep.target**	

14/ Notes d'application

14.1 Générer des clés de démarrage sécurisé personnalisées

Section pertinente :

Installer des clés de démarrage sécurisé personnalisées

Pour installer des clés de démarrage sécurisé personnalisées, il peut être nécessaire de générer des clés. Cet article fournit un exemple utilisant CentOS 7.

14.1.1 Préalables

1	Les paquets efitools et sbsigntools doivent être disponibles. Ces paquets ne sont pas des paquets officiels de CentOS.

14.1.2 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.

14.2 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 sécurisé à partir de l'utilitaire de configuration UEFI

14.2.2.1 Préalables

1	Un ensemble de clés de démarrage sécurisé 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.

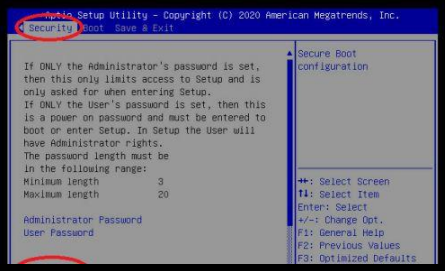
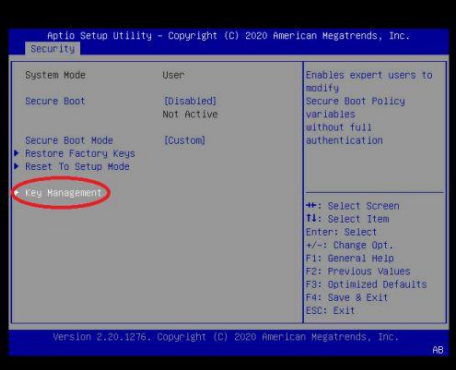
Section pertinente :

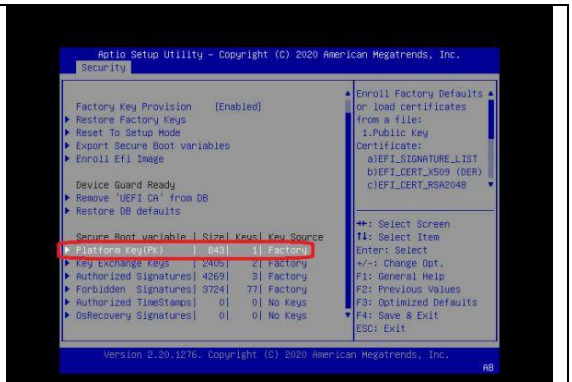
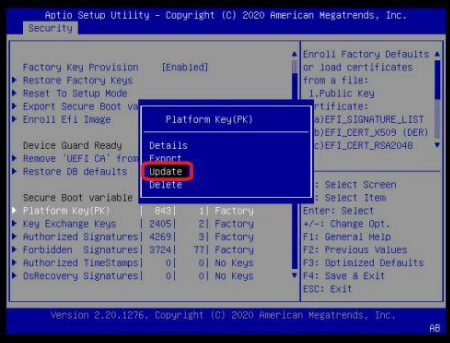
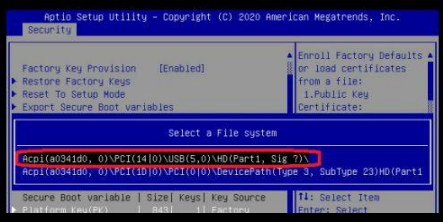
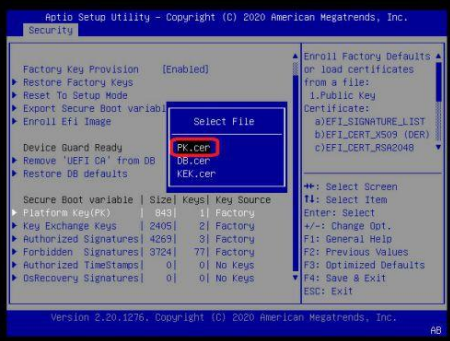
Générer des clés de démarrage sécurisé personnalisées

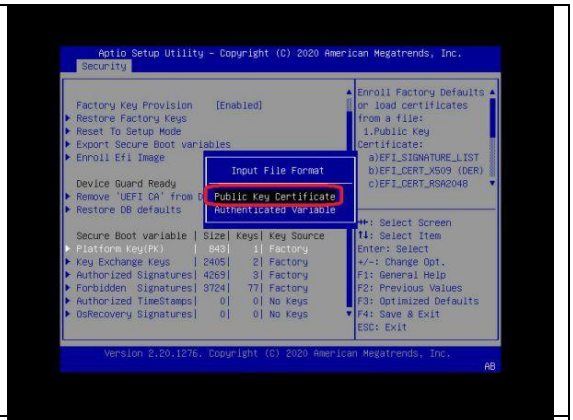
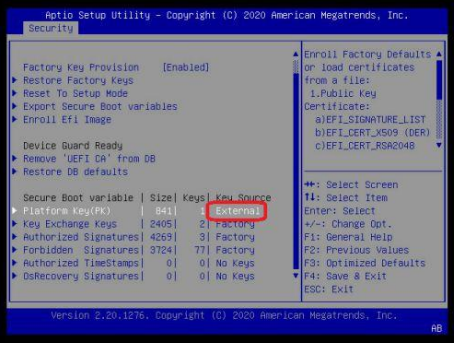
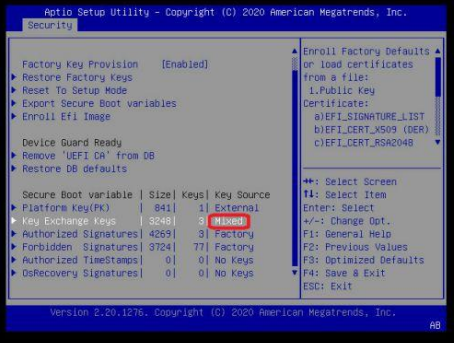
Puisque la date et l'heure actuelles sont vérifiées par rapport aux estampilles temporelles des certificats par mesure de sécurité, s'assurer que la date et l'heure du système sont valides avant de manipuler les variables du démarrage sécurisé. Si ce n'est pas le cas, une erreur de violation de la sécurité (security violation) sera obtenue et aucune modification ne sera possible.

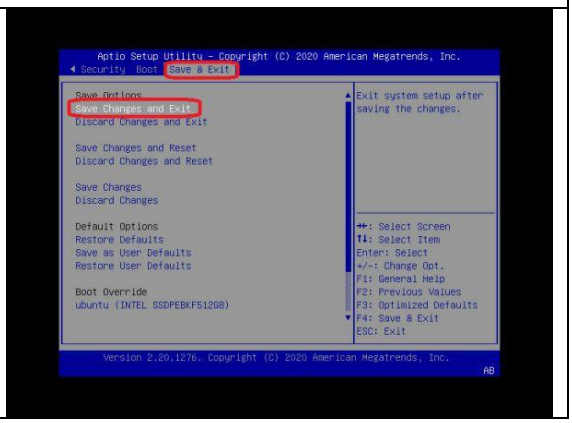
14.2.2.2 Procédure

Voir Accéder à l'UEFI/BIOS pour les instructions d'accès.

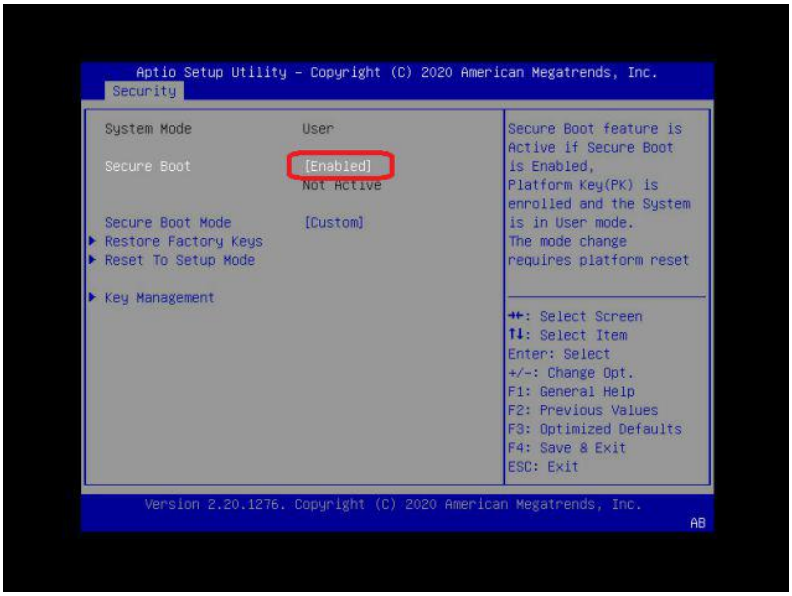
Étape_1	Accéder à l'utilitaire de configuration UEFI en appuyant sur **F2** ou **Suppr [DEL]** lorsque l'écran d'ouverture de session s'affiche pendant le démarrage.	
Étape_2	À partir de l'onglet **Security**, accéder au sous-menu **Secure Boot**.	
Étape_3	Accéder à la page Key Management en sélectionnant 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.	
Étape_12	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.	
Étape_13	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.	

Étape_14	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.	
Étape_15	Sélectionner **Save Changes and Exit** dans le menu.	

Pour profiter de la fonction de démarrage sécurisé, elle doit être activée (Security → sous-menu Secure Boot).



15/ Guides de référence

15.1 Commandes Redfish prises en charge

Les descriptions ne sont pas traduites puisqu'il s'agit de la norme Redfish.

Les informations sont présentées dans le format suivant :

Description | URL | Type

Définition du schéma

La définition du schéma pour un type spécifique peut être récupérée à https://redfish.dmtf.org

15.1.1 URL des systèmes (Systems)

- Collection of computer systems | /redfish/v1/Systems | ComputerSystemCollection
- Information about a specified system | /redfish/v1/Systems/[SYSTEM_INSTANCE] | ComputerSystem.v1_15_0
- Computer system reset action | /redfish/v1/Systems/[SYSTEM_INSTANCE]/ResetActionInfo | ActionInfo.v1_1_2
- Collection of memory devices for this system | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Memory | MemoryCollection
- Collection of processors | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Processors | ProcessorCollection
- Collection of storage devices for this system | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Storage | StorageCollection
- Collection of log services for this system | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices | LogServiceCollection
- EventLog service | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices/EventLog | LogService.v1_1_0
- Collection of EventLog entries | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices/EventLog/Entries | LogEntryCollection
- PostCodes services | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices/PostCodes | LogService.v1_1_0
- Collection of PostCodes entries | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices/PostCodes/Entries | LogEntryCollection
- Information about BIOS Configuration Service | /redfish/v1/Systems/system/Bios | Bios.v1_1_0

15.1.2 URL des gestionnaires (Managers)

- Collection of managers | /redfish/v1/Managers | ManagerCollection
- Information about a specified manager | /redfish/v1/[MANAGER_INSTANCE] | Manager.v1_11_0
- Collection of Ethernet interfaces for a specified manager | /redfish/v1/Managers/[MANAGER_INSTANCE]/EthernetInterfaces | EthernetInterfaceCollection
- Information about a specified Ethernet interface | /redfish/v1/Managers/[MANAGER_INSTANCE]/EthernetInterfaces/[ETHERNET_INTERFACE_INSTANCE] | EthernetInterface.v1_4_1
- Cold reset action for this manager | /redfish/v1/Managers/[MANAGER_INSTANCE]/ResetActionInfo | ActionInfo.v1_1_2
- Collection of network protocol information | /redfish/v1/Managers/[MANAGER_INSTANCE]/NetworkProtocol | ManagerNetworkProtocol.v1_5_0
- Collection of HTTPS Certificates | /redfish/v1/Managers/bmc/NetworkProtocol/HTTPS/Certificates | CertificateCollection
- Collection of Trustore certificates | /redfish/v1/Managers/bmc/Truststore/Certificates | CertificateCollection

15.1.3 URL des registres (Registries)

- Registry repository | /redfish/v1/Registries | MessageRegistryFileCollection
- Summary of a specified registry | /redfish/v1/Registries/[REGISTRY_INSTANCE] | MessageRegistryFile.v1_1_0
- Detailed information about a specified registry | /redfish/v1/Registries/[REGISTRY_INSTANCE.JSON] | MessageRegistryFile.v1_1_0

15.1.4 URL du service de sessions (SessionService)

- Session service | /redfish/v1/SessionService | SessionService.v1_0_2
- Collection of sessions | /redfish/v1/SessionService/Sessions | SessionCollection
- Information about a specified session | /redfish/v1/SessionService/Sessions/[SESSION_ID] | Session.v1_3_0

15.1.5 URL du service des tâches (TaskService)

- Task service | /redfish/v1/TaskService | TaskService.v1_1_4
- Task collection | /redfish/v1/TaskService/Tasks | TaskCollection

15.1.6 URL du service de télémétrie (TelemetryService)

- Information about the telemetry service | /redfish/v1/TelemetryService | TelemetryService.v1_2_1
- Collection of metric definitions | /redfish/v1/TelemetryService/MetricReportDefinitions | MetricReportDefinitionCollection Information about a specified metric definition | /redfish/v1/TelemetryService/MetricReportDefinitions/[METRIC_REPORT_DEF] | MetricReportDefinition.v1_3_0
- Collection of metric reports | /redfish/v1/TelemetryService/MetricReports | MetricReportCollection
- Information about a specified metric report instance | /redfish/v1/TelemetryService/MetricReports/[METRIC_REPORT_INSTANCE] | MetricReport.v1_3_0

15.1.7 URL du châssis (Chassis)

- Chassis collection | /redfish/v1/Chassis | ChassisCollection
- Information about a specified chassis instance | /redfish/v1/Chassis/[CHASSIS_INSTANCE] | Chassis.v1_14_0
- Resets the chassis | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/ResetActionInfo | ActionInfo.v1_1_2
- Collection of voltage sensors | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/Power | Power.v1_5_2
- Collection of thermal sensors | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/Thermal | Thermal.v1_4_0

15.1.8 URL du service de comptes (AccountService)

- Redfish account service | /redfish/v1/AccountService | AccountService.v1_5_0
- Collection of Redfish user accounts | /redfish/v1/AccountService/Accounts | ManagerAccountCollection
- Information about a specified Redfish account | /redfish/v1/AccountService/Accounts/[ACCOUNT_INSTANCE] | ManagerAccount.v1_4_0
- Collection of available roles | /redfish/v1/AccountService/Roles | RoleCollection
- Information about a specified role | /redfish/v1/AccountService/Roles/[ROLE_INSTANCE] | Role.v1_2_2
- Collection of account LDAP Certificates | /redfish/v1/AccountService/LDAP/Certificates | CertificateCollection

15.1.9 URL du service de certificats (CertificateService)

- Certificate service | /redfish/v1/CertificateService | CertificateService.v1_0_0
- Certificate service locations | /redfish/v1/CertificateService/CertificateLocations | CertificateLocations.v1_0_0

15.1.10 URL du service de mise à jour (UpdateService)

- Redfish update service | /redfish/v1/UpdateService | UpdateService.v1_5_0
- Collection of firmware images | /redfish/v1/UpdateService/FirmwareInventory | SoftwareInventoryCollection

15.1.11 URL du service d'événements (EventService)

- Event service | /redfish/v1/EventService | EventService.v1_5_0
- Collection of current event subscriptions | /redfish/v1/EventService/Subscriptions | EventDestinationCollection

15.1.12 URL divers

- List of OEM JSON schemas and extensions | /redfish/v1/JsonSchemas
- Information about a specified JSON schema | /redfish/v1/JsonSchemas/[JSON_SCHEMA_NAME]

15.2 Commandes IPMI prises en charge

15.2.1 Commandes d'application

15.2.1.1 Commandes IPM pour l'unité

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x06	0x01	Get Device ID	Prise en charge
0x06	0x02	Cold Reset	Prise en charge
0x06	0x03	Warm Reset	Non prise en charge
0x06	0x04	Get Self Test Results	Prise en charge
0x06	0x05	Manufacturing Test On	Non prise en charge
0x06	0x06	Set ACPI Power State	Prise en charge
0x06	0x07	Get ACPI Power State	Non prise en charge*
0x06	0x08	Get Device GUID	Prise en charge
0x06	0x09	Get NetFn Support	Non prise en charge
0x06	0x0A	Get Command Support	Non prise en charge
0x06	0x0C	Get Configurable Commands	Non prise en charge
0x06	0x60	Set Command Enables	Non prise en charge
0x06	0x61	Get Command Enables	Non prise en charge
0x06	0x64	Get OEM NetFn IANA Support	Non prise en charge
0x06	0x0B	Get Command Sub-function Support	Non prise en charge
0x06	0x0D	Get Configurable Command Sub-functions	Non prise en charge
0x06	0x62	Set Command Sub-function Enables	Non prise en charge
0x06	0x63	Get Command Sub-function Enables	Non prise en charge
0x06	0x52	Master Write-Read	Non prise en charge

* Les commandes ne sont pas rejetées et peuvent entraîner un comportement imprévisible.

15.2.1.2 Commandes de l'horloge de surveillance (watchdog timer)

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x06	0x22	Reset Watchdog Timer	Prise en charge
0x06	0x24	Set Watchdog Timer	Prise en charge
0x06	0x25	Get Watchdog Timer	Prise en charge

15.2.1.3 Commandes associées à l'unité et aux messages BMC

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x06	0x2E	Set BMC Global Enables	Prise en charge
0x06	0x2F	Get BMC Global Enables	Prise en charge
0x06	0x30	Clear Message Flags	Prise en charge
0x06	0x31	Get Message Flags	Prise en charge
0x06	0x32	Enable Message Channel Receive	Non prise en charge
0x06	0x33	Get Message	Prise en charge

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x06	0x34	Send Message	Prise en charge
0x06	0x35	Read Event Message Buffer	Prise en charge
0x06	0x36	Get BT Interface Capabilities	Prise en charge
0x06	0x37	Get System GUID	Prise en charge
0x06	0x38	Get Channel Authentication Capabilities	Prise en charge
0x06	0x39	Get Session Challenge	Non prise en charge
0x06	0x3A	Activate Session	Non prise en charge
0x06	0x3B	Set Session Privilege Level	Prise en charge
0x06	0x3C	Close Session	Prise en charge
0x06	0x3D	Get Session Info	Prise en charge
0x06	0x3F	Get AuthCode	Non prise en charge
0x06	0x40	Set Channel Access	Prise en charge
0x06	0x41	Get Channel Access	Prise en charge
0x06	0x42	Get Channel Info Command	Prise en charge
0x06	0x43	Set User Access Command	Prise en charge
0x06	0x44	Get User Access Command	Prise en charge
0x06	0x45	Set User Name	Prise en charge
0x06	0x46	Get User Name Command	Prise en charge
0x06	0x47	Set User Password Command	Prise en charge
0x06	0x52	Master Write-Read	Non prise en charge
0x06	0x58	Set System Info Parameters	Prise en charge
0x06	0x59	Get System Info Parameters	Prise en charge

15.2.1.4 Commandes spécifiques à IPMI 2.0

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x06	0x48	Activate Payload	Prise en charge
0x06	0x49	Deactivate Payload	Prise en charge
0x06	0x4A	Get Payload Activation Status	Prise en charge
0x06	0x4B	Get Payload Instance Info	Prise en charge
0x06	0x4C	Set User Payload Access	Prise en charge
0x06	0x4D	Get User Payload Access	Prise en charge
0x06	0x4E	Get Channel Payload Support	Prise en charge
0x06	0x4F	Get Channel Payload Version	Prise en charge
0x06	0x50	Get Channel OEM Payload Info	Non prise en charge
0x06	0x54	Get Channel Cipher Suites	Prise en charge
0x06	0x55	Suspend/Resume Payload Encryption	Non prise en charge
0x06	0x56	Set Channel Security Keys	Non prise en charge
0x06	0x57	Get System Interface Capabilities	Non prise en charge

15.2.2 Commandes de châssis

15.2.2.1 Commandes de châssis de l'unité

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x00	0x00	Get Chassis Capabilities	Prise en charge
0x00	0x01	Get Chassis Status	Prise en charge
0x00	0x02	Chassis Control	Prise en charge
0x00	0x04	Chassis Identify	Prise en charge
0x00	0x05	Set Chassis Capabilities	Prise en charge
0x00	0x06	Set Power Restore Policy	Prise en charge
0x00	0x07	Get System Restart Cause	Non prise en charge*
0x00	0x08	Set System Boot Options	Prise en charge
0x00	0x09	Get System Boot Options	Prise en charge
0x00	0x0A	Set Front Panel Button Enables	Non prise en charge*
0x00	0x0B	Set Power Cycle Interval	Non prise en charge

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x00	0x0F	Get POH Counter	Non prise en charge*

* Les commandes ne sont pas rejetées et peuvent entraîner un comportement imprévisible.

15.2.3 Commandes de pont (bridge)

15.2.3.1 Commandes de gestion de pont

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x02	0x00	Get Bridge State	Non prise en charge
0x02	0x01	Set Bridge State	Non prise en charge
0x02	0x02	Get ICMB Address	Non prise en charge
0x02	0x03	Set ICMB Address	Non prise en charge
0x02	0x04	Set Bridge Proxy Address	Non prise en charge
0x02	0x05	Get Bridge Statistics	Non prise en charge
0x02	0x06	Get ICMB Capabilities	Non prise en charge
0x02	0x08	Clear Bridge Statistics	Non prise en charge
0x02	0x09	Get Bridge Proxy Address	Non prise en charge
0x02	0x0A	Get ICMB Connector Info	Non prise en charge

15.2.3.2 Commandes de découverte de pont

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x02	0x10	Prepare For Discovery	Non prise en charge
0x02	0x11	Get Addresses	Non prise en charge
0x02	0x12	Set Discovered	Non prise en charge
0x02	0x13	Get Chassis Device Id	Non prise en charge
0x02	0x14	Set Chassis Device Id	Non prise en charge

15.2.3.3 Commandes de pontage (bridging)

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x02	0x20	Bridge Request	Non prise en charge
0x02	0x21	Bridge Message	Non prise en charge

15.2.3.4 Commandes d'événements de pont

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x02	0x30	Get Event Count	Non prise en charge
0x02	0x31	Set Event Destination	Non prise en charge
0x02	0x32	Set Event Reception State	Non prise en charge
0x02	0x33	Send ICMB Event Message	Non prise en charge
0x02	0x34	Get Event Destination	Non prise en charge
0x02	0x35	Get Event Reception State	Non prise en charge

15.2.4 Commandes d'événements de capteurs (sensor)

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x04	0x16	Alert Immediate	Non prise en charge
0x04	0x11	Arm PEF Postpone Timer	Non prise en charge
0x04	0x01	Get Event Receiver	Non prise en charge
0x04	0x10	Get PEF Capabilities	Non prise en charge
0x04	0x13	Get PEF Configuration Parameters	Non prise en charge
0x04	0x15	Get Last Processed Event ID	Non prise en charge
0x04	0x20	Get Device SDR Info	Prise en charge
0x04	0x21	Get Device SDR	Prise en charge

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x04	0x23	Get Sensor Reading Factors	Non prise en charge
0x04	0x25	Get Sensor Hysteresis	Non prise en charge
0x04	0x27	Get Sensor Threshold	Prise en charge
0x04	0x29	Get Sensor Event Enable	Prise en charge
0x04	0x2B	Get Sensor Event Status	Prise en charge
0x04	0x2D	Get Sensor Reading	Prise en charge
0x04	0x2F	Get Sensor Type	Prise en charge
0x04	0x17	PET Acknowledge	Non prise en charge
0x04	0x02	Platform Event	Prise en charge
0x04	0x2A	Re-arm Sensor Events	Non prise en charge
0x04	0x22	Reserve Device SDR Repository	Prise en charge
0x04	0x00	Set Event Receiver	Non prise en charge
0x04	0x12	Set PEF Configuration Parameters	Non prise en charge
0x04	0x14	Set Last Processed Event ID	Non prise en charge
0x04	0x24	Set Sensor Hysteresis	Non prise en charge
0x04	0x26	Set Sensor Threshold	Prise en charge
0x04	0x28	Set Sensor Event Enable	Non prise en charge
0x04	0x2E	Set Sensor Type	Non prise en charge
0x04	0x30	Set Sensor Reading And Event Status	Prise en charge

15.2.5 Commandes de stockage

15.2.5.1 Commandes d'information FRU

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x0a	0x10	Get FRU Inventory Area Info	Prise en charge
0x0a	0x11	Read FRU Data	Prise en charge
0x0a	0x12	Write FRU Data	Prise en charge

15.2.5.2 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
0x0a	0x20	Get SDR Repository Info	Prise en charge
0x0a	0x21	Get SDR Repository Allocation Info	Prise en charge
0x0a	0x22	Reserve SDR Repository	Prise en charge
0x0a	0x23	Get SDR	Prise en charge
0x0a	0x24	Add SDR	Non prise en charge
0x0a	0x25	Partial Add SDR	Non prise en charge
0x0a	0x27	Clear SDR Repository	Non prise en charge
0x0a	0x28	Get SDR Repository Time	Non prise en charge
0x0a	0x2C	Run Initialization Agent	Non prise en charge
0x0a	0x26	Delete SDR Repository	Non prise en charge

15.2.5.3 Commandes du SEL

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x0a	0x40	Get SEL Info	Prise en charge
0x0a	0x41	Get SEL Allocation Info	Non prise en charge
0x0a	0x42	Reserve SEL	Prise en charge
0x0a	0x43	Get SEL Entry	Prise en charge
0x0a	0x44	Add SEL Entry	Prise en charge
0x0a	0x45	Partial Add SEL Entry	Non prise en charge
0x0a	0x46	Delete SEL Entry	Prise en charge
0x0a	0x47	Clear SEL	Prise en charge
0x0a	0x48	Get SEL Time	Prise en charge

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x0a	0x49	Set SEL Time	Prise en charge
0x0a	0x5C	Get SEL Time UTC Offset	Non prise en charge
0x0a	0x5D	Set SEL Time UTC Offset	Non prise en charge

15.2.6 Commandes de transport

15.2.6.1 Commandes des unités LAN

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x0c	0x01	Set LAN Configuration Parameters	Prise en charge
0x0c	0x02	Get LAN Configuration Parameters	Prise en charge
0x0c	0x03	Suspend BMC ARPs	Non prise en charge

15.2.6.2 Commandes série sur LAN

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x0c	0x22	Get SOL Configuration Parameters	Prise en charge
0x0c	0x21	Set SOL Configuration Parameters	Prise en charge

15.2.7 Commandes Kontron OEM

Net function	Commande	Nom de la commande	Prise en charge / Non prise en charge
0x3C	0x07	UEFI Recovery	Prise en charge

16/ Symboles et acronymes du document

16.1 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 graves.
⚠CAUTION	CAUTION (ATTENTION) indique une situation dangereuse qui, si elle n'est pas évitée, peut entraîner des blessures mineures ou modérées.
NOTICE	NOTICE (AVIS) indique un message de dommages matériels.
	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.

16.2 Acronymes

ACPI	Interface avancée de configuration et de courant électrique
API	Interface de programmation d'applications
ASIC	Circuit intégré spécifique
BC	Horloge frontière
BIOS	Système d'entrée-sortie de base
BMC	Contrôleur de gestion de carte mère
BMCA	Algorithme du meilleur maître d'horloge
BSP	Package de support de carte
Bus I2C	Bus de circuit inter-intégré
Carte VGA	Carte vidéographique
CBIT	Test intégré continu
CC	Courant continu
CE	Communauté européenne (marquage CE)
CEM	Compatibilité électromagnétique
CIR	Carte d'interface réseau ou contrôleur d'interface réseau
CLI	Interface de ligne de commande
CPU	Unité centrale de traitement
CSA	Association canadienne de normalisation
DDR4	Double débit de données 4
DEEE	Déchet d'équipements électrique et électronique
DEL	Diode électroluminescente
DHCP	Protocole de configuration dynamique des hôtes
DIMM	Module de mémoire à double rangée de connexions
Disque SSD	Disque à circuits intégrés
DRAM	Mémoire vive dynamique
DTS	Capteur thermique numérique
DU	Unité distribuée
E/S	Entrée/sortie
ECC	Code de correction d'erreurs
EEPROM	Mémoire morte effaçable et programmable électriquement
EMI	Perturbation électromagnétique
EOL	Fin de vie
ESD	Décharge électrostatique
ESMC	Canal de messages de synchronisation Ethernet
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
FH¾L	Pleine hauteur/¾ longueur
FHHL	Pleine hauteur/demi-longueur
FPGA	Réseau prédiffusé programmable par l'utilisateur
FRU	Unité remplaçable par l'utilisateur
Gb	Gigabit
GbE	Gigabit Ethernet
GM	Horloge maître
Go	Gigaoctet – 1024 Mo
GPI	Entrée à usage général
GPIO	Entrée/sortie à usage général
GPO	Sortie à usage général
GPS	Système de localisation GPS
GPU	Processeur graphique
HTR	Horloge temps réel
Hz	Hertz – 1 cycle/seconde
IA	Intelligence artificielle

iBMC	Contrôleur de gestion de carte mère intégré
IEC	Commission électrotechnique internationale
IEEE	Institute of Electrical and Electronics Engineers
IOL	IPMI sur LAN
IPMB	Bus de gestion de plateforme intelligente
IPMI	Interface de gestion intelligente de matériel
IRQ	Ligne d'interruption
IUG	Interface utilisateur graphique
KCS	Style de contrôleur de clavier
KEAPI	Interface de programmation d'applications emboitée de Kontron
Ko	Kilo-octet – 1024 octets
KVM	Écran-clavier-souris
LAN	Réseau local
LNA	Amplificateur à faible bruit
LP	Profil bas
LPC	Nombre de broches réduit
LVDS	SCSI différentiel à basse tension
MCU	Microcontrôleur
MEC	Informatique en périphérie multi-accès
Mémoire SDRAM	Mémoire vive dynamique synchrone
Mo	Mégaoctet – 1024 Ko
MXM	Module PCI Express mobile
NCSI	Interface de services de communication réseau
NEBS	Système de construction d'équipement réseau
NMI	Interruption non masquable
NOS	Système d'exploitation de réseau
NVMe	Mémoire non volatile express
OCXO	Oscillateur à quartz thermostaté
PBIT	Test intégré à la mise sous tension
PCH	Horloge matérielle physique
PCH	Contrôleur de plateforme
PCI	Interconnexion de composants périphériques
PCIe	Interconnexion de composants périphériques express
PCS	Protection contre la surchauffe
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
PnP	Prêt à l'emploi
POST	Auto-test de démarrage
PPS	Impulsions par seconde
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
SCME	Serveurs de communication montables en étagère
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
SSH	Protocole Secure Shell
SSM	Message d'état de synchronisation
ST	Sous-tension
TAM	Température ambiante maximale
T-BC	Horloge frontière télécom
TDP	Enveloppe thermique
T-GM	Horloge maître télécom
THOL	Liste du matériel et des systèmes d'exploitation testés
ToD	Heure du jour
TPM	Module de plateforme sécurisée
TSC	Horloge esclave de temps
T-TSC	Horloge esclave de temps télécom
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.
UMI	Unité de mesure inertielle
USB	Bus série universel
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)
vRAN	Réseau d'accès radioélectrique virtualisé
W	Watt
Ω	Ohm