



Intégrité

Les rubriques suivantes décrivent comment utiliser la surveillance de l'intégrité dans le système Firepower :

- [Exigences et conditions préalables du contrôle d'intégrité, à la page 1](#)
- [À propos de la surveillance de l'intégrité, à la page 1](#)
- [Politiques d'intégrité, à la page 15](#)
- [Exclusion de périphériques dans la surveillance de l'intégrité, à la page 19](#)
- [Alertes de moniteur d'intégrité, à la page 22](#)
- [À propos de la surveillance de l'intégrité, à la page 24](#)
- [Vues des événements liés à l'intégrité, à la page 38](#)
- [À propos de l'audit du système, à la page 41](#)

Exigences et conditions préalables du contrôle d'intégrité

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

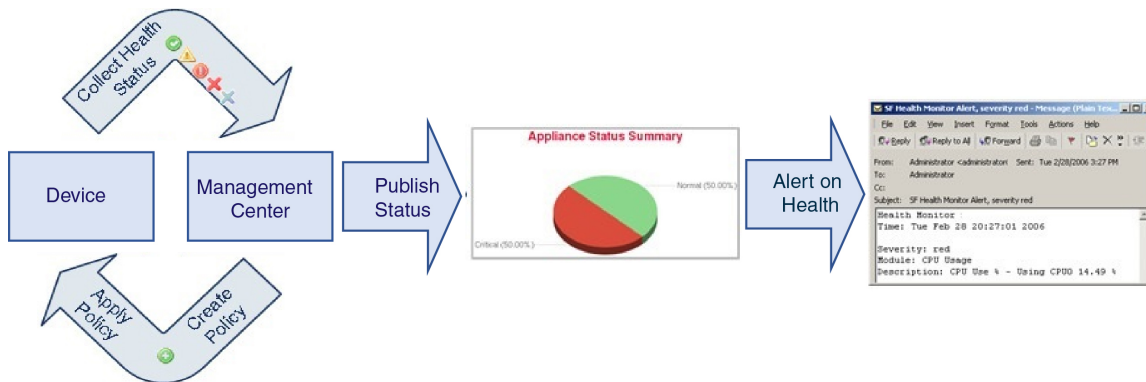
Utilisateur de maintenance

À propos de la surveillance de l'intégrité

Le moniteur d'intégrité du centre de gestion suit divers indicateurs d'intégrité pour s'assurer que le matériel et les logiciels du système fonctionnent correctement. Vous pouvez utiliser le moniteur d'intégrité pour vérifier l'état des fonctionnalités essentielles dans votre déploiement.

Vous pouvez configurer la fréquence d'exécution des modules d'intégrité pour les alertes. Le Centre de gestion prend également en charge la collecte de données de séries chronologiques. Vous pouvez configurer la fréquence de collecte des données de séries chronologiques sur le périphérique et ses modules d'intégrité. Le

moniteur de périphériques signale par défaut ces mesures dans plusieurs tableaux de bord de moniteur d'intégrité prédéfinis. Les données des métriques sont collectées à des fins d'analyse et, par conséquent, aucune alerte ne leur est associée.



Vous pouvez utiliser le moniteur d'intégrité pour créer un ensemble de tests, appelé *politique d'intégrité*, et appliquer la politique d'intégrité à un ou plusieurs périphériques. Les tests, appelés *modules d'intégrité*, sont des scripts qui testent les critères que vous spécifiez. Vous pouvez modifier une politique d'intégrité en activant ou désactivant les tests ou en modifiant les paramètres de test, et vous pouvez supprimer les politiques d'intégrité dont vous n'avez plus besoin. Vous pouvez également supprimer les messages de la sélection de périphériques en les excluant.

Le système de surveillance de l'intégrité exécute les tests dans une politique d'intégrité aux intervalles configurés. Vous pouvez également exécuter tous les tests, ou un test en particulier, à la demande. Le moniteur d'intégrité recueille les événements d'intégrité en fonction des conditions de test configurées.

Les modules d'intégrité sont de deux types : les existants et les télégraphiques.

Le module d'intégrité existant surveille l'état de fonctionnement de certains systèmes, notamment les ventilateurs, les blocs d'alimentation et l'intégrité de la base de données. Lorsque les conditions précisées dans la politique d'intégrité de ces systèmes surveillés sont réunies, les modules d'intégrité basés sur l'infrastructure existants émettent directement des alertes (vert, rouge ou orangé) accompagnées d'un court message.

Le module d'intégrité télégraphique surveille les modules d'extension télégraphiques qui récupèrent les informations métriques du système surveillé. Vous pouvez créer des tableaux de bord personnalisés avec vos mesures d'intégrité préférées pour le module d'intégrité télégraphique, ce qui vous permet de surveiller des statistiques spécifiques ou de résoudre des problèmes spécifiques.



Remarque

Tous les périphériques signalent automatiquement l'état de leur matériel à l'aide du module d'intégrité Hardware Alarms. Le centre de gestion signale également automatiquement l'état à l'aide des modules configurés dans la politique d'intégrité par défaut. Certains modules d'intégrité, comme le module heartbeat du périphérique, s'exécutent sur centre de gestion et signalent l'état des périphériques gérés par centre de gestion. Pour que les modules d'intégrité fournissent l'état des périphériques gérés, vous devez déployer toutes les politiques d'intégrité sur le périphérique.

Vous pouvez utiliser le moniteur d'intégrité pour accéder aux informations sur l'intégrité du système, pour un appareil en particulier ou, dans un déploiement multidomaine, un domaine particulier. Les tableaux hexagonaux et les tableaux d'état de la page Health Monitor fournissent un résumé visuel de l'état de tous les

périphériques de votre réseau, y compris le centre de gestion. Les moniteurs d'intégrité de chaque appareil vous permettent d'explorer les détails de l'intégrité d'un appareil en particulier.

Les affichages des événements entièrement personnalisables vous permettent d'analyser rapidement et facilement les événements d'état d'intégrité recueillis par le moniteur d'intégrité. Ces affichages d'événements vous permettent de rechercher et d'afficher des données d'événements et d'accéder à d'autres informations qui peuvent être liées aux événements sur lesquels vous étudiez. Par exemple, si vous souhaitez voir toutes les occurrences d'utilisation du processeur avec un certain pourcentage, vous pouvez rechercher le module d'utilisation du processeur et saisir la valeur de pourcentage.

Vous pouvez également configurer les alertes par courriel, SNMP ou syslog en réponse à des événements d'intégrité. Une *alerte d'intégrité* est une association entre une alerte standard et un niveau d'état d'intégrité. Par exemple, si vous voulez vous assurer qu'un appareil ne tombe jamais en panne en raison d'une surcharge matérielle, vous pouvez configurer une alerte par courriel. Vous pouvez ensuite créer une alerte d'intégrité qui déclenche une alerte par courriel chaque fois que l'utilisation du processeur, du disque ou de la mémoire atteint le niveau d'avertissement que vous avez configuré dans la politique d'intégrité appliquée à cet appareil. Vous pouvez définir des seuils d'alerte pour minimiser le nombre d'alertes répétées que vous recevez.



Remarque La surveillance de l'intégrité peut prendre de 5 à 6 minutes à partir de l'occurrence de l'événement d'intégrité pour générer l'alerte d'intégrité.

Vous pouvez également générer des fichiers de dépannage pour un appareil si le service d'assistance vous le demande.

Seuls les utilisateurs disposant de privilèges de rôle d'administrateur peuvent accéder aux données sur l'intégrité du système.

Paire de haute disponibilité

Dans un déploiement à haute disponibilité centre de gestion exécutant la version 6.7 ou ultérieure, le centre de gestion actif crée une page de moniteur d'intégrité qui utilise les API REST pour afficher des informations détaillées basées sur les métriques. Le centre de gestion de secours crée la page de moniteur d'intégrité qui affiche les informations d'alerte et fournit un résumé visuel de l'état de tous les périphériques de votre réseau à l'aide de graphiques à secteurs et de tableaux d'état. Le centre de gestion de secours n'affiche pas les informations basées sur les métriques.

Modules d'intégrité

Les modules d'intégrité, ou tests d'intégrité, testent les critères que vous spécifiez dans une politique d'intégrité.

Tableau 1 : Modules d'intégrité (tous les périphériques)

Module	Type de module	Description
Utilisation du CPU (par cœur)	Telegraph	Ce module vérifie que l'utilisation de la CPU sur tous les cœurs n'est pas surchargée et alerte lorsque l'utilisation de la CPU dépasse les seuils configurés pour le module. La valeur par défaut du % de seuil d'avertissement est 80. La valeur par défaut du % de seuil critique est 90.

Module	Type de module	Description
État du disque	Système existant	<p>Ce module examine les performances du disque dur et l'ensemble de stockage contre les programmes malveillants (si installés) sur le périphérique.</p> <p>Ce module génère une alerte d'intégrité d'avertissement (jaune) lorsque le disque dur et le contrôleur RAID (si installé) sont sur le point de tomber en panne ou si un disque dur supplémentaire installé n'est pas un ensemble de stockage malveillant. Ce module génère une alerte d'intégrité Alert (red) lorsqu'un ensemble de stockage de logiciel malveillant installé ne peut pas être détecté.</p>
Utilisation du disque	Telegraph	<p>Ce module compare l'utilisation du disque dur du périphérique et de l'ensemble de stockage contre les programmes malveillants aux limites configurées pour le module et alerte lorsque l'utilisation dépasse les seuils configurés pour le module. Ce module alerte également lorsque le système supprime un nombre excessif de fichiers dans les catégories d'utilisation du disque surveillées ou lorsque l'utilisation du disque à l'exclusion de ces catégories atteint des niveaux excessifs, en fonction des seuils du module.</p> <p>Utilisez le module d'état d'intégrité de l'utilisation du disque pour surveiller l'utilisation du disque pour les partitions de <code>volume/</code> et sur le périphérique et suivre la fréquence de vidage. Bien que le module d'utilisation du disque répertorie la partition <code>/boot</code> comme partition surveillée, la taille de la partition est statique; le module n'émet donc pas d'alerte sur la partition de démarrage.</p> <p>Attention Si vous recevez des alertes pour une utilisation élevée du disque non géré pour la partition ou le <code>volume</code> bien que l'utilisation soit inférieure au seuil critique ou d'avertissement précisé dans la politique d'intégrité, cela peut indiquer que certains fichiers doivent être supprimés manuellement du système. Communiquez avec le Cisco TAC si vous recevez ces alertes.</p>
Vérification de l'intégrité du système de fichier	Système existant	Ce module effectue une vérification de l'intégrité du système de fichiers et s'exécute si le mode CC ou le mode UCAPL est activé, ou si le système exécute une image signée avec une clé DEV. Cette fonction est activée par défaut.
Surveillance de l'intégrité	Système existant	Ce module surveille l'état du moniteur d'intégrité lui-même et alerte si le nombre de minutes depuis le dernier événement d'intégrité reçu par le centre de gestion dépasse les limites d'avertissement ou critique.

Module	Type de module	Description
État d'interface	Système existant	<p>Ce module détermine si le périphérique collecte actuellement du trafic et envoie des alertes en fonction de l'état du trafic des interfaces physiques et des interfaces agrégées. Pour les interfaces physiques, les informations comprennent le nom de l'interface, l'état de la liaison et la bande passante. Pour les interfaces agrégées, les informations comprennent le nom de l'interface, le nombre de liens actifs et la bande passante agrégée totale.</p> <p>Remarque Ce module surveille également le flux de trafic du périphérique en veille à haute disponibilité. Bien que l'on sache que le périphérique en veille ne recevra aucun trafic pour le moment, centre de gestion indique que l'interface ne reçoit aucun trafic. Le même principe d'alerte est appliqué lorsque le trafic n'est pas reçu par certaines des sous-interfaces sur un canal de port.</p> <p>Si vous utilisez la commande de CLI show interface pour connaître les statistiques d'interface de votre appareil, les débits d'entrée et de sortie dans le résultat de la commande de CLI peuvent être différents des débits de trafic qui apparaissent dans le module d'interface.</p> <p>Ce module affiche les débits de trafic en fonction des valeurs de la surveillance des performances Snort. Les intervalles d'échantillonnage de la surveillance des performances Snort et des statistiques de l'interface centre de gestion sont différents. En raison de la différence d'intervalle d'échantillonnage, les valeurs de débit de l'interface graphique centre de gestion peuvent être différentes des valeurs de débit affichées dans le résultat de l'interface de ligne de commande défense contre les menaces .</p>
Analyse locale des programmes malveillants	Système existant	<p>Ce module surveille les mises à jour de ClamAV pour l'analyse locale des programmes malveillants.</p>
Utilisation de la mémoire	Système existant	<p>Ce module compare l'utilisation de la mémoire du périphérique aux limites configurées pour le module et alerte lorsque l'utilisation dépasse les niveaux configurés pour le module.</p> <p>Pour les périphériques dotés de plus de 4 Go de mémoire, les seuils d'alerte prédéfinis sont basés sur une formule qui prend en compte les proportions de mémoire disponible susceptibles de provoquer des problèmes au système. Sur les périphériques supérieurs à 4 Go, parce que l'intervalle entre les seuils d'avertissement et critique peut être très étroit, il est recommandé de définir manuellement le % de seuil d'avertissement sur 50. Ainsi, vous serez certain de recevoir à temps des alertes de mémoire pour votre appareil afin de résoudre le problème.</p> <p>À partir de la version 6.6.0, la RAM minimale requise pour les mises à niveau de centre de gestion virtuel vers la version 6.6.0+ est de 28 Go et la RAM recommandée pour les déploiements de centre de gestion virtuel est de 32 Go. Nous vous recommandons de ne pas diminuer les paramètres par défaut : 32 Go de RAM pour la plupart des instances centre de gestion virtuel , 64 Go pour centre de gestion virtuel 300 (VMware uniquement).</p> <p>Attention Une alerte critique est générée par le moniteur d'intégrité lorsqu'une RAM insuffisante est allouée à un déploiement centre de gestion virtuel .</p> <p>Des politiques et règles de contrôle d'accès complexes peuvent exiger des ressources importantes et nuire aux performances.</p>

Module	Type de module	Description
État du traitement	Système existant	<p>Ce module détermine si les processus de l'appliance quittent ou se terminent en dehors du gestionnaire de processus.</p> <p>Si un processus est délibérément abandonné en dehors du gestionnaire de processus, l'état du module passe à Avertissement et le message d'événement d'intégrité indique quel processus a été abandonné, jusqu'à ce que le module s'exécute à nouveau et que le processus ait redémarré. Si un processus se termine de manière anormale ou se bloque en dehors du gestionnaire de processus, l'état du module passe à Critique et le message d'événement d'intégrité indique que le processus a été arrêté, jusqu'à ce que le module fonctionne à nouveau et que le processus ait redémarré.</p>

Module	Type de module	Description
Mises à jour des périphériques à propos des données sur les menaces	Système existant	<p>Certaines données et certaines configurations utilisées par les périphériques pour détecter les menaces sont mises à jour sur le centre de gestion à partir du nuage toutes les 30 minutes.</p> <p>Ce module vous alerte si ces informations n'ont pas été mises à jour sur les périphériques dans la période que vous avez spécifiée.</p> <p>Les mises à jour surveillées comprennent :</p> <ul style="list-style-type: none"> • Données de catégorie d'URL et de réputation locales • les listes et les flux d'URL de renseignements sur la sécurité, y compris les listes de blocage globales, et Ne pas bloquer et les URL Threat Intelligence Director • Listes et flux de réseau Security Intelligence (adresses IP), y compris les listes de blocage globales et Ne pas bloquer, ainsi que les adresses IP du directeur des vigies des menaces (Threat Intelligence Director) • Listes et flux DNS de renseignements sur la sécurité, y compris les listes de blocage et Ne pas bloquer globales et les domaines de Threat Intelligence Director • Signatures pour les analyses locales de programmes malveillants (de ClamAV) • Listes SHA de Threat Intelligence Director, comme répertoriées sur la page Objects > Gestion des objets > Security Intelligence > Listes et flux de réseaux • Les paramètres d'analyse dynamique configurés sur la page Integration > AMP > Dynamic Analysis Connections (connexions à l'analyse dynamique) • les paramètres de configuration des menaces liés à l'expiration des URL en cache, y compris le paramètre d'expiration des URL en cache dans la page Integration (intégration) > Other Integrations (autres intégrations) > Cloud Services (cisco Cloud Services). (Les mises à jour du cache d'URL ne sont pas surveillées par ce module.) • Problèmes de communication avec le nuage Cisco pour l'envoi des événements. Voir l'encadré Cisco Cloud sur la page Integration > Autres intégrations > Services en nuage. <p>Remarque Les mises à jour de Threat Intelligence Director ne sont incluses que si TID est configuré sur votre système et que vous avez des flux.</p> <p>Par défaut, ce module envoie un avertissement après 1 heure et une alerte critique après 24 heures.</p> <p>Si ce module indique une défaillance sur le centre de gestion ou sur tout périphérique, vérifiez que le centre de gestion peut atteindre les périphériques.</p>

Tableau 2 : Modules d'intégrité Centre de gestion

Module	Type de module	Description
État de AMP for Endpoints	Système existant	Le module envoie une alerte si centre de gestion ne peut pas se connecter au nuage AMP ou au nuage privé Cisco AMP après une connexion initiale réussie, ou si le nuage privé ne peut pas contacter le nuage AMP public. Il vous avertit également si vous annulez l'enregistrement d'une connexion au nuage AMP à l'aide de la console de gestion Cisco Secure Endpoint.
AMP pour l'état de FirePower	Système existant	<p>Ce module alerte si :</p> <ul style="list-style-type: none"> • centre de gestion ne peut pas contacter le nuage (public ou privé) AMP ou le nuage Cisco Secure Malware Analytics ou le périphérique, ou le nuage privé AMP ne peut pas contacter le nuage AMP public. • Les clés de chiffrement utilisées pour la connexion ne sont pas valides. • Un périphérique ne peut pas contacter le nuage Cisco Secure Malware Analytics ou le périphérique Cisco Secure Malware Analytics pour soumettre des fichiers pour une analyse dynamique. • Un nombre excessif de fichiers est détecté dans le trafic réseau en fonction de la configuration de la politique de fichiers. <p>Si votre centre de gestion perd la connectivité à Internet, le système peut prendre jusqu'à 30 minutes pour générer une alerte d'intégrité.</p>
Pulsation de l'appareil	Système existant	Ce module détermine si une pulsation du périphérique est émise par le périphérique et alerte en fonction de son état.
Taille de la base de données	Système existant	Ce module vérifie la taille de la base de données de configuration et alerte lorsque celle-ci dépasse les valeurs (en gigaoctets) configurées pour le module.
Limite de découverte des hôtes	Système existant	Ce module détermine si le nombre d'hôtes que centre de gestion peut surveiller approche de la limite et alerte en fonction du niveau d'avertissement configuré pour le module. Pour en savoir plus, consultez Limite d'hôte du système Firepower .
État du carnet de commandes de l'événement	Système existant	<p>Ce module alerte si l'arriéré des données d'événements en attente de transmission du périphérique au centre de gestion a augmenté de façon continue pendant plus de 30 minutes.</p> <p>Pour réduire l'arriéré, évaluez votre bande passante et envisagez de consigner moins d'événements.</p>
Moniteur d'événements	Telegraph	Ce module surveille le taux global d'événements entrants pour centre de gestion.
État de la diffusion d'événement	Système existant	Ce module surveille les connexions aux applications clientes tierces qui utilisent Event Streamer sur centre de gestion.
Statistiques du matériel	Telegraph	Ce module surveille l'état des entités matérielles centre de gestion, à savoir la vitesse du ventilateur, la température et l'alimentation. Ce module alerte lorsque la valeur du seuil dépasse les limites d'avertissement ou de critique configurées.

Module	Type de module	Description
Moniteur de connexion ISE	Système existant	Ce module surveille l'état des connexions de serveur entre Cisco Identity Services Engine (ISE) et centre de gestion. Cisco ISE fournit des données utilisateur supplémentaires, des données de type d'appareil, des données d'emplacement de périphérique, des services SGT (Security Group Tags) et SXP (Security Exchange Protocol).
Surveillance de licence	Système existant	Ce module surveille l'expiration des licences
État de haute disponibilité de Centre de gestion	Système existant	Ce module surveille l'état de haute disponibilité de centre de gestion, et envoie des alertes. centre de gestion Si vous n'avez pas établi la haute disponibilité, l'état de la haute disponibilité est <code>Not in HA</code> (Non en haute disponibilité). Remarque Ce module remplace le module d'état de haute disponibilité, qui indiquait auparavant l'état de haute disponibilité pour centre de gestion. Dans la version 7.0, nous avons ajouté l'état de haute disponibilité pour les périphériques gérés.
Statistiques MySQL	Telegraph	Ce module surveille l'état de la base de données MySQL, y compris la taille de cette dernière, le nombre de connexions actives et l'utilisation de la mémoire. L'option est désactivée par défaut.
État de RabbitMQ	Telegraph	Ce module recueille diverses statistiques pour RabbitMQ.
Processus du serveur RRD	Système existant	Ce module détermine si le serveur de données tourniquet qui stocke les données de séries chronologiques fonctionne correctement. Le module alerte si le serveur RRD a redémarré depuis la dernière mise à jour; il passe à l'état critique ou d'avertissement si le nombre de mises à jour consécutives avec un redémarrage du serveur RRD atteint les valeurs spécifiées dans la configuration du module.
Domaine	Système existant	Vous permet de définir un seuil d'avertissement pour les incompatibilités de domaine ou d'utilisateur, qui sont : <ul style="list-style-type: none"> • Incompatibilité de l'utilisateur : un utilisateur est signalé à centre de gestion sans être téléchargé. <p>Une raison typique d'une incompatibilité d'utilisateur est que l'utilisateur appartient à un groupe que vous avez exclu du téléchargement sur centre de gestion. Passez en revue les renseignements décrits dans la section Guide de configuration Cisco Secure Firewall Management Center Device.</p> <ul style="list-style-type: none"> • Incompatibilité de domaine : un utilisateur se connecte à un domaine qui correspond à un domaine inconnu de centre de gestion. <p>Guide de configuration Cisco Secure Firewall Management Center Device</p> <p>Ce module affiche également des alertes d'intégrité lorsque vous essayez de télécharger plus d'utilisateurs que le nombre maximal d'utilisateurs téléchargés pris en charge par domaine. Le nombre maximal d'utilisateurs téléchargés pour un seul domaine dépend du modèle de centre de gestion.</p> <p>Pour en savoir plus, voir <i>User Limit</i> dans la Guide de configuration Cisco Secure Firewall Management Center Device</p>

Module	Type de module	Description
Renseignements de sécurité	Système existant	Ce module alerte si Security Intelligence est en cours d'utilisation et centre de gestion ne peut pas mettre à jour un flux, ou les données de flux sont endommagées ou ne contiennent pas d'adresses IP reconnaissables. Consultez également le module Mises à jour des données de menaces sur les périphériques.
Moniteur de licence Smart	Système existant	Ce module surveille l'état des licences Smart et envoie des alertes dans les cas suivants : <ul style="list-style-type: none"> • Il y a une erreur de communication entre l'agent de licences Smart (Smart Agent) et le gestionnaire de logiciels Smart. • Le jeton d'enregistrement de l'instance de produit a expiré. • L'utilisation de la licence Smart n'est pas conforme. • L'autorisation ou le mode d'évaluation de la licence Smart a expiré.
Statistiques Sybase	Telegraph	Ce module surveille l'état de la base de données Sybase sur le centre de gestion, y compris la taille de la base de données, le nombre de connexions actives et l'utilisation de la mémoire.
Moniteur de données de séries chronologiques (RRD)	Système existant	Ce module suit la présence de fichiers corrompus dans le répertoire où les données de séries chronologiques (telles que le nombre d'événements de corrélation) sont stockées et alerte lorsque les fichiers sont marqués comme corrompus et supprimés.
État de la synchronisation du temps	Système existant	Ce module suit la synchronisation de l'horloge du périphérique qui obtient l'heure à l'aide du protocole NTP avec l'horloge du serveur NTP et envoie des alertes si la différence entre les horloges est de plus de dix secondes.
Moniteur de groupes non résolus	Système existant	Surveille les groupes non résolus utilisés dans les politiques
Moniteur de filtrage URL	Système existant	Ce module alerte si le centre de gestion ne parvient pas à : <ul style="list-style-type: none"> • S'enregistrer auprès du nuage Cisco Cloud. • Télécharger les mises à jour des données sur les menaces d'URL à partir du nuage Cisco. • Terminer les recherches d'URL. <p>Vous pouvez configurer des seuils temporels pour ces alertes.</p> <p>Consultez également le module Mises à jour des données de menaces sur les périphériques.</p>
État du RPV	Système existant	Ce module alerte lorsqu'un ou plusieurs tunnels VPN entre périphériques défense contre les menaces sont en panne. Ce module suit les : <ul style="list-style-type: none"> • VPN de site à site pour Cisco Secure Firewall Threat Defense • VPN d'accès à distance pour Cisco Secure Firewall Threat Defense

Tableau 3 : Modules d'intégrité de périphérique

Module	Type de module	Description
État de la connexion AMP	Telegraph	Le module envoie une alerte si défense contre les menaces ne peut pas se connecter au nuage AMP ou au nuage privé Cisco AMP après une connexion initiale réussie, ou si le nuage privé ne peut pas contacter le nuage AMP public. L'option est désactivée par défaut.
Connexion d'AMP Threat Grid	Telegraph	Le module envoie une alerte si le défense contre les menaces ne peut pas se connecter au nuage AMP Threat Grid après une connexion initiale réussie.
Supprimer l'ASP	Telegraph	Ce module surveille les connexions abandonnées par le chemin de sécurité accéléré du plan de données.
Contournement automatique de l'application	Système existant	Ce module surveille les applications de détection du contournement des surveillances
État de l'environnement du châssis	Système existant	Ce module surveille les paramètres du châssis tels que la vitesse et la température du ventilateur et vous permet de définir un seuil d'avertissement et un seuil critique de température. La valeur par défaut de la température critique du châssis (Celsius) est 85 °C. La valeur par défaut de l' avertissement de température du châssis (Celsius) est de 75 °C.
État de l'échec de la grappe ou de la haute disponibilité	Système existant	Ce module surveille l'état des grappes de périphériques. Le module alerte si : <ul style="list-style-type: none"> • Une nouvelle unité principale est choisie dans une grappe. • Une nouvelle unité secondaire rejoint une grappe. • Une unité principale ou secondaire quitte une grappe.
Utilisation des ressources de configuration	Système existant	Ce module vous avertit si la taille des configurations déployées risque de faire manquer de mémoire à un périphérique. L'alerte vous indique la quantité de mémoire requise par vos configurations et son dépassement de la mémoire disponible. Si cela se produit, réévaluez vos configurations. La plupart du temps, vous pouvez réduire le nombre ou la complexité des règles de contrôle d'accès ou des stratégies de prévention des intrusions. Attribution de mémoire Snort <ul style="list-style-type: none"> • <i>La mémoire totale</i> Snort indique la mémoire allouée aux instances de Snort 2 exécutées sur le périphérique défense contre les menaces . • <i>La mémoire disponible</i> indique la mémoire allouée par le système pour une instance Snort 2. Notez que cette valeur ne représente pas seulement la différence entre la <i>mémoire totale</i> Snort et la mémoire combinée réservée aux autres modules. Cette valeur est obtenue après quelques autres calculs, puis divisée par le nombre de processus Snort 2. <p>Une valeur de <i>mémoire disponible</i> négative indique que l'instance Snort 2 n'a pas assez de mémoire pour la configuration déployée. Pour obtenir de l'aide, communiquez avec le centre d'assistance technique de Cisco (TAC).</p>

Module	Type de module	Description
Statistiques de connexion	Telegraph	Ce module surveille les statistiques de connexion et le nombre de traductions NAT.
Utilisation du CPU de plan de données	Telegraph	Ce module vérifie que l'utilisation moyenne de la CPU de tous les processus du plan de données sur le périphérique n'est pas surchargée et alerte lorsque l'utilisation de la CPU dépasse les pourcentages configurés pour le module. La valeur par défaut du % de seuil d'avertissement est 80. La valeur par défaut du % de seuil critique est 90.
Utilisation du CPU Snort	Telegraph	Ce module vérifie que l'utilisation moyenne de la CPU des processus Snort sur le périphérique n'est pas surchargée et alerte lorsque l'utilisation de la CPU dépasse les pourcentages configurés pour le module. La valeur par défaut du % de seuil d'avertissement est 80. La valeur par défaut du % de seuil critique est 90.
Utilisation du CPU du système	Telegraph	Ce module vérifie que l'utilisation moyenne de la CPU de tous les processus système sur le périphérique n'est pas surchargée et alerte lorsque l'utilisation de la CPU dépasse les pourcentages configurés pour le module. La valeur par défaut du % de seuil d'avertissement est 80. La valeur par défaut du % de seuil critique est 90.
Statistiques des processus critiques	Telegraph	Ce module surveille l'état des processus critiques, leur utilisation des ressources et le nombre de redémarrages
Statistiques de la configuration déployée	Telegraph	Ce module surveille les statistiques relatives à la configuration déployée, telles que le nombre d'ACE et de règles IPS.
Défaillances de la plateforme Firewall Threat Defense	Système existant	<p>Ce module génère une alerte pour les défaillances de plateforme pour les périphériques Firepower 1000, 2100 et Secure Firewall 3100. Une défaillance est un objet modifiable géré par centre de gestion. Chaque anomalie représente une défaillance de l'instance de défense contre les menaces ou un seuil d'alarme qui a été élevé. Au cours du cycle de vie d'une défaillance, elle peut passer d'un état ou d'un niveau de gravité à un autre.</p> <p>Chaque défaillance comprend des renseignements sur l'état opérationnel de l'objet touché au moment où l'anomalie est survenue. Si la défaillance est transitoire et qu'elle est résolue, l'objet passe à un état fonctionnel.</p> <p>Pour en savoir plus, consultez le <i>Guide des défaillances et des messages d'erreur de Cisco Firepower 1000/2100 FXOS</i>.</p>
Changements apportés à la configuration d'accès Centre de gestion	Système existant	Ce module surveille les modifications de configuration d'accès du centre de gestion effectuées directement sur le périphérique avec la commande configure network management-data-interface .
Statistiques de déchargement de flux	Telegraph	Ce module surveille les statistiques de déchargement de flux matériel pour un périphérique géré.
Alarmes du matériel	Système existant	Ce module détermine si le matériel doit être remplacé sur un périphérique physique géré et émet des alertes en fonction de l'état du matériel. Le module fournit également des rapports sur l'état des daemons matériels.
Alarmes de différence de liaison en ligne	Système existant	Ce module surveille les ports associés aux ensembles en ligne et envoie des alertes si les deux interfaces d'une paire en ligne négocient des vitesses différentes.

Module	Type de module	Description
Taux d'événements d'intrusion et de fichier	Système existant	<p>Ce module compare le nombre d'incidents d'intrusion par seconde aux limites configurées pour ce module et envoie des alertes si les limites sont dépassées. Si le Taux d'incidents d'intrusions et d'événements de fichier est égal à zéro, le processus de prévention des intrusions peut être en panne ou le périphérique géré peut ne pas envoyer d'événements. Sélectionnez Analysis (analyse) > Intrusions > Events pour vérifier si les événements sont reçus du périphérique.</p> <p>En règle générale, le taux d'événements d'un segment de réseau est en moyenne de 20 événements par seconde. Pour un segment de réseau ayant ce débit moyen, le nombre d'événements par seconde (critiques) doit être défini à 50 et le nombre d'événements par seconde (avertissement) doit être défini à 30. Pour déterminer les limites de votre système, trouvez la valeur Événements/sec sur la page des statistiques pour votre périphérique (System (⚙️) > Monitoring (surveillance) > Statistics (statistiques)), puis calculez les limites à l'aide des formules suivantes :</p> <ul style="list-style-type: none"> Événements par seconde (critique) = Événements/Sec * 2,5 Événements par seconde (avertissement) = Événements/Sec * 1.5 <p>Le nombre maximal d'événements que vous pouvez définir pour l'une ou l'autre des limites est de 999, et la limite critique doit être supérieure à la limite d'avertissement.</p>
Propagation de l'état de liaison	Système existant	<p>ISA 3000 uniquement.</p> <p>Ce module détermine quand un lien dans un ensemble en ligne jumelé échoue et déclenche le mode de propagation de l'état du lien. Si un état de liaison se propage à la paire, la classification d'état pour ce module devient Critical (critique), et l'état indique :</p> <p>Module Link State Propagation: ethx_ethy is Triggered</p> <p>où x et y sont les numéros d'interface jumelée.</p>
Utilisation de la mémoire par le plan de données	Telegraph	Ce module vérifie le pourcentage de mémoire allouée utilisée par les processus du plan de données et alerte lorsque l'utilisation de la mémoire dépasse les pourcentages configurés pour le module. La valeur par défaut du % de seuil d'avertissement est 80. La valeur par défaut du % de seuil critique est 90.
Utilisation de la mémoire par Snort	Telegraph	Ce module vérifie le pourcentage de mémoire allouée utilisée par le processus Snort et alerte lorsque l'utilisation de la mémoire dépasse les pourcentages configurés pour le module. La valeur par défaut du % de seuil d'avertissement est 80. La valeur par défaut du % de seuil critique est 90.
Réinitialisation de la carte réseau	Système existant	Ce module vérifie les cartes réseau qui ont redémarré en raison d'une défaillance matérielle et alerte lorsqu'une réinitialisation se produit.
Statistiques du NTP	Telegraph	Ce module surveille l'état de la synchronisation de l'horloge NTP du périphérique géré. L'option est désactivée par défaut.
Bloc d'alimentation	Système existant	Ce module détermine si les blocs d'alimentation du périphérique doivent être remplacés et alerte en fonction de l'état du bloc d'alimentation.
Statistiques de routage	Telegraph	Ce module surveille l'état actuel de la table de routage.

Module	Type de module	Description
Statistiques de Snort 3	Telegraph	Ce module recueille et surveille les statistiques de Snort 3 pour les événements, les flux et les paquets.
Utilisation de la mémoire par Snort Identity	Système existant	Vous permet de définir un seuil d'avertissement pour le traitement de l'identité Snort et d'alertes lorsque l'utilisation de la mémoire dépasse le niveau configuré pour le module. La valeur par défaut du % de seuil critique est 80. Ce module d'intégrité effectue le suivi de l'espace total utilisé pour les informations d'identité de l'utilisateur dans Snort. Il affiche les détails de l'utilisation actuelle de la mémoire, le nombre total de liaisons utilisateur-IP et les détails de mappage de groupes d'utilisateurs. Snort enregistre ces détails dans un fichier. Si le fichier d'utilisation de la mémoire n'est pas disponible, l'alerte d'intégrité pour ce module affiche <i>En attente de données</i> . Cela peut se produire lors du redémarrage de Snort en raison d'une nouvelle installation ou d'une mise à jour majeure, du passage de Snort 2 à Snort 3 ou d'une sauvegarde précédente, ou du déploiement d'une politique majeure. Selon le cycle de surveillance de l'intégrité et lorsque le fichier est disponible, l'avertissement disparaît et le moniteur de l'intégrité affiche les détails de ce module, qui devient vert.
Détection de reconfiguration de Snort	Telegraph	Ce module alerte en cas d'échec de la reconfiguration d'un périphérique. Ce module détecte les échecs de reconfiguration pour les instances Snort 2 et Snort 3.
Statistiques Snort	Telegraph	Ce module surveille les statistiques de Snort 3 pour les événements, les flux et les paquets.
État de la connexion aux services de sécurité Exchange	Telegraph	Le module alerte si défense contre les menaces ne peut pas se connecter au nuage d'échange des services de sécurité après une connexion initiale réussie. L'option est désactivée par défaut.
Haute disponibilité du Défense contre les menaces (vérification de l'état split-brain)	Système existant	Ce module surveille l'état de haute disponibilité de défense contre les menaces et envoie des alertes et fournit une alerte d'intégrité en cas de scission. défense contre les menaces Si vous n'avez pas établi la haute disponibilité, l'état de la haute disponibilité est <code>Not in HA</code> (Non en haute disponibilité).
Statistiques du VPN	Telegraph	Ce module surveille les tunnels de site à site et de VPN d'accès à distance entre les périphériques défense contre les menaces .
Compteurs XTLS	Telegraph	Ce module surveille les flux des protocoles XTLS /SSL, l'efficacité de la mémoire et du cache L'option est désactivée par défaut.

Configuration de la surveillance de l'intégrité

Procédure

Étape 1

Déterminez quels modules d'intégrité vous souhaitez surveiller, comme indiqué dans [Modules d'intégrité, à la page 3](#).

Vous pouvez configurer des politiques spécifiques pour chaque type d'appareil que vous avez dans votre système Firepower, en activant uniquement les tests appropriés pour cet appareil.

Astuces Pour activer rapidement la surveillance de l'intégrité sans personnaliser le comportement de surveillance, vous pouvez appliquer la politique par défaut fournie à cette fin.

Étape 2 Appliquez une politique d'intégrité à chaque appareil dont vous souhaitez suivre l'état d'intégrité, comme indiqué dans [Création de politiques d'intégrité, à la page 16](#).

Étape 3 (Facultatif) Configurez les alertes du moniteur d'intégrité comme indiqué dans [Création des alertes de moniteur d'intégrité, à la page 23](#).

Vous pouvez configurer des alertes par courriel, par journal système ou par SNMP qui se déclenchent lorsque le niveau d'état d'intégrité atteint un niveau de gravité particulier pour des modules d'intégrité spécifiques.

Politiques d'intégrité

Une politique d'intégrité contient des critères de test d'intégrité configurés pour plusieurs modules. Vous pouvez contrôler les modules d'intégrité qui s'exécutent sur chacun de vos périphériques et configurer les limites spécifiques utilisées dans les tests exécutés par chaque module.

Lorsque vous configurez une politique d'intégrité, vous décidez si vous souhaitez activer chaque module d'intégrité pour cette politique. Vous pouvez également sélectionner les critères qui contrôlent l'état d'intégrité de chaque module activé chaque fois qu'il évalue l'intégrité d'un processus.

Vous pouvez créer une politique d'intégrité qui peut être appliquée à chaque appareil de votre système, personnaliser chaque politique d'intégrité en fonction du périphérique sur lequel vous prévoyez de l'appliquer ou utiliser la politique d'intégrité par défaut fournie pour vous. Dans un déploiement multidomaine, les administrateurs des domaines ascendants peuvent appliquer des politiques d'intégrité aux périphériques des domaines descendants, que les domaines descendants peuvent utiliser ou remplacer par des politiques locales personnalisées.

Politique d'intégrité par défaut

Le processus de configuration centre de gestion crée et applique une politique d'intégrité initiale, dans laquelle la plupart des modules d'intégrité disponibles, mais pas tous, sont activés. Le système applique également cette politique initiale aux périphériques ajoutés à centre de gestion.

Cette politique d'intégrité *initiale* est basée sur une politique d'intégrité *par défaut*, que vous ne pouvez ni afficher ni modifier, mais que vous pouvez copier lorsque vous créez une politique d'intégrité personnalisée.

Les mises à niveau et la politique d'intégrité par défaut

Lorsque vous mettez à niveau centre de gestion, tout nouveau module d'intégrité est ajouté à toutes les politiques d'intégrité, y compris la politique d'intégrité initiale, la politique d'intégrité par défaut et toutes les autres politiques d'intégrité personnalisées. Généralement, les nouveaux modules d'intégrité sont ajoutés s'ils sont activés.



Remarque Pour qu'un nouveau module d'intégrité commence à surveiller et à envoyer des alertes, appliquez de nouveau les politiques d'intégrité après la mise à niveau.

Création de politiques d'intégrité

Si vous souhaitez personnaliser une politique d'intégrité à utiliser avec vos périphériques, vous pouvez créer une nouvelle politique. Les paramètres de la politique sont remplis initialement avec les paramètres de la politique d'intégrité que vous choisissez comme base pour la nouvelle politique. Vous pouvez modifier la politique afin de préciser vos préférences, par exemple activer ou désactiver des modules de la politique, modifier les critères d'alerte pour chaque module au besoin et préciser les intervalles d'exécution.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine. Les administrateurs des domaines ascendants peuvent appliquer des politiques d'intégrité aux périphériques des domaines descendants, que les domaines descendants peuvent utiliser ou remplacer par des politiques locales personnalisées.

Procédure

- Étape 1** Choisissez **System** (⚙) > **Politique** > **d'intégrité**.
 - Étape 2** Cliquez sur **Créer une politique**.
 - Étape 3** Entrez un nom pour la politique.
 - Étape 4** Choisissez la politique existante que vous souhaitez utiliser comme base pour la nouvelle politique dans la liste déroulante **Base Policy** (politique de base).
 - Étape 5** Saisissez une description pour la politique.
 - Étape 6** Choisissez **Save** (Enregistrer).
-

Prochaine étape

- Appliquer la politique d'intégrité sur les périphériques comme décrit dans [Application des politiques d'intégrité](#), à la page 16.
- Modifiez la politique pour spécifier les paramètres de politique au niveau du module, comme décrit dans [Modification des politiques d'intégrité](#), à la page 17.

Application des politiques d'intégrité

Lorsque vous appliquez une politique d'intégrité à un appareil, les tests d'intégrité de tous les modules que vous avez activés dans la politique surveillent automatiquement l'intégrité des processus et du matériel sur cet appareil. Les tests d'intégrité continuent ensuite de s'exécuter aux intervalles que vous avez configurés dans la politique, pour collecter des données d'intégrité pour le périphérique et les transmettre à centre de gestion.

Si vous activez un module dans une politique d'intégrité, puis appliquez la politique à un appareil qui ne nécessite pas ce test d'intégrité, le moniteur d'intégrité signale l'état de ce module d'intégrité comme désactivé.

Si vous appliquez une politique avec tous les modules désactivés à un appareil, toutes les politiques d'intégrité appliquées à l'appareil sont supprimées du périphérique, de sorte qu'aucune politique d'intégrité n'est appliquée.

Lorsque vous appliquez une politique différente à un appareil auquel une politique est déjà appliquée, attendez-vous à une certaine latence dans l'affichage des nouvelles données en fonction des tests nouvellement appliqués.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine. Les administrateurs des domaines ascendants peuvent appliquer des politiques d'intégrité aux périphériques des domaines descendants, que les domaines descendants peuvent utiliser ou remplacer par des politiques locales personnalisées.

Procédure

- Étape 1** Choisissez **System** (⚙️) > **Politique** > **d'intégrité**.
- Étape 2** Cliquez sur **Déployer la politique d'intégrité** (📄) à côté de la politique que vous souhaitez appliquer.
- Étape 3** Choisissez les périphériques auxquels vous souhaitez appliquer la politique d'intégrité.
- Remarque** Vous ne pouvez pas supprimer la politique d'un appareil après l'avoir déployé. Pour arrêter la surveillance de l'intégrité pour un appareil, créez une politique d'intégrité avec tous les modules désactivés et appliquez-la au périphérique.
- Étape 4** Cliquez sur **Apply** (appliquer) pour appliquer la politique aux périphériques que vous avez choisis.
-

Prochaine étape



- Vous pouvez également surveiller l'état de la tâche; voir [Affichage des messages en lien avec les tâches](#).
La surveillance du périphérique commence dès que la politique est appliquée avec succès.

Modification des politiques d'intégrité

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine. Les administrateurs des domaines ascendants peuvent appliquer des politiques d'intégrité aux périphériques des domaines descendants, que les domaines descendants peuvent utiliser ou remplacer par des politiques locales personnalisées.

Procédure

- Étape 1** Choisissez **System** (⚙️) > **Politique** > **d'intégrité**.
- Étape 2** Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.
- Étape 3** Pour modifier le nom de la politique et sa description, cliquez sur l'icône **Edit** (✎) à côté du nom de la politique.

Étape 4 L'onglet **Health Modules** (modules d'intégrité) affiche tous les modules de périphérique et ses attributs. Cliquez sur le bouton à bascule qui est fourni à côté du module et de ses attributs : activez () ou désactivez () pour activer ou désactiver les tests de l'état d'intégrité, respectivement. Pour exécuter des tests d'activation ou de désactivation en bloc sur les modules d'intégrité, cliquez sur le bouton bascule **Tout sélectionner**. Pour obtenir de l'information sur les modules, consultez [Modules d'intégrité, à la page 3](#).

- Remarque**
- Les modules et les attributs sont marqués avec les périphériques de prise en charge de défense contre les menaces : , centre de gestion ou les deux.
 - Vous ne pouvez pas choisir d'inclure ou d'exclure les attributs individuels du processeur et des modules de mémoire.

Étape 5 Le cas échéant, définissez les pourcentages des seuils **critiques** et **d'avertissement** .

Étape 6 Dans l'onglet **Run Time Intervals** (paramètres des intervalles d'exécution), saisissez les valeurs pertinentes dans les champs :

- **Health Module Run Interval** : fréquence d'exécution des modules d'intégrité. L'intervalle minimal est de 5 minutes.
- **Intervalle de collecte des métriques** : la fréquence de collecte des données de séries chronologiques sur le périphérique et ses modules d'intégrité. Le moniteur de périphériques signale par défaut ces mesures dans plusieurs tableaux de bord de moniteur d'intégrité prédéfinis. Pour de plus amples renseignements, sur le tableau de bord, voir [À propos des tableaux de bord](#). Les données des métriques sont collectées à des fins d'analyse et, par conséquent, aucune alerte ne leur est associée.

Étape 7 Cliquez sur **Save** (enregistrer).

Étape 8 Appliquez la politique d'intégrité à votre appareil comme décrit dans [Application des politiques d'intégrité, à la page 16](#).

Appliquez la politique d'intégrité à chaque appareil dont vous souhaitez suivre l'état d'intégrité. Lorsque vous appliquez la politique d'intégrité à un appareil, tous les modules que vous avez activés dans la politique surveillent l'intégrité des processus et du matériel sur le périphérique et transmettent ces données à centre de gestion.

Suppression des politiques d'intégrité

Vous pouvez supprimer les politiques d'intégrité dont vous n'avez plus besoin. Si vous supprimez une politique qui est toujours appliquée à un appareil, les paramètres de la politique restent en vigueur jusqu'à ce que vous appliquiez une autre politique. En outre, si vous supprimez une politique d'intégrité qui est appliquée à un périphérique, toutes les alertes de surveillance de l'intégrité en vigueur pour le périphérique restent actives jusqu'à ce que vous désactiviez la réponse à l'alerte sous-jacente associée.

Dans un déploiement multidomaine, vous pouvez afficher et modifier les alertes du moniteur d'intégrité créées dans le domaine actuel uniquement.



Astuces Pour arrêter la surveillance de l'intégrité pour un appareil, créez une politique d'intégrité avec tous les modules désactivés et appliquez-la au périphérique.

Procédure

- Étape 1** Choisissez **System** (⚙️) > **Politique** > **d'intégrité**.
- Étape 2** Cliquez sur **Supprimer** (🗑️) à côté de la politique que vous souhaitez supprimer, puis cliquez sur **Delete health politique** (supprimer la politique d'intégrité) pour la supprimer. Un message s'affiche pour indiquer si la suppression a réussi.

Exclusion de périphériques dans la surveillance de l'intégrité

Au cours de la maintenance normale du réseau, vous désactivez les périphériques ou les rendez temporairement indisponibles. Étant donné que ces pannes sont délibérées, vous ne souhaitez pas que l'état d'intégrité de ces périphériques affecte l'état d'intégrité récapitulatif sur votre centre de gestion.

Vous pouvez utiliser la fonction d'exclusion de la surveillance de l'intégrité pour désactiver les rapports sur l'état de la surveillance de l'intégrité sur un appareil ou un module. Par exemple, si vous savez qu'un segment de votre réseau ne sera pas disponible, vous pouvez désactiver temporairement la surveillance de l'intégrité pour un périphérique géré sur ce segment afin d'éviter que l'état de fonctionnement sur le centre de gestion affiche un avertissement ou un état critique en raison d'une connexion expirée. sur le périphérique.

Lorsque vous désactivez l'état de surveillance de l'intégrité, les événements d'intégrité sont toujours générés, mais ils ont un état désactivé et n'affectent pas l'état d'intégrité de la surveillance de l'intégrité. Si vous retirez le périphérique ou le module de la liste des exclus, les événements générés pendant l'exclusion continuent d'afficher l'état désactivé.

Pour désactiver temporairement les événements d'intégrité d'un appareil, accédez à la page de configuration d'exclusion et ajoutez un appareil à la liste d'exclusion de périphériques. Une fois que le paramètre prend effet, le système ne prend plus en compte le périphérique exclu lors du calcul de l'état d'intégrité général. Le résumé de l'état du périphérique du moniteur de santé répertorie le périphérique comme désactivé.

Vous pouvez également désactiver un module d'intégrité individuel. Par exemple, lorsque vous atteignez la limite de nombre d'hôtes sur le centre de gestion, vous pouvez désactiver les messages d'état de limite d'hôte .

Notez que dans la page principale de surveillance de l'intégrité, vous pouvez faire la distinction entre les périphériques qui sont exclus si vous développez pour afficher la liste des périphériques ayant un état particulier en cliquant sur la flèche dans cette ligne d'état.



Remarque Sur centre de gestion, les paramètres d'exclusion du moniteur de l'intégrité sont des paramètres de configuration locaux. Par conséquent, si vous excluez un périphérique, que vous supprimez puis que vous le réenregistrez avec centre de gestion, les paramètres d'exclusion restent persistants. Le périphérique nouvellement réenregistré reste exclu.

Dans un déploiement multidomaine, les administrateurs des domaines parents peuvent exclure un périphérique ou un module d'intégrité des domaines descendants. Cependant, les administrateurs des domaines descendants peuvent remplacer la configuration ancêtre et effacer l'exclusion des périphériques de leur domaine.

Exclusion de périphériques de la surveillance de l'intégrité

Vous pouvez exclure des périphériques individuellement ou par groupe, par modèle ou par politique d'intégrité associée.

Si vous devez désactiver les événements et l'état d'intégrité d'un appareil individuel, vous pouvez exclure cet appareil. Une fois les paramètres d'exclusion effectifs, le périphérique apparaît comme désactivé dans le récapitulatif du module de surveillance de l'intégrité du périphérique et les événements d'intégrité du périphérique ont l'état désactivé.

Dans un déploiement multidomaine, l'exclusion d'un appareil dans un domaine ancêtre l'exclut de tous les domaines descendants. Les domaines descendants peuvent remplacer cette configuration héritée et effacer l'exclusion. Vous pouvez exclure centre de gestion uniquement au niveau global.

Procédure

-
- Étape 1** Choisissez **System** (⚙) > **Health (intégrité)** > **Exclude (exclure)**.
 - Étape 2** Cliquez sur **Add Devices** (ajoutez des périphériques).
 - Étape 3** Dans la boîte de dialogue d'**exclusion de périphériques**, sous **Périphériques disponibles**, cliquez sur **Ajouter** (+) à côté du périphérique que vous souhaitez exclure de la surveillance de l'intégrité.
 - Étape 4** Cliquez sur **Exclude** (Exclure). Le périphérique sélectionné s'affiche dans la page principale d'exclusion.
 - Étape 5** Pour supprimer le périphérique de la liste d'exclusion, cliquez sur **Supprimer** (🗑).
 - Étape 6** Cliquez sur **Apply**.
-

Prochaine étape

Pour exclure des modules de politique d'intégrité individuels sur les périphériques, consultez [Exclusion des modules de politique de contrôle d'intégrité](#), à la page 20.

Exclusion des modules de politique de contrôle d'intégrité

Vous pouvez exclure des modules de politique d'intégrité individuels sur les périphériques. Vous souhaitez peut-être procéder ainsi pour empêcher les événements du module de faire passer l'appareil à « avertissement » ou à « critique ».

Une fois que les paramètres d'exclusion prennent effet, le périphérique affiche le nombre de modules exclus du périphérique de la surveillance de l'intégrité.



-
- Astuces** Assurez-vous de garder une trace de chaque module exclu afin de pouvoir les réactiver lorsque vous en avez besoin. Vous pourriez passer à côté de messages d'avertissement ou d'avertissements essentiels si vous laissez accidentellement un module désactivé.
-

Dans un déploiement multidomaine, les administrateurs des domaines ascendants peuvent exclure les modules d'intégrité des domaines descendants. Cependant, les administrateurs des domaines descendants peuvent remplacer cette configuration ascendante et effacer l'exclusion pour les politiques appliquées dans leurs domaines. Vous pouvez exclure uniquement les modules d'intégrité centre de gestion au niveau global.

Procédure

- Étape 1** Choisissez **System** (⚙️) > **Health (intégrité)** > **Exclude (exclure)**.
- Étape 2** Cliquez sur **Edit** (✎) à côté de l'appareil que vous souhaitez modifier.
- Étape 3** Dans la boîte de dialogue **Exclure les modules d'intégrité**, par défaut, tous les modules du périphérique sont exclus de la surveillance de l'intégrité. Certains modules ne s'appliquent qu'à des périphériques précis; pour en savoir plus, consultez [Modules d'intégrité, à la page 3](#).
- Étape 4** Pour préciser la durée de l'exclusion du périphérique, dans la liste déroulante **Exclude Period** (Période d'exclusion), sélectionnez la durée.
- Étape 5** Pour choisir les modules à exclure de la surveillance de l'intégrité, cliquez sur le lien **Enable Module Level Exclusion** (activer l'exclusion au niveau du module). La boîte de dialogue **Exclure les modules d'intégrité** affiche tous les modules du périphérique. Les modules qui ne sont pas applicables aux politiques d'intégrité associées sont désactivés par défaut. Pour exclure un module, procédez comme suit :
1. Cliquez sur le bouton **Curseur** (🔘) situé à côté du module souhaité.
 2. Pour préciser la durée de l'exclusion pour les modules sélectionnés, dans la liste déroulante **Période d'exclusion**, sélectionnez la durée.
- Étape 6** Si vous sélectionnez une **période d'exclusion** autre que **permanente** pour votre configuration d'exclusion, vous pouvez choisir de supprimer automatiquement la configuration à son expiration. Pour activer ce paramètre, cochez la case **Auto-delete expired configurations** (supprimer automatiquement les configurations expirées).
- Étape 7** Cliquez sur **OK**.
- Étape 8** Dans la page principale d'exclusion de périphériques, cliquez sur **Apply** (Appliquer).
-

Exclusions du moniteur d'intégrité expiré

À l'expiration de la période d'exclusion d'un périphérique ou de modules, vous pouvez choisir d'effacer ou de renouveler l'exclusion.

Procédure

- Étape 1** Choisissez **System** (⚙️) > **Health (intégrité)** > **Exclude (exclure)**.
- L'icône **Avertissement** (⚠️) s'affiche à côté du périphérique, indiquant l'expiration de la durée d'exclusion du périphérique ou des modules des alertes.
- Étape 2** Pour renouveler l'exclusion du périphérique, cliquez sur **Edit** (✎) à côté du périphérique. Dans la boîte de dialogue **Exclure les modules d'intégrité**, cliquez sur le lien **Renew** (renouveler). La période d'exclusion du périphérique est prolongée de la valeur actuelle.
- Étape 3** Pour faire en sorte que le périphérique ne soit pas exclu, cliquez sur **Supprimer** (🗑️) à côté du périphérique, cliquez sur **Supprimer le périphérique de l'exclusion**, puis cliquez sur **Appliquer**.
- Étape 4** Pour renouveler ou effacer les modules de l'exclusion, cliquez sur **Edit** (✎) à côté du périphérique. Dans la boîte de dialogue **Exclure Health Modules** (Exclure les modules d'intégrité), cliquez sur le lien **Enable**

Module Level Exclusion (activer l'exclusion au niveau du module), puis sur le lien **Renew** ou **Clear** (renouveler ou effacer) à côté des modules. Lorsque vous cliquez sur **Renew**, la période d'exclusion est prolongée sur le module de la valeur actuelle.

Alertes de moniteur d'intégrité

Vous pouvez configurer des alertes pour vous informer par courriel, par SNMP ou par le journal système lorsque l'état des modules d'une politique d'intégrité change. Vous pouvez associer une réponse à une alerte existante à des niveaux d'événement d'intégrité pour déclencher une alerte lorsque des événements d'intégrité d'un niveau particulier se produisent.

Par exemple, si vous craignez que vos périphériques soient à court d'espace sur votre disque dur, vous pouvez envoyer automatiquement un courriel à un administrateur système lorsque l'espace disque restant atteint le niveau d'avertissement. Si le disque dur continue de se remplir, vous pouvez envoyer un deuxième courriel lorsque le disque dur atteindra le niveau critique.

Dans un déploiement multidomaine, vous pouvez afficher et modifier les alertes du moniteur d'intégrité créées dans le domaine actuel uniquement.

Informations sur les alertes du moniteur d'intégrité

Les alertes générées par le moniteur d'intégrité contiennent les informations suivantes :

- Gravité, qui indique le niveau de gravité de l'alerte.
- Module (module), qui spécifie le module d'intégrité dont les résultats du test ont déclenché l'alerte.
- La description, qui comprend les résultats du test d'intégrité qui a déclenché l'alerte.

Le tableau ci-dessous décrit ces niveaux de gravité.

Tableau 4 : Gravités des alertes

Gravité	Description
Éléments essentiels	Les résultats du test d'intégrité ont atteint les critères pour déclencher un état d'alerte Critique.
Avertissement	Les résultats du test d'intégrité ont atteint les critères pour déclencher un état d'alerte Avertissement.
Normal	Les résultats du test d'intégrité ont rencontré les critères pour déclencher un état d'alerte Normal.
Erreur	Le test d'intégrité n'a pas été exécuté.
Récupéré	Les résultats du test d'intégrité ont rempli les critères pour revenir à un état d'alerte normal, après un état d'alerte Critique ou Avertissement.

Création des alertes de moniteur d'intégrité

Vous devez être un utilisateur administrateur pour effectuer cette procédure.

Lorsque vous créez une alerte de moniteur d'intégrité, vous créez une association entre un niveau de gravité, un module d'intégrité et une réponse à une alerte. Vous pouvez utiliser une alerte existante ou en configurer une nouvelle pour produire un rapport sur l'intégrité du système. Lorsque le niveau de gravité se produit pour le module sélectionné, l'alerte se déclenche.

Si vous créez ou mettez à jour un seuil de manière à en dupliquer un existant, vous êtes informé du conflit. Lorsqu'il existe des seuils en double, le moniteur d'intégrité utilise le seuil qui génère le moins d'alertes et ignore les autres. La valeur du délai d'expiration du seuil doit être comprise entre 5 et 4 294 967 295 minutes.

Dans un déploiement multidomaine, vous pouvez afficher et modifier les alertes du moniteur d'intégrité créées dans le domaine actuel uniquement.

Avant de commencer

- Configurer une réponse à l'alerte qui régit la communication de centre de gestion avec SNMP, syslog ou du serveur de messagerie vers lequel vous envoyez l'alerte d'intégrité. voir [Réponses aux alertes Cisco Secure Firewall Management Center](#).

Procédure

- Étape 1** Choisissez **System** (⚙️) > **Alertes** > **de moniteur d'intégrité**.
- Étape 2** Cliquez sur **Add** (ajouter).
- Étape 3** Dans la boîte de dialogue **Add Health Alert** (ajouter une alerte d'intégrité), saisissez un nom pour l'alerte d'intégrité dans le champ **Health Alert Name** (nom de l'alerte d'intégrité).
- Étape 4** Dans la liste déroulante **Severity**, choisissez le niveau de gravité que vous souhaitez utiliser pour déclencher l'alerte.
- Étape 5** Dans la liste déroulante **Alert** (alerte), choisissez la réponse à l'alerte que vous souhaitez déclencher lorsque le niveau de gravité spécifié est atteint. Si vous n'avez pas encore [configuré les réponses aux alertes](#), cliquez sur **Alerts** (alertes) pour accéder à la page **Alertes** et définissez-les.
- Étape 6** Dans la liste **Health Modules** (modules d'intégrité), choisissez les modules de politique d'intégrité pour lesquels vous souhaitez que l'alerte s'applique.
- Étape 7** Éventuellement, dans le champ **Threshold Timeout** (délai d'expiration de seuil), saisissez le nombre de minutes qui doivent s'écouler avant que chaque période de seuil ne se termine et que le nombre de seuils ne soit réinitialisé.
- Même si la valeur de l'intervalle d'exécution de la politique est inférieure à la valeur du délai d'expiration du seuil, l'intervalle entre deux événements d'intégrité signalés par un module donné est toujours plus long. Par exemple, si vous définissez le délai d'expiration de seuil à 8 minutes et que l'intervalle d'exécution de la politique est de 5 minutes, il y a un intervalle de 10 minutes (5 x 2) entre les événements signalés.
- Étape 8** Cliquez sur **Save** (Enregistrer) pour enregistrer l'alerte d'intégrité.
-

Modification des alertes de moniteur d'intégrité

Vous devez être un utilisateur administrateur pour effectuer cette procédure.

Vous pouvez modifier des alertes de moniteur d'intégrité existantes pour changer le niveau de gravité, le module d'intégrité ou la réponse à l'alerte associée à l'alerte de moniteur d'intégrité.

Dans un déploiement multidomaine, vous pouvez afficher et modifier les alertes du moniteur d'intégrité créées dans le domaine actuel uniquement.

Procédure

- Étape 1** Choisissez **System** (⚙) > **Alertes** > **de moniteur d'intégrité**.
 - Étape 2** Cliquez sur l'icône **Edit** (✎) qui se trouve à côté de l'alerte d'intégrité requise que vous souhaitez modifier.
 - Étape 3** Dans la boîte de dialogue **Edit Health Alert** (Modifier les alertes d'intégrité), dans la liste déroulante **Alert**, sélectionnez l'entrée d'alerte requise ou cliquez sur le lien **Alerts** pour configurer une nouvelle entrée d'alerte.
 - Étape 4** Cliquez sur **Save** (enregistrer).
-

Suppression des alertes de moniteur d'intégrité

Dans un déploiement multidomaine, vous pouvez afficher et modifier les alertes du moniteur d'intégrité créées dans le domaine actuel uniquement.

Procédure

- Étape 1** Choisissez **System** (⚙) > **Alertes** > **de moniteur d'intégrité**.
 - Étape 2** Cliquez sur **Supprimer** (🗑) à côté de l'alerte d'intégrité que vous souhaitez supprimer, puis cliquez sur **Supprimer l'alerte d'intégrité** pour la supprimer.
-

Prochaine étape

- Désactivez ou supprimez la réponse à l'alerte sous-jacente pour éviter que l'alerte ne se poursuive; voir [Réponses aux alertes Cisco Secure Firewall Management Center](#).

À propos de la surveillance de l'intégrité

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

La surveillance de l'intégrité fournit l'état d'intégrité compilé de tous les périphériques gérés par centre de gestion, ainsi que centre de gestion lui-même. La surveillance de l'intégrité est composée de :

- La page de résumé de l'état de l'intégrité : vous offre un aperçu rapide de l'intégrité de centre de gestion et de tous les périphériques gérés par centre de gestion. Les périphériques sont répertoriés individuellement ou groupés en fonction de leur géolocalisation, de leur haute disponibilité ou de l'état de la grappe, le cas échéant.
 - Affichez le récapitulatif de l'intégrité du centre de gestion et de tout périphérique lorsque vous passez le curseur sur l'hexagone qui représente l'intégrité du périphérique.
 - Le point à gauche d'un périphérique indique son intégrité :
 - Vert : aucune alarme.
 - Orange : au moins une mise en garde relative à l'intégrité.
 - Rouge : au moins une alarme d'intégrité critique.
- Le volet de navigation Monitoring (surveillance) vous permet de naviguer dans la hiérarchie des périphériques. Vous pouvez afficher les moniteurs d'intégrité pour les périphériques individuels à partir du volet de navigation.

Dans un déploiement multidomaine, le moniteur d'intégrité d'un domaine ancêtre affiche les données de tous les domaines descendants. Dans les domaines descendants, il affiche uniquement les données du domaine actuel.

Procédure

Étape 1

Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Étape 2

Affichez l'état de centre de gestion et de ses périphériques gérés dans la page de destination **Health Status** (État de l'intégrité).

- Passez votre pointeur sur un hexagone pour afficher le résumé de l'intégrité d'un périphérique. La fenêtre contextuelle affiche un résumé tronqué des cinq principales alertes d'intégrité. Cliquez sur dans la fenêtre contextuelle pour ouvrir une vue détaillée du résumé de l'alerte d'intégrité.
- Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (v) pour développer ou réduire la liste des alertes d'intégrité pour un périphérique.

Lorsque vous développez la ligne, toutes les alertes d'intégrité sont répertoriées, y compris l'état, le titre et les détails.

Remarque Les alertes d'intégrité sont triées par niveau de gravité.

Étape 3

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au périphérique. Lorsque vous utilisez le volet de navigation Monitoring (Surveillance) :

- Cliquez sur **Home** (Accueil) pour revenir à la page sommaire de l'état d'intégrité.
- Cliquez sur **Firewall Management Center** pour afficher le moniteur d'intégrité du Cisco Secure Firewall Management Center.
- Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (v) pour développer ou réduire la liste des périphériques gérés.

Lorsque vous développez la ligne, tous les périphériques sont répertoriés.

- d) Cliquez sur un périphérique pour afficher un moniteur d'intégrité spécifique au périphérique.

Prochaine étape

- Consultez [Moniteurs d'intégrité des périphériques, à la page 30](#) pour obtenir des renseignements sur l'état d'intégrité et les mesures compilées de tout périphérique géré par centre de gestion.
- Consultez [Utilisation du moniteur d'intégrité Centre de gestion, à la page 26](#) pour obtenir des renseignements sur l'état de fonctionnement de centre de gestion.

Pour revenir à la page d'accueil de l'état d'intégrité à tout moment, cliquez sur **Home** (Accueil).

Utilisation du moniteur d'intégrité Centre de gestion

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Le moniteur centre de gestion fournit une vue détaillée de l'état de fonctionnement de centre de gestion. La surveillance de l'intégrité est composée de :

- High Availability (Haute disponibilité) (si configurée) : le panneau High Availability (HA) affiche l'état actuel de la haute disponibilité, y compris l'état des unités actives et en veille, l'heure de la dernière synchronisation et l'intégrité générale du périphérique.
- Event Rate (Taux d'événements) : Le panneau Event Rate affiche le taux d'événements maximal comme référence ainsi que le taux global d'événements reçus par centre de gestion.
- Event Capacity (Capacité d'événements) : le panneau Capacité d'événements affiche la consommation actuelle par catégorie d'événements, y compris la durée de rétention des événements, la capacité actuelle par rapport à la capacité maximale d'événements, et un mécanisme de dépassement de capacité par lequel vous êtes alerté lorsque les événements sont stockés au-delà de la capacité maximale configurée du centre de gestion.
- Process Health (Intégrité du processus) : le panneau Intégrité du processus offre un aperçu général des processus critiques ainsi qu'un onglet qui vous permet de voir l'état de tous les processus, y compris l'utilisation du processeur et de la mémoire pour chaque processus.
- CPU (processeur) : le panneau CPU vous permet d'alterner entre l'utilisation moyenne du processeur (par défaut) et l'utilisation du processeur de tous les cœurs.
- Memory (Mémoire) : le panneau Mémoire affiche l'utilisation globale de la mémoire sur centre de gestion.
- Interface : le panneau Interface affiche le débit moyen d'entrée et de sortie de toutes les interfaces.
- Disk Usage (Utilisation du disque) : le panneau Utilisation du disque affiche l'utilisation du disque entier et l'utilisation des partitions critiques où les données centre de gestion sont stockées.
- Hardware Statistics (Statistiques du matériel) : les statistiques du matériel affichent la vitesse du ventilateur, l'alimentation et la température du châssis du centre de gestion. Pour en savoir plus, consultez [Statistiques du matériel sur le centre de gestion, à la page 29](#).



Astuces Votre session vous déconnecte normalement après une heure d'inactivité (ou un autre intervalle configuré). Si vous prévoyez surveiller passivement l'état d'intégrité pendant de longues périodes de temps, pensez à exempter certains utilisateurs du délai d'expiration de session ou à modifier les paramètres d'expiration de délai du système.

Procédure

- Étape 1** Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.
- Étape 2** Utilisez le volet de navigation **Monitoring** (surveillance) pour accéder aux centre de gestion et aux moniteurs d'intégrité spécifiques au périphérique.
- Un centre de gestion autonome s'affiche comme un nœud unique; Un centre de gestion à haute disponibilité est affiché comme une paire de nœuds.
 - La surveillance de l'intégrité est disponible pour les centre de gestion actifs et en veille dans une paire à haute disponibilité.
- Étape 3** Découvrir le tableau de bord centre de gestion.
- Le tableau de bord centre de gestion comprend une vue récapitulative de l'état à haute disponibilité de centre de gestion (si configuré), ainsi qu'un aperçu des processus et des mesures du périphérique centre de gestion, comme l'utilisation du processeur, de la mémoire et du disque.

Exécution de tous les modules d'un appareil

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Les tests du module d'intégrité s'exécutent automatiquement à l'intervalle d'exécution de la politique que vous configurez lorsque vous créez une politique d'intégrité. Cependant, vous pouvez également exécuter tous les tests de module d'intégrité à la demande pour recueillir des informations à jour sur l'intégrité du périphérique .

Dans un déploiement multidomaine, vous pouvez exécuter des tests de module d'intégrité pour les périphériques du domaine actuel et de n'importe quel domaine descendant.

Procédure

- Étape 1** Afficher le moniteur d'intégrité du périphérique .
- Étape 2** Cliquez sur **Run All Modules** (Exécuter tous les modules). La barre d'état indique la progression des tests, puis la page Health Monitor Appliance (Appareil de surveillance d'intégrité) est actualisée.

Remarque Lorsque vous exécutez manuellement des modules d'intégrité, la première actualisation qui se produit automatiquement peut ne pas refléter les données des tests exécutés manuellement. Si la valeur n'a pas changé pour un module que vous venez d'exécuter manuellement, attendez quelques secondes, puis actualisez la page en cliquant sur le nom du périphérique. Vous pouvez également attendre que la page s'actualise à nouveau automatiquement.

Exécution d'un module d'intégrité spécifique

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Les tests du module d'intégrité s'exécutent automatiquement à l'intervalle d'exécution de la politique que vous configurez lorsque vous créez une politique d'intégrité. Cependant, vous pouvez également exécuter un test de module d'intégrité sur demande pour recueillir des informations sur l'intégrité à jour pour ce module.

Dans un déploiement multidomaine, vous pouvez exécuter des tests de module d'intégrité pour les périphériques du domaine actuel et de n'importe quel domaine descendant.

Procédure

-
- Étape 1** Afficher le moniteur d'intégrité du périphérique .
- Étape 2** Dans le graphique **Module Status Summary** (résumé de l'état du module), cliquez sur la couleur de la catégorie d'état d'alerte d'intégrité que vous souhaitez afficher.
- Étape 3** Sur la ligne **Détail** de l'alerte pour l'alerte pour laquelle vous souhaitez afficher une liste des événements, cliquez sur **Exécuter**.
- La barre d'état indique la progression du test, puis la page Health Monitor Appliance (Appareil de surveillance de l'intégrité) est actualisée.
- Remarque** Lorsque vous exécutez manuellement des modules d'intégrité, la première actualisation qui se produit automatiquement peut ne pas refléter les données des tests exécutés manuellement. Si la valeur n'a pas changé pour un module que vous venez d'exécuter manuellement, attendez quelques secondes, puis actualisez la page en cliquant sur le nom du périphérique. Vous pouvez également attendre que la page s'actualise à nouveau automatiquement.
-

Génération de graphiques d'alertes du module d'intégrité

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Vous pouvez faire un graphique des résultats sur une période donnée d'un test d'intégrité particulier pour un appareil spécifique.

Procédure

-
- Étape 1** Afficher le moniteur d'intégrité du périphérique .

Étape 2 Dans le graphique **Module Status Summary** (Résumé de l'état du module) de la page Health Monitor Appliance (Appareil de surveillance de l'intégrité), cliquez sur la couleur de la catégorie d'état d'alerte d'intégrité que vous souhaitez afficher.

Étape 3 Sur la ligne **Détail** de l'alerte pour l'alerte pour laquelle vous souhaitez afficher une liste des événements, cliquez sur **Graphique**.

Astuces Si aucun événement ne s'affiche, vous devrez peut-être ajuster la plage temporelle.

Statistiques du matériel sur le centre de gestion

Les statistiques matérielles de l'appareil du centre de gestion (uniquement physique) comprennent des informations sur ses entités matérielles, telles que la vitesse du ventilateur, l'alimentation et la température. Pour que SNMP interroge et envoie des dérivations pour surveiller l'état et l'intégrité d'un centre de gestion :

1. Activez SNMP sur le centre de gestion pour interroger les MIB. Par défaut, le SNMP sur le centre de gestion est désactivé.
2. Ajoutez une entrée ACL pour chaque hôte SNMP requis pour activer les dérivations. Assurez-vous de spécifier l'adresse IP de l'hôte et de sélectionner le port comme SNMP. Consultez [Configurer une liste d'accès](#).

Pour afficher les statistiques du matériel dans la page **Health > Monitor** (surveillance de l'intégrité) :

1. Dans la page **Health > Policy** (politique d'intégrité), assurez-vous que le module Statistiques matérielles est activé. Vous pouvez modifier les valeurs de seuil par défaut.
2. Ajoutez un portlet au tableau de bord de surveillance de l'intégrité du centre de gestion : sélectionnez le groupe de mesures Hardware Statistics (statistiques matérielles), puis sélectionnez les mesures Fan Speed and Température (vitesse et température du ventilateur).

Vous pouvez afficher l'état du bloc d'alimentation dans le centre de gestion du pare-feu dans la page **Health Monitoring > Home** (Accueil de la surveillance de l'intégrité).



Remarque

- La vitesse du ventilateur est affichée en tr/min.
 - La température est affichée en ° C (Celsius).
 - Lorsqu'un logement du bloc d'alimentation est actif, le tableau de bord l'affiche comme *En ligne* et l'autre comme *No Power* (pas d'alimentation).
 - Chaque ligne horizontale des graphiques indique l'état de chaque bloc d'alimentation et de chaque ventilateur, respectivement.
 - Passez votre curseur sur le graphique pour afficher les données de ces statistiques individuelles.
-

Moniteurs d'intégrité des périphériques

La surveillance de l'intégrité des périphériques fournit l'état d'intégrité compilé dans le temps de tout périphérique géré par centre de gestion. Le moniteur d'intégrité des périphériques recueille les mesures d'intégrité des périphériques Firepower afin de prédire les événements du système et d'y répondre. Le moniteur d'intégrité du périphérique comprend les éléments suivants :

- System Details (détails du système) : affiche des renseignements sur le périphérique géré, y compris la version de Firepower installée et d'autres détails sur le déploiement.
- Dépannage et liens : fournit des liens pratiques vers les rubriques et les procédures de dépannage fréquemment utilisées.
- Alertes d'intégrité : un moniteur d'alertes d'intégrité fournit un aperçu de l'intégrité du périphérique.
- Plage de temps : une fenêtre temporelle réglable pour restreindre les informations qui s'affichent dans les différentes fenêtres de mesures du périphérique.
- Indicateurs des périphériques : un tableau de métriques clés sur l'état des périphériques Firepower, classées dans des tableaux de bord prédéfinis, notamment :
 - CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
 - Mémoire : utilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
 - Interfaces : état de l'interface et statistiques de trafic agrégées.
 - Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
 - Snort : statistiques liées au processus Snort.
 - Utilisation du disque : utilisation du disque du périphérique, y compris la taille du disque et l'utilisation du disque par partition.
 - Processus critiques : les statistiques relatives aux processus gérés, y compris les redémarrages de processus et d'autres paramètres de surveillance d'intégrité tels que l'utilisation du processeur et de la mémoire.

Reportez-vous à la section [Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense](#) pour obtenir une liste complète des indicateurs pris en charge.

Affichage des détails du système et dépannage

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

La section System Details (détails du système) fournit des renseignements généraux sur le système pour un périphérique sélectionné. Vous pouvez également lancer les tâches de dépannage pour ce périphérique.

Procédure

Étape 1 Choisissez **System** (⚙️) > **Moniteur** > **d'intégrité**.

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au périphérique.

Étape 2 Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (<) pour développer ou réduire la liste des périphériques gérés.

Étape 3 Cliquez sur un périphérique pour afficher un moniteur d'intégrité spécifique au périphérique.

Étape 4 Cliquez sur le lien pour **Afficher les détails du système et du dépannage**

Ce panneau est réduit par défaut. Cliquez sur le lien développe la section réduite pour afficher **les détails du système** et les **liens de dépannage** pour le périphérique. Les détails du système comprennent :

- **Version** : version du logiciel Firepower.
- **Modèle** : le modèle du périphérique.
- **Mode** : Le mode de pare-feu. Le périphérique Firepower Threat Defense prend en charge deux modes de pare-feu pour les interfaces de pare-feu standard : le mode routé et le mode transparent.
- **VDB** : version de la base de données sur les vulnérabilités de Cisco (VDB).
- **SRU** : version de l'ensemble de règles de prévention des intrusions.
- **Snort** : la version de Snort.

Étape 5 Les possibilités de dépannage suivantes s'offrent à vous :

- Générer les fichiers de dépannage; consultez [Production de fichiers de dépannage liés à des fonctions système spécifiques](#)
- Générer et télécharger des fichiers de dépannage avancé; consultez [Téléchargement des fichiers de dépannage avancé](#).
- Créer et modifier les politiques de contrôle d'intégrité; consultez [Création de politiques d'intégrité, à la page 16](#).
- Créer et modifier les alertes du moniteur d'intégrité; consultez [Création des alertes de moniteur d'intégrité, à la page 23](#).

Affichage du moniteur d'intégrité du périphérique

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Le moniteur d'intégrité des périphériques fournit une vue détaillée de l'état d'intégrité d'un périphérique de pare-feu. Le moniteur d'intégrité des périphériques compile les mesures du périphérique et fournit l'état d'intégrité et les tendances du périphérique dans un ensemble de tableaux de bord.

Procédure

Étape 1 Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au périphérique.

- Étape 2** Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (v) pour développer ou réduire la liste des périphériques gérés.
- Étape 3** Affichez les **alertes d'intégrité** du périphérique dans la notification d'alerte en haut de la page, directement à droite du nom du périphérique.
- Passer votre pointeur sur les **alertes d'intégrité** pour afficher le résumé de l'intégrité du périphérique. La fenêtre contextuelle affiche un résumé tronqué des cinq principales alertes d'intégrité. Cliquez sur dans la fenêtre contextuelle pour ouvrir une vue détaillée du résumé de l'alerte d'intégrité.
- Étape 4** Vous pouvez configurer la plage temporelle à partir de la liste déroulante dans le coin supérieur droit. La plage de temporelle peut refléter une période aussi courte que la dernière heure (par défaut) ou aussi longue que deux semaines. Sélectionnez **Custom** (Personnalisé) dans la liste déroulante pour configurer des dates de début et de fin personnalisées.
- Cliquez sur l'icône d'actualisation pour définir l'actualisation automatique à 5 minutes ou pour la désactiver.
- Étape 5** Cliquez sur l' **Afficher les informations sur le déploiement** (📄) pour obtenir une superposition du déploiement sur le graphique de tendance, par rapport à la plage temporelle sélectionnée.
- L' **Afficher les informations sur le déploiement** (📄) indique le nombre de déploiements au cours de la plage temporelle sélectionnée. Une bande verticale indique les heures de début et de fin de déploiement. Dans le cas de déploiements multiples, plusieurs bandes/lignes peuvent apparaître. Cliquez sur l'icône en haut de la ligne en pointillé pour afficher les détails du déploiement.
- Étape 6** Le moniteur de périphériques signale par défaut les mesures d'intégrité et de performances dans plusieurs tableaux de bord prédéfinis. Les tableaux de bord des mesures comprennent :
- Aperçu : met en évidence les mesures clés des autres tableaux de bord prédéfinis, y compris les statistiques du processeur, de la mémoire, des interfaces et de la connexion; ainsi que l'utilisation du disque et des informations sur les processus critiques.
 - CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
 - Mémoire : utilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
 - Interfaces : état de l'interface et statistiques de trafic agrégées.
 - Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
 - Snort : statistiques liées au processus Snort.
 - Abandons ASP : statistiques relatives aux performances et au comportement du chemin de sécurité accélérée (ASP).
- Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Reportez-vous à la section [Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense](#) pour obtenir une liste complète des indicateurs pris en charge.
- Étape 7** Cliquez sur le bouton **Add Dashboard** (+) pour créer un tableau de bord de corrélation personnalisé en créant votre propre ensemble de variables à partir des groupes de mesures disponibles; voir [Mettre en corrélation les mesures du périphérique, à la page 33](#).

Mettre en corrélation les mesures du périphérique

Le moniteur d'intégrité des périphériques comprend un tableau des mesures de périphérique clés défense contre les menaces qui servent à prédire les événements du système et à y répondre. L'intégrité de tout périphérique défense contre les menaces peut être déterminée par ces mesures rapportées.

Le moniteur de périphérique signale ces mesures dans plusieurs tableaux de bord prédéfinis par défaut. Ces tableaux de bord comprennent :

- Aperçu : met en évidence les mesures clés des autres tableaux de bord prédéfinis, y compris les statistiques du processeur, de la mémoire, des interfaces et de la connexion; ainsi que l'utilisation du disque et des informations sur les processus critiques.
- CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
- Mémoire : utilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
- Interfaces : état de l'interface et statistiques de trafic agrégées.
- Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
- Snort : statistiques liées au processus Snort.
- Abandons ASP : statistiques relatives aux performances et au comportement du chemin de sécurité accélérée (ASP).

Vous pouvez ajouter des tableaux de bord personnalisés pour corréler des mesures interdépendantes. Sélectionner parmi des groupes de corrélation prédéfinis, tels que le CPU et Snort; ou créez un tableau de bord de corrélation personnalisé en concevant votre propre ensemble de variables à partir des groupes de mesures disponibles. Reportez-vous à la section [Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense](#) pour obtenir une liste complète des indicateurs pris en charge.

Avant de commencer

- Pour afficher et corréler les données de séries chronologiques (métriques de périphérique) dans le tableau de bord de la surveillance de l'intégrité, activez l'API REST (**Settings > Configuration > REST API Preferences**) (Paramètres > Configuration > Préférences de l'API REST).
- Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.



Remarque

La corrélation des métriques de périphériques est disponible uniquement pour défense contre les menaces 6.7 et les versions ultérieures. Par conséquent, pour les versions de défense contre les menaces antérieures à la 6.7, le tableau de bord du moniteur de l'intégrité n'affiche pas ces métriques, même si vous activez l'API REST.

Procédure

Étape 1

Choisissez **System (⚙️) > Moniteur > d'intégrité**.

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au périphérique.

- Étape 2** Dans la liste des **périphériques**, cliquez sur **Développer** (>) et **Réduire** (<) pour développer ou réduire la liste des périphériques gérés.
- Étape 3** Choisissez le périphérique pour lequel vous souhaitez modifier le tableau de bord.
- Étape 4** Cliquez sur l'icône **Ajouter un tableau de bord** (+) dans le coin supérieur droit du moniteur de périphérique pour ajouter un nouveau tableau de bord.
- Étape 5** Dans le menu déroulant **Select Correlation Group** (sélectionner un groupe de corrélation), choisissez un groupe de corrélation prédéfini ou créez un groupe personnalisé.
- Étape 6** Pour créer un tableau de bord à partir d'un groupe de corrélation prédéfini, sélectionnez le groupe et cliquez sur **Add** (Ajouter).
- Étape 7** Pour créer un tableau de bord de corrélation personnalisé :
- Choisissez **Custom** (Personnalisé).
 - Saisissez un nom unique dans le champ de **nom du tableau de bord** ou acceptez le nom par défaut.
 - Choisissez un groupe dans la liste déroulante **Select Metric Group**, puis sélectionnez les mesures correspondantes dans la liste déroulante **Select Metrics**.
- Reportez-vous à la section [Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense](#) pour obtenir une liste complète des indicateurs pris en charge.
- Étape 8** Cliquez sur **Add Metrics** (ajouter des mesures) pour ajouter et sélectionner des indicateurs d'un autre groupe.
- Étape 9** Pour supprimer une mesure en particulier, cliquez sur l'icône **x** à droite de l'élément. Cliquez sur l'icône de suppression pour supprimer le groupe entier.
- Étape 10** Cliquez sur **Add** pour ajouter le tableau de bord au moniteur d'intégrité.
- Étape 11** Vous pouvez **modifier** ou **supprimer** des tableaux de bord de corrélation personnalisés.

Moniteur d'intégrité de la grappe

Lorsque défense contre les menaces est le nœud de contrôle d'une grappe, centre de gestion recueille régulièrement diverses métriques à partir du collecteur de données des métriques du périphérique. Le moniteur d'intégrité de la grappe comprend les composants suivants :

- Tableau de bord de présentation : affiche des informations sur la topologie de la grappe, les statistiques de la grappe et les tableaux de mesures :
 - La section de topologie affiche l'état actuel d'une grappe, l'intégrité de la défense contre les menaces individuelles, le type de nœud de défense contre les menaces (nœud de contrôle ou nœud de données) et l'état du périphérique. L'état du périphérique peut être *Désactivé* (lorsque le périphérique quitte la grappe), *Ajouté prêt à l'emploi* (dans une grappe de nuage public, les nœuds supplémentaires qui n'appartiennent pas à centre de gestion) ou *Normal* (état idéal du nœud) .
 - La section des statistiques de la grappe affiche les métriques actuelles de la grappe en ce qui concerne l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.

**Remarque**

Les mesures de CPU et de mémoire affichent la moyenne individuelle de l'utilisation du plan de données et Snort.

- Les tableaux de mesures, à savoir l'utilisation de la CPU, l'utilisation de la mémoire, le débit et les connexions, affichent sous forme de diagramme les statistiques de la grappe sur la période de temps spécifiée.
- Tableau de bord de répartition de la charge : affiche la répartition de la charge sur les nœuds de la grappe dans deux gadgets :
 - Le gadget Distribution affiche la distribution moyenne des paquets et de la connexion sur la plage temporelle sur les nœuds de la grappe. Ces données décrivent comment la charge est répartie par les nœuds. Ce gadget vous permet de repérer facilement toute anomalie dans la répartition de la charge et d'y remédier.
 - Le gadget Statistiques de nœud affiche les mesures au niveau du nœud sous forme de tableau. Il affiche des données de métriques sur l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions de NAT sur les nœuds de la grappe. Cette vue du tableau vous permet de corréler les données et d'identifier facilement les écarts.
- Tableau de bord des performances des membres : affiche les mesures actuelles des nœuds de la grappe. Vous pouvez utiliser le sélecteur pour filtrer les nœuds et afficher les détails d'un nœud en particulier. Les données de la métrique comprennent l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.
- Tableau de bord CCL : affiche sous forme graphique les données de liaison de commande de grappe, à savoir le débit d'entrée et de sortie.
- Dépannage et liens : contient des liens pratiques vers des rubriques et des procédures de dépannage fréquemment utilisées.
- Plage de temps : une fenêtre temporelle réglable permet de limiter les informations qui s'affichent dans les divers tableaux de bord et gadgets de métriques de grappe.
- Tableau de bord personnalisé : affiche des données sur les mesures à l'échelle de la grappe et au niveau des nœuds. Cependant, la sélection du nœud s'applique uniquement aux mesures de défense contre les menaces et non à l'ensemble de la grappe à laquelle le nœud appartient.

Affichage du moniteur d'intégrité de la grappe

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Le moniteur d'intégrité de grappe fournit une vue détaillée de l'état d'intégrité d'une grappe et de ses nœuds. Ce moniteur d'intégrité de grappe fournit l'état d'intégrité et les tendances de la grappe dans un tableau de bord.

Avant de commencer

- Assurez-vous d'avoir créé une grappe à partir d'un ou de plusieurs périphériques du centre de gestion.

Procédure

- Étape 1** Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.
- Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au nœud.
- Étape 2** Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (v) pour développer ou réduire la liste des périphériques de grappe gérés.
- Étape 3** Pour afficher les statistiques d'intégrité de la grappe, cliquez sur le nom de la grappe. Le moniteur de grappe signale par défaut les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis. Les tableaux de bord des mesures comprennent :
- **Présentation** : met en évidence les mesures clés d'autres tableaux de bord prédéfinis, y compris les nœuds, le processeur, la mémoire, les débits d'entrée et de sortie, les statistiques de connexion et les informations de traduction NAT.
 - **Répartition de la charge** : répartition du trafic et des paquets sur les nœuds de la grappe.
 - **Rendement des membres** : statistiques au niveau du nœud sur l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, la connexion active et la traduction NAT.
 - **CCL** : État de l'interface et statistiques de trafic agrégé.
- Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Pour obtenir une liste complète des mesures de grappe prises en charge, consultez les [Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense](#).
- Étape 4** Vous pouvez configurer la plage temporelle à partir de la liste déroulante dans le coin supérieur droit. La plage de temporelle peut refléter une période aussi courte que la dernière heure (par défaut) ou aussi longue que deux semaines. Sélectionnez **Custom** (Personnalisé) dans la liste déroulante pour configurer des dates de début et de fin personnalisées.
- Cliquez sur l'icône d'actualisation pour définir l'actualisation automatique à 5 minutes ou pour la désactiver.
- Étape 5** Cliquez sur l'icône de déploiement pour une superposition de déploiement sur le graphique de tendance, par rapport à la plage temporelle sélectionnée.
- L'icône de déploiement indique le nombre de déploiements au cours de la plage temporelle sélectionnée. Une bande verticale indique les heures de début et de fin de déploiement. Pour les déploiements multiples, plusieurs bandes/lignes s'affichent. Cliquez sur l'icône en haut de la ligne en pointillé pour afficher les détails du déploiement.
- Étape 6** (Pour la surveillance de l'intégrité spécifique au nœud) Affichez les **alertes d'intégrité** du nœud dans la notification d'alerte en haut de la page, directement à droite du nom du périphérique.
- Passez votre pointeur sur les **alertes d'intégrité** pour afficher le résumé de l'intégrité du nœud. La fenêtre contextuelle affiche un résumé tronqué des cinq principales alertes d'intégrité. Cliquez sur dans la fenêtre contextuelle pour ouvrir une vue détaillée du résumé de l'alerte d'intégrité.
- Étape 7** (Pour le moniteur d'intégrité propre à un nœud) Le moniteur de périphérique signale les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis par défaut. Les tableaux de bord des mesures comprennent :

- Aperçu : met en évidence les mesures clés des autres tableaux de bord prédéfinis, y compris les statistiques du processeur, de la mémoire, des interfaces et de la connexion; ainsi que l'utilisation du disque et des informations sur les processus critiques.
- CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
- Mémoire : utilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
- Interfaces : état de l'interface et statistiques de trafic agrégées.
- Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
- Snort : Statistiques liées au processus Snort.
- Abandons ASP : Statistiques sur les paquets abandonnés pour diverses raisons.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Reportez-vous à la section [Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense](#) pour obtenir une liste complète des indicateurs pris en charge.

Étape 8

Cliquez sur le signe plus (+) dans le coin supérieur droit du moniteur d'intégrité pour créer un tableau de bord personnalisé en concevant votre propre ensemble de variables à partir des groupes de mesures disponibles.

Pour le tableau de bord à l'échelle de la grappe, choisissez Groupe de mesures de la grappe, puis choisissez la métrique.

Catégories d'état du moniteur de surveillance de l'intégrité

Les catégories d'état disponibles sont répertoriées par gravité dans le tableau ci-dessous.

Tableau 5 : Indicateur d'état d'intégrité

Niveau d'état	Icône d'état	Couleur de l'état dans le graphique à secteurs	Description
Erreur	Erreur (✖)	Noir	Indique qu'au moins un module de surveillance de l'intégrité est défaillant sur le périphérique et n'a pas été réexécuté avec succès depuis la défaillance. Contactez votre représentant du soutien technique pour obtenir une mise à jour du module de surveillance de l'intégrité.
Éléments essentiels	Critique (⚠)	Rouge	Indique que les limites critiques ont été dépassées pour au moins un module d'intégrité du périphérique et que le problème n'a pas été corrigé.

Niveau d'état	Icône d'état	Couleur de l'état dans le graphique à secteurs	Description
Avertissement	Avertissement (⚠)	Jaune	Indique que les limites d'avertissement ont été dépassées pour au moins un module d'intégrité sur le périphérique et que le problème n'a pas été corrigé. Cet état indique également un état transitoire, dans lequel les données requises sont temporairement indisponibles ou n'ont pas pu être traitées en raison de modifications dans la configuration du périphérique. Selon le cycle de surveillance, cet état transitoire est corrigé automatiquement.
Normal	Normal (✓)	Vert	Indique que tous les modules d'intégrité du périphérique fonctionnent dans les limites configurées dans la politique d'intégrité appliquée au périphérique.
Récupéré	Récupéré (✓)	Vert	Indique que tous les modules d'intégrité du périphérique fonctionnent dans les limites configurées dans la politique d'intégrité appliquée au périphérique, y compris les modules qui étaient dans un état critique ou d'avertissement.
Désactivé	Désactivé (⊘)	Bleu	Indique qu'un appareil est désactivé ou exclu, qu'aucune politique d'intégrité n'est appliquée au périphérique ou que le périphérique est actuellement inaccessible.

Vues des événements liés à l'intégrité

La page Health Event View (affichage des événements d'intégrité) vous permet d'afficher les événements d'intégrité enregistrés par le moniteur d'intégrité dans les journaux d'intégrité centre de gestion. Les affichages des événements entièrement personnalisables vous permettent d'analyser rapidement et facilement les événements d'état d'intégrité recueillis par le moniteur d'intégrité. Vous pouvez rechercher des données d'événements pour accéder facilement à d'autres informations qui peuvent être liées aux événements sur lesquels vous étudiez. Si vous comprenez les conditions que teste chaque module d'intégrité, vous pouvez configurer plus efficacement les alertes pour les événements d'intégrité.

Vous pouvez effectuer la plupart des fonctions standard de l'affichage des événements dans les pages d'affichage des événements d'intégrité.

Affichage des événements d'intégrité

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

La page Tableau des événements d'intégrité fournit une liste de tous les événements d'intégrité sur le périphérique spécifié.

Lorsque vous accédez aux événements d'intégrité à partir de la page Health Monitor (Moniteur d'intégrité) de votre centre de gestion, vous récupérez tous les événements d'intégrité pour tous les périphériques gérés.

Dans un déploiement multidomaine, vous pouvez afficher les données du domaine actuel et de tous les domaines descendants. Vous ne pouvez pas afficher les données des domaines de niveau supérieur ou connexes.



Astuces Vous pouvez mettre cet affichage en signet pour vous permettre de revenir à la page du flux de travail des événements d'intégrité contenant le tableau des événements Health Events (d'intégrité). La vue mise en signet récupère les événements de la plage temporelle que vous consultez actuellement, mais vous pouvez ensuite modifier cette plage pour mettre à jour le tableau avec des informations plus récentes si nécessaire.

Procédure

Choisissez **System** (⚙️) > **Événements** > **liés à l'intégrité**.

Astuces Si vous utilisez un flux de travail personnalisé qui n'inclut pas l'affichage du tableau des événements d'intégrité, cliquez sur (**switch workflow**) (changer de flux de travail). Dans la page Select Workflow (sélectionner un flux de travaux), cliquez sur **Health Events (événements d'intégrité)**.

Remarque Si aucun événement ne s'affiche, vous devrez peut-être ajuster la plage temporelle.

Affichage du tableau des événements d'intégrité

Dans un déploiement multidomaine, vous pouvez afficher les données du domaine actuel et de tous les domaines descendants. Vous ne pouvez pas afficher les données des domaines de niveau supérieur ou connexes.

Procédure

Étape 1 Choisissez **System** (⚙️) > **Événements** > **liés à l'intégrité**.

Étape 2 Vous avez les choix suivants :

- **Signet** : pour mettre la page actuelle en signet afin que vous puissiez y revenir rapidement, cliquez sur **Bookmark this page (Créer un signet à partir de cette page)**, attribuez un nom au signet, puis cliquez sur **Save** (Enregistrer).
- **Modifier le flux de travail** : pour choisir un autre flux de travail d'événements d'intégrité, cliquez sur (**switch workflow**) (**changer de flux de travail**).
- **Supprimer les événements** : pour supprimer des événements d'intégrité, cochez la case en regard des événements que vous souhaitez supprimer, puis cliquez sur **Delete** (Supprimer). Pour supprimer tous les événements de la vue limitée actuelle, cliquez sur **Delete All** (Supprimer tout), puis confirmez que vous souhaitez supprimer tous les événements.
- **Générer des rapports** : pour générer un rapport en fonction des données de la vue tableau, cliquez sur **Concepteur de rapports**.

- **Modifier** : modifiez la plage temporelle et de date des événements répertoriés dans la vue du tableau Intégrité. Notez que les événements générés en dehors de la fenêtre temporelle configurée de l'appareil (qu'ils soient globaux ou spécifiques à un événement) peuvent apparaître dans une vue d'événements si vous limitez la vue d'événements en fonction du temps. Ce problème peut se produire même si vous avez configuré une fenêtre temporelle glissante pour l'appareil.
- **Naviguer** : naviguez dans les pages d'affichage des événements.
- **Naviguer dans les signets** : pour accéder à la page de gestion des signets, cliquez sur **View Bookmarks** (afficher les signets) dans n'importe quel affichage d'événement.
- **Naviguer autre** : naviguez vers d'autres tableaux d'événements pour afficher les événements associés.
- **Trier** : permet de trier les événements qui s'affichent, de modifier les colonnes du tableau des événements ou de restreindre les événements qui s'affichent
- **Afficher tout** : pour afficher les détails de tous les événements dans la vue, cliquez sur **View All**(afficher tout).
- **Afficher les détails** : pour afficher les détails associés à un événement d'intégrité unique, cliquez sur le lien fléché vers le bas à gauche de l'événement.
- **Afficher plusieurs** : pour afficher les détails de plusieurs événements d'intégrité, cochez la case à côté des lignes qui correspondent aux événements dont vous souhaitez afficher les détails, puis cliquez sur **View** (Afficher).
- **Afficher l'état** : pour afficher tous les événements d'un état particulier, cliquez sur état dans la colonne Status (état) pour un événement avec cet état.

Tableau des événements d'intégrité

Les modules du moniteur de l'intégrité que vous choisissez d'activer dans votre politique d'intégrité exécutent divers tests pour déterminer l'état d'intégrité de l'appareil. Lorsque l'état d'intégrité répond aux critères que vous spécifiez, un événement d'intégrité est généré.

Le tableau ci-dessous décrit les champs qui peuvent être affichés et recherchés dans le tableau des événements d'intégrité.

Tableau 6 : Champs des événements liés à l'intégrité

Champ	Description
Nom du module	Précisez le nom du module qui a généré les événements d'intégrité que vous souhaitez afficher. Par exemple, pour afficher les événements qui mesurent les performances de la CPU, tapez <code>CPU</code> . La recherche devrait récupérer les événements applicables d'utilisation de la CPU et de température de la CPU.
Nom du test (Recherche uniquement)	Le nom du module d'intégrité qui a généré l'événement.
Durée (Recherche uniquement)	Horodatage de l'événement d'intégrité.

Champ	Description
Description	La description du module d'intégrité qui a généré l'événement. Par exemple, les événements d'intégrité générés lorsqu'un processus n'a pas pu s'exécuter sont étiquetés <code>Unable to Execute</code> .
Valeur	Valeur (nombre d'unités) du résultat obtenu par le test d'intégrité qui a généré l'événement. Par exemple, si centre de gestion génère un événement d'intégrité chaque fois qu'un périphérique qu'il surveille utilise 80 % ou plus de ses ressources de CPU, la valeur peut être un nombre compris entre 80 et 100.
Unités	Descripteur d'unités pour le résultat. Vous pouvez utiliser l'astérisque (*) pour créer des recherches avec des caractères génériques. Par exemple, si le centre de gestion génère un événement d'intégrité lorsqu'un périphérique qu'il surveille utilise 80 % ou plus de ses ressources de CPU, le descripteur d'unités est un signe de pourcentage (%).
État	L'état (critique, jaune, vert ou désactivé) signalé pour le périphérique.
Domaine	Pour les événements d'intégrité signalés par les périphériques gérés, domaine du périphérique qui a signalé l'événement d'intégrité. Pour les événements d'intégrité physique signalés par centre de gestion, <code>global</code> . Ce champ n'est présent que dans un déploiement multidomaine.
Périphérique	L'appareil sur lequel l'événement d'intégrité a été signalé.

À propos de l'audit du système

Les périphériques qui font partie du système Firepower génèrent un enregistrement d'audit pour chaque interaction de l'utilisateur avec l'interface Web.

Dossiers d'audit

Les consignent des renseignements d'audit en lecture seule pour l'activité des utilisateurs. Les journaux d'audit sont présentés dans une vue d'événements standard qui vous permet d'afficher, de trier et de filtrer les messages des journaux d'audit en fonction de tout élément de la vue d'audit. Vous pouvez facilement supprimer les informations d'audit, en faire un rapport, et afficher des rapports détaillés sur les modifications apportées par les utilisateurs.

Le journal d'audit stocke un maximum de 100 000 entrées. Lorsque le nombre d'entrées du journal d'audit dépasse 100 000, le périphérique élague les enregistrements les plus anciens de la base de données pour réduire le nombre à 100 000.

Les journaux d'audit n'affichent pas l'utilisateur ou l'adresse IP source pour les erreurs de connexion :

- Lorsqu'un mauvais mot de passe est utilisé, l'adresse IP source ne s'affiche pas.
- Lorsque le compte d'utilisateur n'existe pas, l'adresse IP source et le nom d'utilisateur ne s'affichent pas.

- Si la tentative pour un utilisateur LDAP échoue, aucun journal d'audit n'est déclenché.

Sujets connexes

[Directives SSO pour Centre de gestion](#)

Champs de flux de travail du journal d'audit

Le tableau suivant décrit les champs du journal d'audit qui peuvent être affichés et recherchés.

Tableau 7 : Champs du journal d'audit

Champ	Description
Durée	Heure et date auxquelles le périphérique a généré l'enregistrement d'audit.
Utilisateur	Nom d'utilisateur de l'utilisateur qui a déclenché l'événement d'audit.
Sous-système	Dans les quelques cas où le chemin de menu n'est pas pertinent, le champ Sous-système affiche uniquement le type d'événement. Par exemple, Login (connexion) classe les tentatives de connexion des utilisateurs.
Message	L'action que l'utilisateur a effectuée ou le bouton de la page sur lequel l'utilisateur a cliqué. Par exemple, <code>Page View</code> signifie que l'utilisateur a simplement consulté la page indiquée dans le sous-système, tandis que <code>save</code> signifie que l'utilisateur a cliqué sur le bouton Save (Enregistrer) de la page. Les modifications apportées au système apparaissent avec une icône de comparaison sur laquelle vous pouvez cliquer pour voir un résumé des modifications.
IP de la source	Adresse IP associée à l'hôte utilisé par l'utilisateur. Remarque : Lors de la recherche dans ce champ, vous devez taper une adresse IP précise; vous ne pouvez pas utiliser de plages d'adresses IP lors de la recherche dans les journaux d'audit.
Domaine	Domaine actuel de l'utilisateur lorsque l'événement d'audit a été déclenché. Ce champ n'est présent que si vous avez déjà configuré centre de gestion pour la multilocalisation de détention.
Modification de configuration (recherche uniquement)	Spécifie s'il faut afficher les enregistrements d'audit des modifications de configuration dans les résultats de la recherche. (<i>oui ou non</i>)
Nombre	Le nombre d'événements correspondant aux informations affichées dans chaque ligne. Notez que le champ Nombre ne s'affiche qu'après l'application d'une restriction qui crée deux lignes identiques ou plus. Il n'est pas possible de rechercher ce champ.

La vue de tableau des événements d'audit

Vous pouvez modifier la présentation de la vue des événements ou restreindre les événements de la vue par une valeur de champ. Lors de la désactivation des colonnes, après avoir cliqué sur **Fermer** (✕) dans l'en-tête

de la colonne que vous souhaitez masquer, dans la fenêtre contextuelle qui apparaît, cliquez sur **Apply** (Appliquer). Lorsque vous désactivez une colonne, elle est désactivée pour la durée de votre session (sauf si vous la rajoutez ultérieurement). Notez que lorsque vous désactivez la première colonne, la colonne Nombre est ajoutée.

Pour masquer ou afficher d'autres colonnes, ou pour rajouter une colonne désactivée à la vue, cochez ou décochez les cases appropriées avant de cliquer sur **Apply** (Appliquer).

Le fait de cliquer sur une valeur dans une ligne dans un affichage tableau restreint l'affichage tableau et ne fait pas défiler vers le bas à la page suivante dans le flux de travail.



Astuces Les affichages tableaux comprennent toujours « Table View » dans le nom de la page.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.