

Journalisation

Ce chapitre décrit comment consigner les messages système et les utiliser pour la résolution de problèmes.

- À propos de la journalisation, à la page 1
- Lignes directrices relatives à la journalisation, à la page 9
- Configurer la journalisation, à la page 11
- Supervision des journaux, à la page 33
- Historique de journalisation, à la page 38

À propos de la journalisation

La journalisation du système est une méthode de collecte de messages des périphériques vers un serveur exécutant un daemon syslog. La journalisation sur un serveur syslog central facilite l'agrégation des journaux et des alertes. Les périphériques Cisco peuvent envoyer leurs messages de journal à un service syslog de type UNIX. Un service syslog accepte les messages et les stocke dans des fichiers ou les imprimés conformément à un fichier de configuration simple. Cette forme de journalisation offre un stockage protégé à long terme pour les journaux. Les journaux sont utiles pour les dépannages de routine et pour le traitement des incidents.

Les journaux système d'ASA vous fournissent des renseignements pour superviser et dépanner l'ASA. La fonction de journalisation vous permet d'effectuer les opérations suivantes :

- Spécifier quels messages du journal système doivent être enregistrés.
- Désactiver ou modifier le niveau de gravité d'un message du journal système.
- Préciser au moins un emplacement où les messages du journal système doivent être envoyés, notamment :
    - Un tampon interne
    - Un ou plusieurs serveurs de journal système
    - ASDM
    - Une station de gestion SNMP
    - Des adresses courriel spécifiées
    - Console
    - Sessions Telnet et SSH.

- Configurer et gérer les messages de journal système en groupes, par exemple par niveau de gravité ou classe de message.
- Spécifier si une limite de débit est appliquée ou non à la génération du journal système.
- Préciser ce qu'il arrive au contenu du tampon du journal interne lorsqu'il est plein : écraser le tampon, envoyer le contenu du tampon à un serveur FTP ou enregistrer le contenu dans la mémoire flash interne.
- Filtrer les messages du journal système par emplacements, niveau de gravité, classe ou liste de messages sur mesure.

Journalisation dans le mode de contexte multiple

Chaque contexte de sécurité comprend sa propre configuration de journalisation et génère ses propres messages. Si vous vous connectez au contexte de système ou d'administration, puis passez à un autre contexte, les messages que vous affichez dans votre session ne sont que les messages liés au contexte actuel.

Les messages de journal système qui sont générés dans l'espace d'exécution du système, y compris les messages de basculement, sont consultés dans le contexte d'administration avec les messages générés dans le contexte d'administration. Vous ne pouvez pas configurer la journalisation ni afficher des renseignements de journalisation dans l'espace d'exécution du système.

Vous pouvez configurer l'ASA pour inclure le nom de contexte dans chaque message, ce qui vous aide à différencier les messages de contexte qui sont envoyés à un seul serveur de journal système. Cette fonctionnalité vous aide également à déterminer quels messages proviennent du contexte d'administration et lesquels proviennent du système. Les messages qui proviennent de l'espace d'exécution du système utilisent un ID de périphérique de **système**, et les messages qui proviennent du contexte d'administration utilisent le nom du contexte d'administration comme ID de périphérique.

Analyse des messages du journal système

Voici quelques exemples du type de renseignements que vous pouvez obtenir en examinant différents messages du journal système :

- Les connexions autorisées par les politiques de sécurité d'ASA. Ces messages vous aident à repérer les failles qui restent ouvertes dans vos politiques de sécurité.
- Les connexions refusées par les politiques de sécurité d'ASA. Ces messages indiquent quels types d'activités sont dirigées vers votre réseau interne sécurisé.
- L'utilisation de la fonctionnalité de journalisation du taux de refus ACE affiche les attaques qui se produisent sur votre ASA.
- Les messages d'activité d'IDS peuvent afficher les attaques qui se sont produites.
- L'authentification de l'utilisateur et l'utilisation des commandes fournissent une piste d'audit des modifications des politiques de sécurité.
- Les messages d'utilisation de la bande passante affichent chaque connexion qui a été établie et détruite, ainsi que la durée et le volume de trafic utilisés.
- Les messages d'utilisation des protocoles affichent les protocoles et les numéros de port utilisés pour chaque connexion.

- Les messages de piste d'audit de traduction d'adresses enregistrent les connexions NAT ou PAT en cours d'établissement ou de destruction, ce qui est utile si vous recevez un rapport des activités malveillantes provenant de l'intérieur de votre réseau vers l'extérieur.

Format des messages du journal système

Les messages du journal système sont structurés comme suit :

`[<PRI>]: [Timestamp] [Device-ID] : %-Level-Message_number: Message_text`

Les descriptions des champs sont les suivantes :

<PRI>	Valeur de la priorité. Lorsque la journalisation EMBLEM est activée, cette valeur s'affiche dans le message de journal système. La journalisation EMBLEM est compatible avec UDP et non avec TCP.
Horodatage	La date et l'heure de l'événement s'affichent. Lorsque la journalisation des horodatages est activée, et si l'horodatage est configuré pour être au format RFC 5424, tous les horodatages dans les messages de journal système affichent l'heure en heure UTC, comme indiqué par la norme RFC 5424.
Device-ID	La chaîne d'identifiant du périphérique qui a été configurée lors de l'activation de l'option logging device-id par l' interface utilisateur. Si cette option est activée, l'ID de périphérique n'apparaît pas dans les messages de journal système au format EMBLEM.
	Le code d'installation du message de journal système pour les messages générés par l'. .
Level (Niveau)	Le niveau reflète la gravité de la condition décrite par le message de journal système : plus le nombre est bas, plus la condition est critique.
Message_number	Un numéro à six chiffres unique qui identifie le message de journal système.
Message_text	Une chaîne de texte qui décrit la condition. Cette partie du message de journal système comprend parfois des adresses IP, des numéros de port ou des noms d'utilisateurs.

Tous les messages de journal système générés par le périphérique sont documentés dans le guide Messages de journal système de la série Cisco Secure Firewall ASA.

Le format syslog EMBLEM est une convention propre à Cisco, fondée sur les normes RFC 3164 et RFC 5424. Ainsi, lorsque EMBLEM est activé, le message syslog affiche deux-points (:) après le champ <PRI>.

Exemple de message de journal système avec la journalisation EMBLEM, la journalisation de l'horodatage RFC 5424 et l'ID de périphérique activés. Notez les deux-points (:) après le champ <PRI> (*<166>*).

`<166>:2018-06-27T12:17:46Z: %-6-110002 : échec de localisation de l'interface de sortie pour le protocole de l'interface src : port IP/src à l'adresse IP/au port de destination`

Exemple de message de journal système avec la journalisation de l'horodatage RFC 5424 et l'ID de périphérique activés. Il n'y a pas de deux-points (:) avant l'horodatage.

`2018-06-27T12:17:46Z : %-6-110002 : échec de localisation de l'interface de sortie pour le protocole de l'interface src : port IP/src à l'adresse IP/au port de destination`

Niveaux de gravité des messages Syslog

Les niveaux de gravité des messages syslog définissent l'importance des messages système. Vous pouvez affecter des couleurs personnalisées à chacun des niveaux de gravité pour faciliter leur distinction dans les visualiseurs de journaux ASDM. Pour configurer les paramètres de couleur des messages du journal système, sélectionnez l'onglet **Outils > Préférences » Syslog** ou, dans la visionneuse de journal elle-même, cliquez sur **Paramètres de couleur** dans la barre d'outils.

Tableau 1 : Niveaux de gravité des messages Syslog

Numéro de niveau	Niveau de gravité	Description
0	**urgences**	Vous ne pouvez pas utiliser le système.
1	**alerte**	Vous devez agir immédiatement.
2	**critique**	Le système présente des conditions critiques à traiter.
3	**erreur**	Conditions d'erreur.
4	**avertissement**	Le système comporte des avertissements que vous devez consulter.
5	**notification**	Le système signale les événements importants que vous devez superviser.
6	**renseignements**	Messages informatifs seulement.
7	**débogage**	Le système génère uniquement des messages de débogage. Ne journalisez à ce niveau que temporairement, lors du débogage des problèmes. Ce niveau de journalisation peut générer de nombreux messages, ce qui peut affecter les performances du système.

Remarque ASA ne génère pas de messages syslog avec un niveau de gravité établi à zéro (urgences).

Filtres de messages syslog

Critères de filtrage des messages Syslog

Vous pouvez diriger les messages syslog vers une destination de sortie en fonction des critères suivants :

- Numéros d'ID des messages Syslog
- Niveau de gravité des messages du journal système
- Classe de messages Syslog (équivalente à une zone fonctionnelle)

Vous pouvez créer une liste de messages avec des critères spécifiques, que vous pouvez ensuite préciser lorsque la destination de la sortie est définie. Sinon, vous pouvez configurer les ASA pour envoyer une classe de messages particulière à chaque type de destination de sortie indépendamment de la liste de messages.

Classes de messages syslog et numéros d'ID de messages associés

Vous pouvez utiliser les classes de messages syslog de deux manières :

- Précisez un emplacement de sortie pour toute une catégorie de messages du journal système.
- Créez une liste de messages qui spécifie la classe du message.

Utilisez la classe de messages syslog pour catégoriser les messages syslog par type, comme les fonctionnalités ou les fonctions du périphérique. Par exemple, utilisez la classe RIP pour le routage RIP.

Tous les messages syslog d'une classe particulière partagent les trois mêmes chiffres initiaux dans leurs numéros d'ID de message syslog. Par exemple, les messages syslog pour la fonctionnalité de client VPN utilisent les numéros d'ID de 611101 à 611323.

La plupart des messages syslog ISAKMP comprennent des objets ajoutés au début qui identifient le tunnel. Ces objets précèdent le texte descriptif d'un message syslog lorsqu'ils sont disponibles. Si l'objet est inconnu lorsque le message syslog est généré, la combinaison d'en-tête et de valeur est omise.

Les objets sont préfixés de cette manière :

Group = *groupname*, Username = *user*, IP = *IP_address*

Le terme « groupe » ici fait référence à la configuration de groupe de tunnel. Le nom d'utilisateur provient de la base de données locale ou du serveur AAA. Il s'agit de l'adresse IP publique du client d'accès à distance ou de l'homologue de couche 2.

Le tableau suivant répertorie les classes de messages et la plage d'ID de message dans chaque classe.

Tableau 2 : Classes de messages syslog et numéros d'ID de messages associés

Classe	Définition	Numéros d'ID des messages Syslog
auth	Authentification de l'utilisateur	109, 113
—	Listes d'accès	106
—	Pare-feu d'application	415
—	Filtre de trafic de réseau de zombies	338
bridge (pont)	Pare-feu transparent	110, 220
ca	Autorité de certification de l'infrastructure de clé publique (PKI)	717
citrix	Client Citrix	723
—	Mise en grappe	747
—	Gestion des cartes	323

Classe	Définition	Numéros d'ID des messages Syslog
config (configurer)	Interface de commande	111, 112, 208, 308
csd	Poste de travail sécurisé	724
cts	TrustSec de Cisco	776
DAP	Politiques d'accès dynamique	734
EAP, eapoudp	EAP ou EAPoUDP pour le contrôle d'admission au réseau	333, 334
EIGRP	Routage EIGRP	336
e-mail	Serveur mandataire de courriel	719
—	Surveillance de l'environnement	735
ha	Basculement	101, 102, 103, 104, 105, 210, 311, 709
—	Pare-feu basé sur l'identité	746
ids	Système de détection des intrusions	400, 733
—	Boîte à outils IKEv2	750, 751, 752
IP	Pile d'adresse IP	209, 215, 313, 317, 408
ipaa	Affectation d'adresse IP	735
ips	Système de protection contre les intrusions	400, 401, 420
—	IPv6	325
—	Licence	444
MDM-proxy	Mandataire MDM	802
NAC	Contrôle d'admission au réseau (NAC)	731, 732
nacpolicy	Politique NAC	731
nacsettings	Paramètres NAC pour appliquer la politique NAC	732
—	NAT et PAT	305
—	Point d'accès réseau	713
NP	Processeur de réseau	319
—	NP SSL	725

Classe	Définition	Numéros d'ID des messages Syslog
OSPF	Routage OSPF	318, 409, 503, 613
—	Chiffrement de mot de passe	742
—	Serveur mandataire téléphonique	337
RIP	Routage RIP	107, 312
rm	Gestionnaire des ressources	321
—	Smart Call Home	120
séance de formation	Séance d'utilisateur	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
SNMP	SNMP	212
—	ScanSafe	775
SSL	Pile SSL	725
svc	Client VPN SSL	722
sys	Système	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
—	Détection des menaces	733
tag-switching	Commutation de balise de service	779
transactional-rule-engine-tre	Moteur de règles transactionnelles	780
uc-IMS	UC-IMS	339
vm	Mise en correspondance VLAN	730
vpdn	Sessions PPTP et L2TP	213, 403, 603
VPN	IKE et IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	Client VPN	611
vpnfo	Basculement du VPN	720
vpnlb	Équilibrage de la charge VPN	718
—	VXLAN	778
webfo	Basculement WebVPN	721

Classe	Définition	Numéros d'ID des messages Syslog
webvpn	WebVPN et Secure Client (services client sécurisés)	716

Trier les messages dans les visionneuses de journaux

Vous pouvez trier les messages dans toutes les visionneuses de journaux ASDM (c'est-à-dire la visionneuse de journaux en temps réel, la visionneuse de tampons de journaux et la dernière visionneuse d'événements du journal système ASDM). Pour trier les tableaux en fonction de plusieurs colonnes, cliquez sur l'en-tête de la première colonne que vous souhaitez trier, puis maintenez la touche **Ctrl** enfoncée et cliquez simultanément sur les en-têtes des autres colonnes que vous souhaitez inclure dans l'ordre de tri. Pour trier les messages par ordre chronologique, sélectionnez les colonnes de date et d'heure; sinon, les messages sont triés uniquement par date (peu importe l'heure) ou uniquement par heure (peu importe la date).

Lorsque vous triez des messages dans la visionneuse de journaux en temps réel et dans la dernière visionneuse d'événements du journal système ASDM, les nouveaux messages qui arrivent apparaissent dans l'ordre de tri, et non en haut, comme c'est normalement le cas. Autrement dit, ils sont mélangés avec les autres messages.

Listes de messages personnalisés

La création d'une liste de messages personnalisée est un moyen flexible d'exercer un contrôle sur les messages du journal système qui sont envoyés vers une destination de sortie spécifique. Dans une liste de messages de journal système personnalisée, vous spécifiez des groupes de messages de journal système à l'aide d'un ou de tous les critères suivants :

- Niveau de gravité
- ID du message
- Plages d'ID des messages du journal système
- Classe de messages.

Par exemple, vous pouvez utiliser des listes de messages pour effectuer les opérations suivantes :

- Sélectionnez les messages du journal système avec les niveaux de gravité 1 et 2 et envoyez-les à une ou plusieurs adresses courriel.
- Sélectionnez tous les messages du journal système associés à une classe de messages (comme ha) et enregistrez-les dans le tampon interne.

Une liste de messages peut inclure plusieurs critères de sélection des messages. Cependant, vous devez ajouter chaque critère de sélection des messages à l'aide d'une nouvelle entrée de commande. Il est possible de créer une liste de messages qui comprend des critères de sélection des messages qui se chevauchent. Si deux critères d'une liste de messages sélectionnent le même message, le message est journalisé une seule fois.

Mise en grappe

Les messages du journal système sont un outil inestimable pour la comptabilité, la surveillance et le dépannage dans un environnement de grappe. Chaque unité ASA de la grappe (jusqu'à huit unités sont autorisées) génère

des messages de journal système de manière indépendante; certaines commandes **logging** vous permettent ensuite de contrôler les champs d'en-tête, qui comprennent un horodatage et un ID de périphérique. Le serveur de journal système utilise l'ID de périphérique pour identifier le générateur de journaux systèmes. Vous pouvez utiliser la commande **logging device-id** pour générer des messages de journal système avec des ID de périphérique identiques ou différents afin de faire apparaître les messages comme provenant d'unités identiques ou différentes dans la grappe.



Remarque Pour superviser les messages de journal système provenant des unités d'une grappe, vous devez ouvrir une session ASDM pour chacune des unités que vous souhaitez superviser.

Lignes directrices relatives à la journalisation

Restrictions pour la journalisation IPv6

- IPv6 est pris en charge. Un message syslog peut être envoyé à l'aide de TCP ou d'UDP.
- Assurez-vous que l'interface configurée pour l'envoi des journaux système est activée, qu'elle est compatible avec IPv6, et que le serveur syslog est accessible par l'intermédiaire de l'interface désignée.
- Vous ne pouvez pas utiliser IPv6 pour une journalisation sécurisée.

Lignes directrices relatives à la configuration du serveur syslog

- Le serveur syslog doit exécuter un programme de serveur appelé syslogd. Windows fournit un serveur syslog dans le cadre de son système d'exploitation.
- Le serveur syslog fonctionne selon le processus syslog-ng du système de pare-feu. N'utilisez pas de fichiers de configuration externes, comme le fichier *scwx.conf* de SecureWorks. Étant donné que ces fichiers ne sont pas compatibles avec le périphérique, leur utilisation entraîne des erreurs d'analyse et l'échec du processus syslog-ng.
- Vous pouvez configurer jusqu'à seize serveurs de journaux système. Cependant, en mode contexte multiple, la limitation est de 4 serveurs par contexte.
- Attribuez une seule liste ou classe à chaque serveur syslog et emplacement.
- Le serveur syslog doit être accessible au moyen de l'ASA. Vous devez configurer le périphérique pour refuser les messages ICMP unreachable (ICMP injoignable) sur l'interface par laquelle le serveur syslog est accessible et pour envoyer des journaux syslog au même serveur. Activez la journalisation pour tous les niveaux de gravité. Pour éviter que le serveur syslog ne se bloque, supprimez la génération des syslogs 313001, 313004 et 313005.
- Pour afficher les journaux générés par ASA, vous devez spécifier une destination de sortie de journalisation. Si vous activez la journalisation sans préciser de destination de sortie de journalisation, l'ASA génère des messages mais ne les enregistre pas à un emplacement à partir duquel vous pouvez les afficher. Vous devez spécifier chaque destination de sortie de journalisation séparément. Par exemple, pour désigner plusieurs serveurs syslog comme destination de sortie, et spécifiez des entrées distinctes dans le volet **Serveur Syslog** pour chaque serveur syslog.

- Pour une journalisation sécurisée, le Syslog Firewall Threat Defense prend en charge le protocole TLS unidirectionnel. Il ne prend pas en charge l'authentification par certificat client, la configuration de point de confiance pour syslog ou le protocole TLS mutuel (certificat X.509).
- Le certificat de serveur reçu d'un serveur Syslog doit contenir « ServAuth » dans le champ Extended Key Usage (Utilisation de la clé étendue). Cette vérification sera effectuée uniquement pour les certificats non autosignés. Les certificats autosignés ne fournissent aucune valeur dans ce champ.

Interfaces pour la configuration du journal système

- Détermination de l'interface de sortie (egress) pour le syslog :
  - Si l'interface de gestion uniquement indiquée a l'accès de gestion activé, le centre de gestion effectuera des recherches dans le tableau de routage et déterminera l'interface de sortie (peut être des données ou une gestion) en fonction de la meilleure logique de routage.
  - Si vous configurez une interface de gestion uniquement en tant qu'hôte de journalisation, qui n'a pas d'accès de gestion activé, le centre de gestion utilisera l'interface, quelles que soient les entrées de la table de routage.

    Ainsi, pour que le centre de gestion utilise toujours un chemin de gestion dédié pour le trafic syslog, configurez l'interface de gestion sans accès de gestion, puis précisez l'interface dans l'hôte de journalisation :

    ```
    interface <management-interface>
    management-only ----->Do not include management-access
    logging host <management-interface> <syslog-server-ip>
    ```

- Lorsque le débit syslog dépasse 50 000 messages par seconde, veillez à utiliser une interface de données comme interface de sortie plutôt qu'une interface de gestion.
- Lorsque vous utilisez une liste de messages personnalisée pour correspondre uniquement aux résultats de liste d'accès, les journaux de liste d'accès ne sont pas générés pour les listes dont le niveau de gravité de journalisation a été augmenté à débogage (niveau 7). Le niveau de gravité de la journalisation par défaut est défini à 6 pour la commande **logging list** (liste de journalisation). Ce comportement par défaut a été prévu. Lorsque vous modifiez explicitement le niveau de gravité de la journalisation de la configuration de la liste d'accès à Débogage, vous devez également modifier la configuration de journalisation elle-même.

  Voici un exemple de sortie de la commande **show running-config logging** qui n'inclut pas les résultats de la liste d'accès, car leur niveau de gravité de journalisation a été remplacé par « débogage » :

  ```
  ciscoasa# show running-config logging
  logging enable
  logging timestamp
  logging list test message 106100
  logging buffered test
  ```

  Voici un exemple de sortie de la commande **show running-config logging** qui inclut les résultats de la liste d'accès :

  ```
  ciscoasa# show running-config logging
  logging enable
  logging timestamp
  logging buffered debugging
  ```

Dans ce cas, la configuration de la liste d'accès ne change pas et le nombre d'occurrences de la liste d'accès s'affiche, comme le montre l'exemple suivant :

```
ciscoasa(config)# access-list global line 1 extended
permit icmp any host 4.2.2.2 log debugging interval 1 (hitcnt=7) 0xf36b5386
ciscoasa(config)# access-list global line 2 extended
permit tcp host 10.1.1.2 any eq www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
ciscoasa(config)# access-list global line 3 extended
permit ip any any (hitcnt=543) 0x25f9e609
```

Connexions TCP et UDP pour syslog

- L'envoi de journaux du système sur TCP n'est pas pris en charge sur un périphérique de secours.
- Si vous utilisez TCP comme protocole de transport, le système ouvre quatre connexions au serveur syslog pour s'assurer que les messages ne sont pas perdus. Si vous utilisez le serveur syslog pour collecter les messages d'un très grand nombre de périphériques et que le surdébit de la connexion combinée est trop important pour le serveur, utilisez plutôt UDP.
- Le nombre de connexions UDP pour syslog est directement lié au nombre de CPU sur la plateforme matérielle et au nombre de serveurs syslog que vous configurez. À tout moment, il peut y avoir autant de connexions syslog UDP qu'il y a de CPU multiplié par le nombre de serveurs syslog configurés. Notez que le délai d'inactivité de la connexion UDP globale s'applique à ces sessions et que la valeur par défaut est de 2 minutes. Vous pouvez ajuster ce paramètre si vous souhaitez fermer ces sessions plus rapidement, mais le délai d'expiration s'applique à toutes les connexions UDP, pas seulement au syslog. Il s'agi du comportement prévu.
- Lorsque ASA envoie des journaux système via TCP, la connexion prend environ une minute pour s'établir après le redémarrage du service syslogd.
- Lorsque l'hôte de journalisation TCP tombe en panne, il faut environ 6 minutes pour faire passer son état de connexion de *Connected* (Connecté) à *Not connected* (Non connecté). La journalisation s'appuie sur le TCP pour détecter l'état du canal; jusqu'à ce moment-là, la journalisation envoie les journaux par le canal. Pendant ce temps, lorsque vous exécutez **show log**, la sortie affiche l'hôte de journalisation TCP comme connecté. Une fois que le canal TCP est fermé, l'état de l'hôte de journalisation TCP est mis à jour à *Not connected* (Non connecté).

Configurer la journalisation

Cette section décrit comment configurer la journalisation.

Activer la journalisation

Pour activer la journalisation, procédez comme suit :

Procédure

Étape 1 Dans ASDM, choisissez l'une des options suivantes :

- **Home (Accueil)** > **Latest ASDM Syslog Messages (Derniers messages du journal système ASDM)** > **Enable Logging (Activer la journalisation)**
- **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Setup (Configuration de la journalisation)**
- **Monitoring (Supervision)** > **Real-Time Log Viewer (Visionneuse de journal en temps réel)** > **Enable Logging (Activer la journalisation)**
- **Monitoring (Supervision)** > **Log Buffer (Tampon de journal)** > **Enable Logging (Activer la journalisation)**

Étape 2 Cochez la case **Enable logging** (Activer la journalisation) pour activer la journalisation.

Configurer une destination de sortie

Pour optimiser l'utilisation des messages de journal système pour le dépannage et la surveillance des performances, nous vous conseillons de préciser un ou plusieurs emplacements où les messages de journal système doivent être envoyés, y compris un tampon de journal interne, un ou plusieurs serveurs de journal système externes, ASDM, une station de gestion SNMP, le port de console, des adresses courriel spécifiées ou des sessions Telnet et SSH.

Lorsque vous configurez la journalisation syslog sur une interface avec accès de gestion uniquement activé, les journaux liés au plan de données (ID du journal système 302015, 302014, 106023 et 304001) sont abandonnés et n'atteignent pas le serveur de journal système. Les messages du journal système sont abandonnés, car la table de routage du chemin d'accès ne dispose pas du routage de l'interface de gestion. Par conséquent, assurez-vous que l'accès réservé à la gestion est désactivé sur l'interface que vous configurez.

Envoyer des messages du journal système à un serveur externe de journal système

Vous pouvez archiver les messages en fonction de l'espace disque disponible sur le serveur de journal système externe et manipuler les données de journalisation après leur enregistrement. Par exemple, vous pouvez préciser les actions à exécuter lorsque certains types de messages Syslog sont enregistrés, extraire les données du journal et enregistrer les enregistrements dans un autre fichier pour créer des rapports ou suivre les statistiques à l'aide d'un script spécifique au site.

Pour envoyer des messages de journal système à un serveur de journal système externe, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Setup (Configuration de la journalisation)**.

Étape 2 Cochez la case **Enable logging** (Activer la journalisation) pour activer la journalisation pour l'ASA.

Étape 3 Cochez la case **Enable logging on the failover standby unit** (Activer la journalisation sur l'unité de secours de basculement) pour activer la journalisation de l'ASA de secours, si disponible.

Étape 4 Cochez la case **Send debug messages as syslogs** (Envoyer les messages de débogage sous forme de journaux système) pour rediriger toute la sortie de trace de débogage vers les journaux système. Le message du journal système ne s'affiche pas sur la console si cette option est activée. Par conséquent, pour afficher les messages

de débogage, vous devez activer la journalisation sur la console et la configurer comme destination pour le numéro de débogage et le niveau de gravité du message de journal système. Le numéro du message de journal système utilisé est **711001**. Le niveau de gravité par défaut pour ce message de journal système est le débogage.

Étape 5 Cochez la case **Send syslogs in EMBLEM format** (Envoyer les journaux système au format EMBLEM) pour activer le format EMBLEM afin qu'il soit utilisé pour toutes les destinations de journalisation, à l'exception des serveurs de journal système.

Étape 6 Spécifiez la taille du tampon de journal interne dans lequel les messages du journal système sont enregistrés si le tampon de journalisation est activé. Lorsque le tampon est plein, les messages sont remplacés, sauf si vous enregistrez les journaux sur un serveur FTP ou dans la mémoire flash interne. La taille du tampon par défaut est de 4096 octets. La plage va de 4096 à 1048576.

Étape 7 Pour enregistrer le contenu du tampon sur le serveur FTP avant qu'il ne soit remplacé, cochez la case **Save Buffer To FTP Server** (Enregistrer le tampon sur le serveur FTP). Pour autoriser le remplacement du contenu du tampon, décochez cette case.

Étape 8 Cliquez sur **Configure FTP Settings** (Configurer les paramètres FTP) pour identifier le serveur FTP et configurer les paramètres FTP utilisés pour enregistrer le contenu du tampon.

Étape 9 Cochez la case **Save Buffer To Flash** (Enregistrer le tampon dans la mémoire flash) pour enregistrer le contenu du tampon dans la mémoire flash interne avant de le remplacer.



Remarque Cette option est uniquement disponible en mode unique routé ou transparent.

Étape 10 Cliquez sur **Configure Flash Usage** (Configurer l'utilisation de la mémoire flash) pour préciser l'espace maximum à utiliser dans la mémoire flash interne pour la journalisation et l'espace libre minimum à préserver (en Ko). L'activation de cette option crée un répertoire appelé « journal système » sur le disque du périphérique sur lequel les messages sont stockés.



Remarque Cette option est uniquement disponible en mode routé ou transparent unique.

Étape 11 Spécifiez la taille de la file d'attente pour les journaux système qui doivent être consultés dans l'ASA.

Configurer les paramètres FTP

Pour spécifier la configuration du serveur FTP utilisé pour enregistrer le contenu du tampon du journal, procédez comme suit :

Procédure

Étape 1 Cochez la case **Enable FTP client** (Activer le client FTP) pour activer la configuration du client FTP.

Étape 2 Spécifiez l'adresse IP du serveur FTP.

Étape 3 Spécifiez le chemin d'accès au répertoire sur le serveur FTP pour stocker le contenu du tampon du journal enregistré.

Étape 4 Spécifiez le nom d'utilisateur pour vous connecter au serveur FTP.

Étape 5 Spécifiez le mot de passe associé au nom d'utilisateur pour vous connecter au serveur FTP.

Étape 6 Confirmez le mot de passe, puis cliquez sur **OK**.

Configurer l'utilisation de la mémoire flash de journalisation

Pour spécifier les limites d'enregistrement du contenu du tampon de journalisation dans la mémoire flash interne, procédez comme suit :

Procédure

Étape 1 Spécifiez la quantité maximum de mémoire flash interne pouvant être utilisée pour la journalisation (en Ko).

Étape 2 Spécifiez la quantité de mémoire flash interne conservée (en Ko). Lorsque la mémoire flash interne approche cette limite, les nouveaux journaux ne sont plus enregistrés.

Étape 3 Cliquez sur **OK** pour fermer la boîte de dialogue **Configure Logging Flash Usage** (Configurer l'utilisation de la mémoire flash de journalisation).

Activer la journalisation sécurisée

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Server (Serveur de journal système)**.

Étape 2 Sélectionnez un serveur de journal système pour lequel vous souhaitez activer la journalisation sécurisée, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Syslog Server** (Modifier le serveur de journal système) s'affiche.

Étape 3 Cliquez sur le bouton radio **TCP**.

La journalisation sécurisée ne prend pas en charge UDP; une erreur se produit si vous essayez d'utiliser ce protocole.

Étape 4 Cochez la case **Enable secure syslog with SSL/TLS** (Activer le journal système sécurisé avec SSL/TLS), puis cliquez sur **OK**.

Étape 5 (Facultatif) Spécifiez un objet **Reference Identity** (Identité de référence) par nom pour activer les vérifications d'identité de référence RFC 6125 sur le certificat reçu du serveur de journal système.

Consultez Configurer les identités de référence pour en savoir plus sur l'objet d'identité de référence.

Générer des messages du journal système en format EMBLEM vers un serveur de journal système

Pour générer des messages de journal système au format EMBLEM vers un serveur de journal système, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Server (Serveur de journal système)**.

L'envoi de jounaux système sur IPv6 est pris en charge.

Étape 2 Pour ajouter un nouveau serveur syslog, cliquez sur **Add** (Ajouter).

La boîte de dialogue **Add Syslog Server** (Ajouter un serveur de journal système) s'affiche.



Remarque Vous pouvez configurer un maximum de quatre serveurs de journal système par contexte de sécurité (jusqu'à un total de 16).

Étape 3 Spécifiez le nombre de messages qui peuvent être mis en file d'attente sur l'ASA lorsqu'un serveur de journal système est occupé. Une valeur zéro signifie qu'un nombre illimité de messages peuvent être mis en file d'attente.

Étape 4 Cochez la case **Allow user traffic to pass when TCP syslog server is down** (Autoriser le trafic à passer lorsque le serveur de journal système TCP est en panne) pour autoriser tout le trafic si un serveur de journal système est hors service.

Lorsque l'ASA est configuré pour envoyer des messages de journal système à un serveur de journal système connecté au TCP et si le serveur de journal système tombe en panne, en tant que protection de sécurité, les nouvelles connexions par l'ASA sont bloquées. Pour autoriser de nouvelles connexions, même lorsque le serveur de journal système n'est pas opérationnel, cochez cette case.

Si vous spécifiez UDP, l'ASA continue d'autoriser les nouvelles connexions, que le serveur de journal système soit opérationnel ou non. Les valeurs de port valides sont comprises entre 1025 et 65535, pour l'un ou l'autre de ces protocoles. Le port UDP par défaut est 514. Le port TCP par défaut est 1470.



Remarque L'envoi de journaux système sur TCP n'est pas pris en charge sur un ASA de secours.

Générer des messages du journal système en format EMBLEM vers d'autres destinations de sortie

Pour générer des messages de journal système au format EMBLEM vers d'autres destinations de sortie, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Setup (Configuration de la journalisation)**.

Étape 2 Cochez la case **Send syslogs in EMBLEM format** (Envoyer les journaux système au format EMBLEM).

Ajouter ou modifier les paramètres du serveur de journal système

Pour ajouter ou modifier les paramètres du serveur de journal système, procédez comme suit :

Procédure

Étape 1 Choisissez l'interface utilisée pour communiquer avec le serveur de journal système dans la liste déroulante.

Étape 2 Saisissez l'adresse IP utilisée pour communiquer avec le serveur de journal système.

Choisissez le protocole (TCP ou UDP) utilisé par le serveur de journal système pour communiquer avec l'ASA ou l'ASASM. Vous pouvez configurer l'ASA et l'ASASM pour envoyer des données à un serveur de journal système en utilisant UDP ou TCP. Le protocole par défaut est UDP si vous n'indiquez pas de protocole.

Avertissement Si vous spécifiez TCP, lorsque l'ASA détecte les défaillances du serveur de journal système, pour des raisons de sécurité, les nouvelles connexions par l'ASA sont bloquées. Pour autoriser de nouvelles connexions malgré les défaillances du serveur de journal système, consultez l'étape 4 de Générer des messages du journal système en format EMBLEM vers un serveur de journal système, à la page 14.

Étape 3 Saisissez le numéro de port utilisé par le serveur de journal système pour communiquer avec l'ASA ou l'ASASM.

Étape 4 Cochez la case **Log messages in Cisco EMBLEM format (UDP only)** (enregistrer les messages au format Cisco EMBLEM (UDP uniquement)) pour indiquer s'il faut consigner les messages au format Cisco EMBLEM (disponible uniquement si UDP est sélectionné comme protocole).

Étape 5 Cochez la case **Enable secure logging using SSL/TLS (TCP only)** (Activer la journalisation sécurisée à l'aide de SSL/TLS (TCP uniquement)) pour préciser que la connexion au serveur de journal système est sécurisée par l'utilisation de SSL/TLS sur TCP et que le contenu du message de journal système est chiffré. Vous pouvez éventuellement mentionner l'identité de référence pour valider le certificat en fonction de l'objet d'identité de référence précédemment configuré. Pour en savoir plus, consultez Activer la journalisation sécurisée, à la page 14.

Étape 6 Cliquez sur **OK** pour terminer la configuration.

Envoyer les messages du journal système au tampon du journal interne

Vous devez spécifier quels messages de journal système doivent être envoyés au tampon du journal interne, qui sert d'emplacement de stockage temporaire. Les nouveaux messages sont ajoutés à la fin de la liste. Lorsque le tampon est plein, c'est-à-dire lorsqu'il arrive à saturation, les anciens messages sont remplacés par de nouveaux messages, sauf si vous configurez l'ASA pour enregistrer le tampon complet à un autre emplacement.

Pour envoyer des messages de journal système au tampon du journal interne, procédez comme suit :

Procédure

Étape 1 Choisissez l'une des options suivantes pour spécifier quels messages de journal système doivent être envoyés au tampon du journal interne :

- **Home (Accueil)** > **Latest ASDM Syslog Messages (Derniers messages du journal système ASDM)** > **Configure ASDM Syslog Filters (Configurer les filtres du journal système ASDM)**
- **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**

Étape 2 Choisissez **Monitoring (Supervision)** > **Logging (Journalisation)** > **Log Buffer (Tampon de journal)** > **View (Afficher)**. Sélectionnez ensuite **File (Fichier)** > **Clear Internal Log Buffer (Effacer le tampon du journal interne)** dans le volet **Log Buffer** (Tampon du journal) pour vider le tampon du journal interne.

Étape 3 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Setup (Configuration de la journalisation)** pour changer la taille du tampon du journal interne. La taille du tampon par défaut est de 4 Ko.

Remarque Lorsque vous modifiez la taille du tampon de journalisation, les journaux existants dans le tampon sont purgés et un nouveau tampon est créé avec la taille nouvellement configurée.

L'ASA continue d'enregistrer les nouveaux messages dans le tampon du journal interne et d'enregistrer le contenu complet de ce tampon dans la mémoire flash interne. Lors de l'enregistrement du contenu du tampon à un autre emplacement, l'ASA crée des fichiers journaux avec des noms qui utilisent le format d'horodatage suivant :

```
LOG-YYYY-MM-DD-HHMMSS.TXT
```

où *AAAA* est l'année, *MM* est le mois, *JJ* est le jour du mois et *HHMMSS* est la durée en heures, minutes et secondes.

Étape 4 Pour enregistrer les nouveaux messages à un autre emplacement, choisissez l'une des options suivantes :

- Cochez la case **Flash** pour envoyer de nouveaux messages à la mémoire flash interne, puis cliquez sur **Configure Flash Usage** (Configurer l'utilisation de la mémoire flash). La boîte de dialogue **Configure Logging Flash Usage** (Configurer l'utilisation de la mémoire flash de journalisation) s'affiche.
  1. Spécifiez la quantité maximum de mémoire flash en Ko que vous souhaitez utiliser pour la journalisation.
  2. Spécifiez la quantité minimum d'espace libre en Ko que la journalisation conservera dans la mémoire flash.
  3. Cliquez sur **OK** pour fermer cette boîte de dialogue.
- Cochez la case **FTP Server** (Serveur FTP) pour envoyer de nouveaux messages à un serveur FTP, puis cliquez sur **Configure FTP Settings** (Configurer les paramètres FTP). La boîte de dialogue **Configure FTP Settings** (Configurer les paramètres FTP) s'affiche.

1. Cochez la case **Enable FTP Client** (Activer le client FTP).
2. Saisissez les renseignements suivants dans les champs fournis : adresse IP du serveur FTP, chemin d'accès, nom d'utilisateur et mot de passe.
3. Confirmez le mot de passe, puis cliquez sur **OK** pour fermer cette boîte de dialogue.

Enregistrer un tampon de journal interne dans la mémoire flash

Pour enregistrer le tampon de journal interne dans la mémoire flash, procédez comme suit :

Procédure

Étape 1 Choisissez **File (Fichier)** > **Save Internal Log Buffer to Flash (Enregistrer le tampon du journal interne dans la mémoire flash)**.

La boîte de dialogue **Enter Log File Name** (Saisir le nom du fichier journal) apparaît.

Étape 2 Choisissez la première option pour enregistrer le tampon du journal avec le nom de fichier par défaut, LOG-YYYY-MM-DD-hhmmss.txt.

Étape 3 Choisissez la deuxième option pour spécifier un nom de fichier pour le tampon du journal.

Étape 4 Saisissez le nom de fichier du tampon du journal, puis cliquez sur **OK**.

Modifier la quantité de mémoire flash interne disponible pour les journaux

Pour modifier la quantité de mémoire flash interne disponible pour les journaux, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Setup (Configuration de la journalisation)**.

Étape 2 Cochez la case **Enable Logging** (Activer la journalisation).

Étape 3 Cochez la case **Save Buffer to Flash** (Enregistrer le tampon dans la mémoire flash) dans la zone **Logging to Internal Buffer** (Journaliser dans le tampon interne).

Étape 4 Cliquez sur **Configure Flash Usage** (Configurer l'utilisation de la mémoire flash).

La boîte de dialogue **Configure Logging Flash Usage** (Configurer l'utilisation de la mémoire flash de journalisation) s'affiche.

Étape 5 Saisissez la quantité maximum de mémoire flash en Ko autorisée pour la journalisation.

Par défaut, l'ASA peut utiliser jusqu'à 50 Mo de mémoire flash interne pour les données des journaux. La quantité minimum de mémoire flash interne qui doit être libre pour que l'ASA enregistre les données du journal est de 3 Mo. Si un fichier journal enregistré dans la mémoire flash interne entraîne une diminution de l'espace libre dans la mémoire flash interne en dessous de la limite minimum configurée, l'ASA supprime les fichiers journaux les plus anciens afin de garantir qu'il reste suffisamment d'espace libre après

l'enregistrement du nouveau fichier journal. S'il n'y a aucun fichier à supprimer ou si, après la suppression de tous les anciens fichiers, la mémoire libre reste inférieure à la limite, l'ASA ne parvient pas à enregistrer le nouveau fichier journal. La limite maximum de la valeur flash-maximum-allocation est de 2 Go.

Étape 6 Saisissez la quantité minimum d'espace libre en Ko à conserver pour la journalisation dans la mémoire flash.

Étape 7 Cliquez sur **OK** pour fermer la boîte de dialogue **Configure Logging Flash Usage** (Configurer l'utilisation de la mémoire flash de journalisation).

Afficher et copier les entrées enregistrées avec la console Java ASDM

Utilisez la console Java ASDM pour afficher et copier les entrées enregistrées dans un format texte, ce qui peut vous aider à résoudre les erreurs ASDM.

Pour accéder à la console Java ASDM, procédez comme suit :

Procédure

Étape 1 Choisissez **Tools (Outils)** > **ASDM Java Console (Console Java ASDM)**.

Étape 2 Saisissez **m** dans la console pour afficher les statistiques de mémoire de la machine virtuelle.

Étape 3 Saisissez **g** dans la console pour effectuer la collecte des ordures.

Étape 4 Ouvrez le gestionnaire de tâches de Windows et cliquez deux fois sur le fichier **asdm_launcher.exe** pour superviser l'utilisation de la mémoire.

Remarque L'allocation de mémoire maximale autorisée est de 256 Mo.

Envoyer des messages Syslog à une adresse courriel

Pour envoyer des messages de journal système à une adresse courriel, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **E-Mail Setup (Configuration du courriel)**.

Étape 2 Spécifiez l'adresse de courriel utilisée comme adresse source pour les messages syslog envoyés comme courriels.

Étape 3 Cliquez sur **Add** (ajouter) pour saisir la nouvelle adresse de courriel des messages syslog précisés.

Étape 4 Choisissez le niveau de gravité des messages syslog qui sont envoyés au destinataire dans la liste déroulante. Le filtre de gravité des messages syslog utilisé pour l'adresse de courriel de destination entraîne l'envoi des messages du niveau de gravité spécifié et du niveau supérieur. Le filtre global spécifié dans le volet **Logging Filters** (Filtres de journalisation) est également appliqué à chaque destinataire de courriel.

Étape 5 Cliquez sur **Edit** (Modifier) pour modifier un niveau de gravité existant des messages de journal système envoyés à ce destinataire.

Étape 6 Cliquez sur **OK** pour fermer la boîte de dialogue **Add E-mail Recipient** (Ajouter un destinataire de courriel).

Ajouter ou modifier des destinataires de courriel

Pour ajouter ou modifier des destinataires de courriels et des niveaux de gravité, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **E-mail Setup (Configuration du courriel)**.

Étape 2 Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) pour afficher la boîte de dialogue **Add/Edit E-Mail Recipient** (Ajouter/modifier le destinataire de courriel).

Étape 3 Saisissez l'adresse courriel de destination et choisissez le niveau de gravité du journal système dans la liste déroulante. Les niveaux de gravité sont définis comme suit :

- Urgence (niveau 0, système inutilisable)

Remarque Il est déconseillé d'utiliser le niveau de gravité zéro.

- Alerte (niveau 1, action immédiate requise)
- Critique (niveau 2, conditions critiques)
- Erreur (niveau 3, conditions d'erreur)
- Avertissement (niveau 4, conditions d'avertissement)
- Notification (niveau 5, conditions normales mais significatives)
- Information (niveau 6, messages d'information uniquement)
- Débogage (niveau 7, messages de débogage uniquement)

Remarque Le niveau de gravité utilisé pour filtrer les messages de l'adresse courriel de destination est le plus élevé entre le niveau de gravité spécifié dans la boîte de dialogue **Add/Edit E-Mail Recipient** (Ajouter/modifier le destinataire de courriel) et le filtre global défini pour tous les destinataires de courriel dans le volet **Logging Filters** (Filtres de journalisation).

Étape 4 Cliquez sur **OK** pour fermer la boîte de dialogue **Add/Edit E-Mail Recipient** (Ajouter/modifier le destinataire de courriel).

L'entrée ajoutée ou révisée apparaît dans le volet **E-mail Recipients** (Destinataires de courriels).

Étape 5 Cliquez sur **Apply** (Appliquer) pour enregistrer vos modifications dans la configuration en cours d'exécution.

Configurer le serveur SMTP distant

Pour configurer le serveur SMTP distant auquel les alertes et les notifications par courriel sont envoyées en réponse à des événements spécifiques, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Logging (Journalisation)** > **SMTP**.

Étape 2 Saisissez l'adresse IP du serveur SMTP principal.

Étape 3 (Facultatif) Saisissez l'adresse IP du serveur SMTP de secours, puis cliquez sur **Apply** (Appliquer) pour enregistrer vos modifications dans la configuration en cours d'exécution.

Envoyer les messages du journal système au port de console

Pour envoyer des messages de journal système au port de console, procédez comme suit :

Procédure

Étape 1 Choisissez une des options suivantes :

- **Home (Accueil)** > **Latest ASDM Syslog Messages (Derniers messages du journal système ASDM)** > **Configure ASDM Syslog Filters (Configurer les filtres du journal système ASDM)**
- **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**

Étape 2 Sélectionnez la console dans la colonne **Logging Destination** (Destination de journalisation), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Logging Filters** (Modifier les filtres de journalisation) s'affiche.

Étape 3 Choisissez des journaux système de toutes les classes d'événements ou des journaux système de classes d'événements spécifiques pour spécifier quels messages de journal système doivent être envoyés au port de console.

Envoyer les messages du journal système à une session Telnet ou SSH

Pour envoyer des messages de journal système à une session Telnet ou SSH, procédez comme suit :

Procédure

Étape 1 Choisissez une des options suivantes :

- **Home (Accueil)** > **Latest ASDM Syslog Messages (Derniers messages du journal système ASDM)** > **Configure ASDM Syslog Filters (Configurer les filtres du journal système ASDM)**
- **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**

Étape 2 Sélectionnez les options **Telnet** et **SSH Sessions** (Sessions SSH) dans la colonne **Logging Destination** (Destination de journalisation), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Logging Filters** (Modifier les filtres de journalisation) s'affiche.

Étape 3 Choisissez des journaux système de toutes les classes d'événements ou des journaux système de classes d'événements spécifiques pour spécifier quels messages de journal système doivent être envoyés à une session Telnet ou SSH.

Étape 4 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Setup (Configuration de la journalisation)** pour activer la journalisation pour la session en cours uniquement.

Étape 5 Cochez la case **Enable logging** (Activer la journalisation), puis cliquez sur **Apply** (Appliquer).

Configurer les messages du journal système

Configurer la messagerie du journal système

Pour configurer la messagerie du journal système, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Setup (Configuration du journal système)**.

Étape 2 Choisissez une fonction de journalisation du système que les serveurs Syslog doivent utiliser comme base pour classer les messages. La valeur par défaut est LOCAL(4)20, ce qui est attendu de la plupart des systèmes UNIX. Cependant, comme vos périphériques réseau partagent huit installations disponibles, vous devrez peut-être modifier cette valeur pour les journaux système.

Étape 3 Cochez la case **Include timestamp in syslogs** (Inclure l'horodatage dans les journaux système) pour ajouter la date et l'heure dans chaque message de journal système envoyé.

Utilisez la liste déroulante **Timestamp Format** (Format d'horodatage) pour sélectionner le format existant (mm:dd:yyyy hh:mm:ss) ou RFC 5424 (yyyy:dd:mmTHH:mm:ssZ).

Étape 4 Décochez la case **Hide username if its validity cannot be determined** (Masquer le nom d'utilisateur si sa validité ne peut pas être déterminée) pour afficher les noms d'utilisateur non valides dans les messages du journal système en cas de tentatives de connexion infructueuses. Le paramètre par défaut consiste à masquer

les noms d'utilisateur lorsque le nom d'utilisateur est non valide ou si la validité est inconnue. Si un utilisateur saisit accidentellement un mot de passe au lieu d'un nom d'utilisateur, par exemple, il est plus sûr de masquer le « nom d'utilisateur » dans le message du journal système résultant. Vous souhaiterez peut-être afficher les noms d'utilisateur non valides pour résoudre les problèmes de connexion.

Étape 5 Choisissez les renseignements à afficher dans le tableau **Syslog ID** (ID de journal système). Les options disponibles sont les suivantes :

- Choisissez **Show all syslog IDs** (Afficher tous les ID du journal système) pour spécifier que le tableau **Syslog ID** (ID du journal système) doit afficher la liste complète des ID des messages du journal système.
- Choisissez **Show disabled syslog IDs** (Afficher les ID de journal système) pour spécifier que le tableau **Syslog ID** (ID de journal système) ne doit afficher que les ID des messages de journal système qui ont été désactivés explicitement.
- Choisissez **Show syslog IDs with changed logging** (Afficher les ID de journal système avec la journalisation modifiée) pour spécifier que le tableau **Syslog ID** (ID de journal système) ne doit afficher que les ID des messages de journal système avec les niveaux de gravité qui ont changé par rapport à leurs valeurs par défaut.
- Choisissez **Show syslog IDs that are disabled or with a changed logging level** (Afficher les ID qui sont désactivés ou avec un niveau de journalisation modifié) pour préciser que le tableau **Syslog ID** (ID de journal système) ne doit afficher que les ID des messages de journal système avec les niveaux de gravité qui ont été modifiés et les ID des messages de journal système qui ont été explicitement désactivés.

Étape 6 Le **Syslog ID Setup Table** (Tableau de configuration d'ID de journal système) affiche la liste des messages de journal système en fonction des paramètres du tableau de configuration d'ID de journal système. Choisissez des messages individuels ou des plages d'ID de message que vous souhaitez modifier. Vous pouvez soit désactiver les ID des messages sélectionnés, soit modifier leurs niveaux de gravité. Pour sélectionner plusieurs ID de message dans la liste, cliquez sur le premier ID de la plage et à l'aide de la touche Maj, cliquez sur le dernier ID de la plage.

Étape 7 Cliquez sur **Advanced** (Avancé) pour configurer les messages du journal système afin d'inclure un ID de périphérique.

Modifier les paramètres d'ID du journal système

Pour modifier les paramètres des messages du journal système, procédez comme suit :



Remarque Le champ **Syslog ID(s)** (ID(s) du journal système) est en lecture seule. Les valeurs qui apparaissent dans cette zone sont déterminées par les entrées que vous avez choisies dans le tableau **Syslog ID** (ID de journal système), situé dans le volet **Syslog Setup** (Configuration du journal système).

Procédure

Étape 1 Cochez la case **Disable Message(s)** (Désactiver le(s) message(s)) pour désactiver les messages correspondant aux ID des messages du journal système affichés dans la liste **Syslog ID(s)** (ID(s) du journal système).

Étape 2 Choisissez le niveau de gravité des messages à envoyer pour les ID des messages du journal système affichés dans la liste **Syslog ID(s)** (ID(s) du journal système). Les niveaux de gravité sont définis comme suit :

- Urgence (niveau 0, système inutilisable)

Remarque Il est déconseillé d'utiliser le niveau de gravité zéro.

- Alerte (niveau 1, action immédiate requise)
- Critique (niveau 2, conditions critiques)
- Erreur (niveau 3, conditions d'erreur)
- Avertissement (niveau 4, conditions d'avertissement)
- Notification (niveau 5, conditions normales mais significatives)
- Information (niveau 6, messages d'information uniquement)
- Débogage (niveau 7, messages de débogage uniquement)

Étape 3 Cliquez sur **OK** pour fermer la boîte de dialogue **Edit Syslog ID Settings** (Modifier les paramètres d'ID de journal système).

Inclure un ID de périphérique dans les messages du journal système au format non EMBLEM

Pour inclure un ID de périphérique dans les messages du journal système au format non EMBLEM, procédez comme suit :

Procédure

Étape 1 Cochez la case **Enable syslog device ID** (Activer l'ID de périphérique du journal système) pour préciser qu'un ID de périphérique doit être inclus dans tous les messages de journal système au format non EMBLEM.

Étape 2 Pour préciser lequel utiliser comme identifiant de périphérique, choisissez l'une des options suivantes :

- Nom de domaine de l'ASA
- Adresse IP de l'interface

  Choisissez le nom d'interface qui correspond à l'adresse IP sélectionnée dans la liste déroulante.

  Cochez la case **In an ASA cluster, always use control's IP address for the selected interface** (Dans une grappe ASA, toujours utiliser l'adresse IP du contrôle pour l'interface sélectionnée) si vous utilisez la mise en grappe.

- Chaîne

  Spécifiez une chaîne alphanumérique définie par l'utilisateur.

- Nom de la grappe ASA

Étape 3 Cliquez sur **OK** pour fermer la boîte de dialogue **Advanced Syslog Configuration** (Configuration du journal système avancée).

Inclure la date et l'heure dans les messages du journal système

Pour inclure la date et l'heure dans les messages du journal système, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Setup (Configuration du journal système)**.

Étape 2 Cochez la case **Include timestamp in syslogs** (Inclure l'horodatage dans les journaux système) dans la zone **Syslog ID Setup** (Configuration de l'ID du journal système).

Étape 3 Cliquez sur **Apply** pour enregistrer vos modifications.

Désactiver un message du journal système

Pour désactiver un message du journal système spécifié, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Setup (Configuration du journal système)**.

Étape 2 Sélectionnez le journal système que vous souhaitez désactiver dans le tableau, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Syslog ID Settings** (Modifier les paramètres d'ID du journal système) s'affiche.

Étape 3 Cochez la case **Disable messages** (Désactiver les messages), puis cliquez sur **OK**.

Modifier le niveau de gravité d'un message du journal système

Pour modifier le niveau de gravité d'un message du journal système, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Setup (Configuration du journal système)**.

Étape 2 Sélectionnez le journal système dont vous souhaitez modifier le niveau de gravité dans le tableau, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Syslog ID Settings** (Modifier les paramètres d'ID du journal système) s'affiche.

Étape 3 Choisissez le niveau de gravité souhaité dans la liste déroulante **Logging Level** (Niveau de journalisation), puis cliquez sur **OK**.

Bloquer les messages du journal système sur une unité de secours

Pour bloquer la génération de messages de journal système spécifiques sur une unité de secours, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Settings (Paramètres du journal système)**.

Étape 2 Choisissez un ID de journal système dans le tableau, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Syslog ID Settings** (Modifier les paramètres d'ID du journal système) s'affiche.

Étape 3 Cochez la case **Disable messages on standby unit** (Désactiver les messages sur l'unité en veille) pour empêcher la génération des messages du journal système sur une unité en veille.

Étape 4 Cliquez sur **OK** pour fermer cette boîte de dialogue.

Inclure l'ID de périphérique dans les messages du journal système au format non EMBLEM

Pour inclure l'ID de périphérique dans les messages du journal système au format non EMBLEM, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Setup (Configuration du journal système)** > **Advanced (Avancé)** > **Advanced Syslog Configuration (Configuration du journal système avancée).**

Étape 2 Cochez la case **Enable syslog device ID** (Activer l'ID de périphérique de journal système).

Étape 3 Cliquez sur le bouton radio **Hostname** (Nom d'hôte), **Interface IP Address** (Adresse IP de l'interface) ou **String** (Chaîne) dans la zone **Device ID** (ID de périphérique).

- Si vous avez choisi l'option **Interface IP Address** (Adresse IP de l'interface), assurez-vous que la bonne interface est sélectionnée dans la liste déroulante.
- Si vous avez choisi l'option **String** (Chaîne), saisissez l'ID de périphérique dans le champ **User-Defined ID** (ID défini par l'utilisateur). La chaîne peut inclure jusqu'à 16 caractères.



Remarque Si cette option est activée, l'ID de périphérique n'apparaît pas dans les messages de journal système au format EMBLEM ni dans les alertes SNMP.

Étape 4 Cliquez sur **OK** pour fermer la boîte de dialogue **Advanced Syslog Configuration** (Configuration du journal système avancée).

Créer une liste d'événements personnalisée

Vous utilisez les trois critères suivants pour définir une liste d'événements :

- Classe d'événement
- Gravité
- ID du message

Pour créer une liste d'événements personnalisé à envoyer à une destination de journalisation spécifique (par exemple, un serveur SNMP), procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Event Lists (Listes d'événements)**.

Étape 2 Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Event List** (Ajouter une liste d'événements).

Étape 3 Saisissez le nom de la liste d'événements. Aucun espace n'est autorisé.

Étape 4 Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Class and Severity Filter** (Ajouter un filtre de classe et de gravité).

Étape 5 Dans la liste déroulante, choisissez la classe d'événement. Les classes d'événements disponibles varient en fonction du mode de périphérique que vous utilisez.

Étape 6 Choisissez le niveau de gravité dans la liste déroulante. Les niveaux de gravité sont les suivants :

- Urgence (niveau 0, système inutilisable)

Remarque Il est déconseillé d'utiliser le niveau de gravité zéro.

- Alerte (niveau 1, action immédiate requise)
- Critique (niveau 2, conditions critiques)
- Erreur (niveau 3, conditions d'erreur)
- Avertissement (niveau 4, conditions d'avertissement)
- Notification (niveau 5, conditions normales mais significatives)
- Information (niveau 6, messages d'information uniquement)
- Débogage (niveau 7, messages de débogage uniquement)

Étape 7 Cliquez sur **OK** pour fermer la boîte de dialogue **Add Event List** (Ajouter une liste d'événements).

Étape 8 Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Syslog Message ID Filter** (Ajouter un filtre d'ID de message du journal système).

Étape 9 Saisissez un ID de message du journal système ou une plage d'ID (par exemple, 101001-199012) à inclure dans le filtre.

Étape 10 Cliquez sur **OK** pour fermer la boîte de dialogue **Add Event List** (Ajouter une liste d'événements).

L'événement d'intérêt apparaît dans la liste.

Configurer les filtres de journalisation

Appliquer des filtres de message à une destination de journalisation

Pour appliquer des filtres de message à une destination de journalisation, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**.

Étape 2 Choisissez le nom de la destination de journalisation à laquelle vous souhaitez appliquer un filtre. Les destinations de journalisation disponibles sont les suivantes :

- ASDM
- Port de console
- Courriel
- Tampon interne
- Serveur de SNMP
- Serveur journal système
- Session Telnet ou SSH

Cette sélection comprend la deuxième colonne, Journaux système de toutes les classes d'événements, et la troisième colonne, Journaux système de classes d'événements spécifiques. La deuxième colonne répertorie la gravité ou la classe d'événements à utiliser pour filtrer les messages pour la destination de journalisation, ou si la journalisation est désactivée pour toutes les classes d'événements. La troisième colonne répertorie la classe d'événements à utiliser pour filtrer les messages pour cette destination de journalisation.

Étape 3 Cliquez sur **Edit** (Modifier) pour afficher la boîte de dialogue **Edit Logging Filters** (Modifier les filtres de journalisation). Pour appliquer, modifier ou désactiver les filtres, consultez Appliquer des filtres de journalisation, à la page 29.

Appliquer des filtres de journalisation

Pour appliquer des filtres, procédez comme suit :

Procédure

Étape 1 Choisissez l'option **Filter on severity** (Filtrer par gravité) pour filtrer les messages du journal système en fonction de leur niveau de gravité.

Étape 2 Choisissez l'option **Use event list** (Utiliser la liste d'événements) pour filtrer les messages du journal système en fonction d'une liste d'événements.

Étape 3 Choisissez l'option **Disable logging from all event classes** (Désactiver la journalisation de toutes les classes d'événements) pour désactiver toute la journalisation vers la destination sélectionnée.

Étape 4 Cliquez sur **New** (Nouveau) pour ajouter une nouvelle liste d'événements. Pour ajouter une nouvelle liste d'événements, consultez Créer une liste d'événements personnalisée, à la page 27.

Étape 5 Dans la liste déroulante, choisissez la classe d'événement. Les classes d'événements disponibles varient en fonction du mode de périphérique que vous utilisez.

Étape 6 Choisissez le niveau de journalisation des messages dans la liste déroulante. Les niveaux de gravité sont les suivants :

- Urgence (niveau 0, système inutilisable)

Remarque Il est déconseillé d'utiliser le niveau de gravité zéro.

- Alerte (niveau 1, action immédiate requise)
- Critique (niveau 2, conditions critiques)
- Erreur (niveau 3, conditions d'erreur)
- Avertissement (niveau 4, conditions d'avertissement)
- Notification (niveau 5, conditions normales mais significatives)
- Information (niveau 6, messages d'information uniquement)
- Débogage (niveau 7, messages de débogage uniquement)

Étape 7 Cliquez sur **Add** (Ajouter) pour ajouter la classe d'événement et le niveau de gravité, puis cliquez sur **OK**.

La destination de journalisation sélectionnée pour un filtre s'affiche en haut.

Ajouter ou modifier un filtre d'ID de message du journal système

Pour ajouter ou modifier un filtre d'ID de message du journal système, consultez Modifier les paramètres d'ID du journal système, à la page 23.

Ajouter ou modifier un filtre de classe de message et de gravité

Pour ajouter ou modifier une classe de messages et un niveau de gravité pour le filtrage des messages, procédez comme suit :

Procédure

Étape 1 Dans la liste déroulante, choisissez la classe d'événement. Les classes d'événements disponibles varient en fonction du mode de périphérique que vous utilisez.

Étape 2 Choisissez le niveau de journalisation des messages dans la liste déroulante. Les niveaux de gravité sont les suivants :

- Urgence (niveau 0, système inutilisable)

Remarque Il est déconseillé d'utiliser le niveau de gravité zéro.

- Alerte (niveau 1, action immédiate requise)
- Critique (niveau 2, conditions critiques)
- Erreur (niveau 3, conditions d'erreur)
- Avertissement (niveau 4, conditions d'avertissement)
- Notification (niveau 5, conditions normales mais significatives)
- Information (niveau 6, messages d'information uniquement)
- Débogage (niveau 7, messages de débogage uniquement)

Étape 3 Cliquez sur **OK** lorsque vous avez terminé vos sélections.

Envoyer tous les messages du journal système d'une classe vers une destination de sortie spécifiée

Pour envoyer tous les messages du journal système d'une classe vers une destination de sortie spécifiée, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**.

Étape 2 Pour remplacer la configuration dans la destination de sortie spécifiée, choisissez la destination de sortie que vous souhaitez modifier, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Logging Filters** (Modifier les filtres de journalisation) s'affiche.

Étape 3 Révisez les paramètres dans la zone **Syslogs from All Event Classes** (Journaux système de toutes les classes d'événements) ou **Syslogs from Specific Event Classes** (Journaux système de classes d'événements spécifiques), puis cliquez sur **OK** pour fermer cette boîte de dialogue.

Par exemple, si vous précisez que les messages de niveau de gravité 7 doivent être envoyés au tampon de journal interne et que les messages de classe ha de niveau de gravité 3 doivent être envoyés au tampon de journal interne, la dernière configuration prévaut.

Pour spécifier qu'une classe doit être envoyée à plusieurs destinations, sélectionnez une option de filtrage différente pour chaque destination de sortie.

Limiter le débit de génération des messages Syslog

Pour limiter le débit de génération des messages du journal système, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Rate Limit (Limite de débit)**.

Étape 2 Choisissez le niveau de journalisation (niveau de gravité du message) auquel vous souhaitez attribuer des limites de débit. Les niveaux de gravité sont définis comme suit :

- Urgence (niveau 0, système inutilisable)
- Alerte (niveau 1, action immédiate requise)
- Critique (niveau 2, conditions critiques)
- Erreur (niveau 3, conditions d'erreur)
- Avertissement (niveau 4, conditions d'avertissement)
- Notification (niveau 5, conditions normales mais significatives)
- Information (niveau 6, messages d'information uniquement)
- Débogage (niveau 7, messages de débogage uniquement)

Étape 3 Le champ **No of Messages** (Nombre de messages) affiche le nombre de messages envoyés. Le champ **Interval (Seconds)** (Intervalle (secondes)) affiche l'intervalle, en secondes, utilisé pour limiter le nombre de messages qui peuvent être envoyés à ce niveau de journalisation. Choisissez un niveau de journalisation dans le tableau et cliquez sur **Edit** (Modifier) pour afficher la boîte de dialogue **Edit Rate Limit for Syslog Logging Level** (Modifier la limite de débit pour le niveau de journalisation système).

Étape 4 Pour continuer, consultez Attribuer ou modifier des limites de débit pour les messages du journal système individuels, à la page 32.

Attribuer ou modifier des limites de débit pour les messages du journal système individuels

Pour affecter ou modifier des limites de débit à des messages de journal système individuels, procédez comme suit :

Procédure

Étape 1 Pour attribuer la limite de débit d'un message de journal système spécifique, cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Rate Limit for Syslog Message** (Ajouter une limite de débit pour le message de journal système).

Étape 2 Pour continuer, consultez Ajouter ou modifier la limite de débit pour un message du journal système, à la page 32.

Étape 3 Pour modifier la limite de débit d'un message de journal système spécifique, cliquez sur **Edit** (Modifier) pour afficher la boîte de dialogue **Edit Rate Limit for Syslog Message** (Modifier la limite de débit pour le message de journal système).

Étape 4 Pour continuer, consultez Modifier la limite de débit pour un niveau de gravité du journal système, à la page 32.

Ajouter ou modifier la limite de débit pour un message du journal système

Pour ajouter ou modifier la limite de débit pour un message de journal système donné, procédez comme suit :

Procédure

Étape 1 Pour ajouter une limite de débit à un message de journal système spécifique, cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Rate Limit for Syslog Message** (Ajouter une limite de débit pour le message de journal système). Pour modifier une limite de débit pour un message de journal système, cliquez sur **Edit** (Modifier) pour afficher la boîte de dialogue **Edit Rate Limit for Syslog Message** (Modifier la limite de débit pour le message de journal système).

Étape 2 Saisissez l'ID de message du journal système que vous souhaitez limiter.

Étape 3 Saisissez le nombre maximum de messages pouvant être envoyés dans l'intervalle de temps spécifié.

Étape 4 Saisissez la durée, en secondes, utilisée pour limiter le débit du message spécifié, puis cliquez sur **OK**.

Remarque Pour autoriser un nombre illimité de messages, laissez les champs **Number of Messages** (Nombre de messages) et **Time Interval** (Intervalle de temps) vides.

Modifier la limite de débit pour un niveau de gravité du journal système

Pour modifier la limite de débit d'un niveau de gravité du journal système spécifié, procédez comme suit :

Procédure

Étape 1 Saisissez le nombre maximum de messages à ce niveau de gravité qui peuvent être envoyés.

Étape 2 Saisissez la durée, en secondes, utilisée pour limiter le débit de messages à ce niveau de gravité, puis cliquez sur **OK**.

Le niveau de gravité des messages sélectionné s'affiche.

Remarque Pour autoriser un nombre illimité de messages, laissez les champs **Number of Messages** (Nombre de messages) et **Time Interval** (Intervalle de temps) vides.

Attribuer ou modifier des limites de débit pour la journalisation dynamique

Vous pouvez attribuer des limites de débit pour la journalisation en fonction des ressources utilisées (taille des blocs). En spécifiant une valeur de seuil (pourcentage), le débit de génération des messages du journal système est limité. Vous pouvez également définir le nombre de messages pouvant être générés lorsque l'utilisation de la taille des blocs dépasse la valeur du seuil.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Rate Limit (Limite de débit)**.

Étape 2 Sous **Rate Limits for Dynamic Logging** (Limites de débit pour la journalisation dynamique), précisez les éléments suivants :

- **Block** (Bloc) : indiquez le pourcentage de blocs libres qui servent de seuil pour déclencher la limitation dynamique du débit.
- **Message Limit (Limite de messages)** : indiquez le nombre de messages autorisés pour la limite dynamique. La valeur par défaut est 10.

Étape 3 Cliquez sur **Apply** (Appliquer).

Étape 4 Pour modifier les valeurs enregistrées, saisissez les nouvelles valeurs, puis cliquez sur **Apply** (Appliquer).

Étape 5 Pour désactiver la limite de débit de journalisation dynamique, laissez les champs vides.

Supervision des journaux

Consultez les commandes suivantes pour superviser l'état de la journalisation.

- **Monitoring (Supervision)** > **Logging (Journalisation)** > **Log Buffer (Tampon de journal)** > **View (Afficher)**

  Ce volet vous permet d'afficher le tampon du journal.

- **Monitoring (Supervision)** > **Logging (Journalisation)** > **Real-Time Log Viewer (Visionneuse de journal en temps réel)** > **View (Afficher)**

  Ce volet vous permet d'afficher le journal en temps réel.

- **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**

  Ce volet vous permet d'exécuter diverses commandes non interactives et d'afficher les résultats.

- **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Critères d'accès)**

  Ce volet vous permet de filtrer la visionneuse en direct de la journalisation de ces journaux en fonction des critères de recherche (ID hexadécimal de la règle). Pour afficher les résultats, sélectionnez la règle et cliquez sur **Show Log** (Afficher le journal).

Filtrer les messages du journal système à l'aide des visionneuses de journaux

Vous pouvez filtrer les messages du journal système en fonction d'une ou plusieurs valeurs correspondant à n'importe quelle colonne de la visionneuse de journal en temps réel et de la visionneuse de tampon de journal.

Pour filtrer les messages du journal système dans l'une des visionneuses de journaux, procédez comme suit :

Procédure

Étape 1 Choisissez une des options suivantes :

- **Monitoring (Supervision)** > **Logging (Journalisation)** > **Real-Time Log Viewer (Visionneuse de journal en temps réel)** > **View (Afficher)**
- **Monitoring (Supervision)** > **Logging (Journalisation)** > **Log Buffer (Tampon de journal)** > **View (Afficher)**

Étape 2 Dans la boîte de dialogue **Real-Time Log Viewer** (Visionneuse de journal en temps réel) ou **Log Buffer Viewer** (Visionneuse de tampon de journal), cliquez sur **Build Filter** (Créer un filtre) dans la barre d'outils.

Étape 3 Dans la boîte de dialogue **Build Filter** (Créer un filtre), spécifiez les critères de filtrage à appliquer aux messages du journal système :

a) Choisissez l'une des trois options suivantes dans la zone **Date and Time** (Date et heure) : en temps réel, heure précise ou plage horaire. Si vous avez choisi une heure précise, indiquez l'heure en saisissant le nombre et en choisissant les heures ou les minutes dans la liste déroulante. Si vous avez choisi une plage horaire, cliquez sur la flèche de la liste déroulante dans le champ **Start Time** (Heure de début) pour afficher un calendrier. Choisissez une date et une heure de début dans la liste déroulante, puis cliquez sur **OK**. Cliquez sur la flèche de la liste déroulante dans le champ **End Time** (Heure de fin) pour afficher un calendrier. Choisissez une date et une heure de fin dans la liste déroulante, puis cliquez sur **OK**.

b) Saisissez un niveau de gravité valide dans le champ **Severity** (Gravité). Vous pouvez également cliquer sur l'icône **Edit** (Modifier) à droite du champ **Severity** (Gravité). Cliquez sur les niveaux de gravité dans la liste que vous souhaitez filtrer. Pour inclure les niveaux de gravité 1 à 7, cliquez sur **All** (Tous). Cliquez sur **OK** pour afficher ces paramètres dans la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur

l'icône **Info** à droite du champ **Severity** (Gravité) pour obtenir des renseignements supplémentaires sur le format d'entrée à utiliser.

c) Saisissez un ID de journal système valide dans le champ **Syslog ID** (ID de journal système). Vous pouvez également cliquer sur l'icône **Edit** (Modifier) à droite du champ **Syslog ID** (ID de journal système). Choisissez une condition de filtrage dans la liste déroulante, puis cliquez sur **Add** (Ajouter). Cliquez sur **OK** pour afficher ces paramètres dans la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur l'icône **Info** à droite du champ **Syslog ID** (ID de journal système) pour obtenir des renseignements supplémentaires sur le format d'entrée à utiliser.

d) Saisissez une adresse IP source valide dans le champ **Source IP Address** (Adresse IP source), ou cliquez sur l'icône **Edit** (Modifier) à droite du champ **Source IP Address** (Adresse IP source). Choisissez une adresse IP unique ou une plage spécifiée d'adresses IP, puis cliquez sur **Add** (Ajouter). Cochez la case **Do not include (exclude) this address or range** (Ne pas inclure (exclure) cette adresse ou cette plage) pour exclure une adresse IP ou une plage d'adresses IP spécifiques, cliquez sur **OK** pour afficher ces paramètres dans la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur l'icône **Info** à droite du champ **Source IP Address** (Adresse IP source) pour obtenir des renseignements supplémentaires sur le format d'entrée à utiliser.

e) Saisissez un port source valide dans le champ **Source Port** (Port source) ou cliquez sur l'icône **Edit** (Modifier) à droite du champ **Source Port** (Port source). Choisissez une condition de filtrage dans la liste déroulante, puis cliquez sur **Add** (Ajouter). Cliquez sur **OK** pour afficher ces paramètres dans la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur l'icône **Info** à droite du champ **Source Port** (Port source) pour obtenir des renseignements supplémentaires sur le format d'entrée à utiliser.

f) Saisissez une adresse IP de destination valide dans le champ **Destination IP Address** (Adresse IP de destination), ou cliquez sur l'icône **Edit** (Modifier) à droite du champ **Destination IP Address** (Adresse IP de destination). Choisissez une adresse IP unique ou une plage spécifiée d'adresses IP, puis cliquez sur **Add** (Ajouter). Cochez la case **Do not include (exclude) this address or range** (Ne pas inclure (exclure) cette adresse ou cette plage) pour exclure une adresse IP ou une plage d'adresses IP spécifiques. Cliquez sur **OK** pour afficher ces paramètres dans la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur l'icône **Info** à droite du champ **Destination IP Address** (Adresse IP de destination) pour obtenir des renseignements supplémentaires sur le format d'entrée à utiliser.

g) Saisissez un port de destination valide dans le champ **Destination Port** (Port de destination) ou cliquez sur l'icône **Edit** (Modifier) à droite du champ **Destination Port** (Port de destination). Choisissez une condition de filtrage dans la liste déroulante, puis cliquez sur **Add** (Ajouter). Cliquez sur **OK** pour afficher ces paramètres dans la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur l'icône **Info** à droite du champ **Destination Port** (Port de destination) pour obtenir des renseignements supplémentaires sur le format d'entrée à utiliser.

h) Saisissez le texte de filtrage dans le champ **Description**. Le texte peut être n'importe quelle chaîne d'un ou plusieurs caractères, y compris une expression régulière. Cependant, les points-virgules ne sont pas des caractères valides et ce paramètre est sensible à la casse. Les entrées multiples doivent être séparées par des virgules.

i) Cliquez sur **OK** pour ajouter les paramètres de filtre que vous venez de spécifier à la liste déroulante **Filter By** (Filtrer par) dans les visionneuses de journaux. Les chaînes de filtre suivent un format spécifique. Le préfixe FILTRE : désigne tous les filtres personnalisés qui apparaissent dans la liste déroulante **Filter By** (Filtrer par). Vous pouvez toujours saisir du texte aléatoire dans ce champ.

Le tableau suivant présente des exemples du format utilisé.

Créer un exemple de filtre	Format de chaîne de filtre
IP source = 192.168.1.1 ou 0.0.0.0 Port source = 67	FILTRE : srcIP=192.168.1.1,0.0.0.0;srcPort=67;

Créer un exemple de filtre	Format de chaîne de filtre
Gravité = informationnelle IP de destination = 1.1.1.1 à 1.1.1.10	FILTRE : sev=6;dstIP=1.1.1.1-1.1.1.10;
ID du journal système non compris entre 725 001 et 725 003	FILTRE : sysID=!725001-725003;
IP source = 1.1.1.1 Description = sortie générée	FILTRE : srcIP=1.1.1.1;descr=sortie générée

Étape 4 Choisissez l'un des paramètres dans la liste déroulante **Filter By** (Filtrer par) pour filtrer les messages du journal système, puis cliquez sur **Filter** (Filtrer) dans la barre d'outils. Ce paramètre s'applique également à tous les futurs messages du journal système. Cliquez sur **Show All** (Afficher tout) dans la barre d'outils pour effacer tous les filtres.

Remarque Vous ne pouvez pas enregistrer des filtres que vous avez spécifiés dans la boîte de dialogue **Build Filter** (Créer un filtre). Ces filtres ne sont valides que pour la session ASDM au cours de laquelle ils ont été créés.

Modifier les paramètres de filtrage

Pour modifier les paramètres de filtrage que vous avez créés à l'aide de la boîte de dialogue **Build Filter** (Créer un filtre), procédez comme suit :

Procédure

Choisissez une des options suivantes :

- Révisez un filtre directement en saisissant les modifications dans la liste déroulante **Filter By** (Filtrer par).
- Choisissez un filtre dans la liste déroulante **Filter By** (Filtrer par), puis cliquez sur **Build Filter** (Créer un filtre) pour afficher la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur **Clear Filter** (Effacer le filtre) pour supprimer les paramètres de filtre actuels et en saisir de nouveaux. Sinon, modifiez les paramètres qui s'affichent, puis cliquez sur **OK**.

Remarque Ces paramètres de filtre s'appliquent uniquement à ceux définis dans la boîte de dialogue **Build Filter** (Créer un filtre).

- Cliquez sur **Show All** (Afficher tout) dans la barre d'outils pour arrêter le filtrage et afficher tous les messages du journal système.

Émettre certaines commandes à l'aide des visionneuses de journaux

Vous pouvez exécuter les commandes suivantes à l'aide de l'une des visionneuses de journaux : **ping**, **traceroute**, **whois** et **dns lookup**.

Pour exécuter l'une de ces commandes, procédez comme suit :

Procédure

Étape 1 Choisissez une des options suivantes :

- **Monitoring (Supervision)** > **Logging (Journalisation)** > **Real-Time Log Viewer (Visionneuse de journal en temps réel)** > **View (Afficher)**
- **Monitoring (Supervision)** > **Logging (Journalisation)** > **Log Buffer (Tampon de journal)** > **View (Afficher)**

Étape 2 Cliquez sur **Tools (Outils)** dans le volet **Real-Time Log Viewer** (Visionneuse de journal en temps réel) ou **Log Buffer** (Tampon du journal), puis choisissez la commande que vous souhaitez exécuter. Sinon, vous pouvez cliquer avec le bouton droit sur un message de journal système répertorié pour afficher un menu contextuel, puis choisir la commande que vous souhaitez exécuter.

La boîte de dialogue **Entering command** (Saisie de la commande) s'affiche. La commande que vous avez sélectionnée s'affiche automatiquement dans la liste déroulante.

Étape 3 Saisissez l'adresse IP source ou de destination du message de journal système sélectionné dans le champ **Address** (Adresse), puis cliquez sur **Go** (Aller).

La sortie de la commande s'affiche dans la zone fournie.

Étape 4 Cliquez sur **Clear** (Effacer) pour supprimer la sortie et choisissez une autre commande à exécuter dans la liste déroulante. Répétez l'étape 3, si nécessaire. Cliquez sur **Close** (Fermer) lorsque vous avez terminé.

Historique de journalisation

Tableau 3 : Historique de journalisation

Nom de la caractéristique	Versions de plateforme	Description
Logging (journalisation)	7.0(1)	Fournit des informations de journalisation sur le réseau ASA par le biais de diverses destinations de sortie, et comprend l'option permettant d'afficher et d'enregistrer les fichiers journaux. Nous avons introduit l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Logging Setup (Configuration de la journalisation).
Limite de débit	7.0(4)	Limite le débit auquel les messages de journal système sont générés. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Rate Limit (Limite de débit).
Liste de journalisation	7.2(1)	Crée une liste de journalisation à utiliser dans d'autres commandes pour spécifier les messages selon divers critères (niveau de journalisation, classe d'événement et ID de message). Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Event Lists (Listes d'événements).
Journalisation de sécurité	8.0(2)	Indique que la connexion à l'hôte de journalisation distant doit utiliser SSL/TLS. Cette option est valide uniquement si le protocole sélectionné est TCP. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Server (Serveur de journal système).
Classe de journalisation	8.0(4), 8.1(1)	Ajout de la prise en charge de la classe d'événements ipaa des messages de journalisation. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Logging Filters (Filtres de journalisation).
Classe de journalisation et tampons de journalisation enregistrés	8.2(1)	Ajout de la prise en charge de la classe d'événements dap des messages de journalisation. Ajout de prise en charge pour effacer les tampons de journalisation enregistrés (ASDM, internes, FTP et flash). Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Logging Setup (Configuration de la journalisation).
Chiffrement de mot de passe	8.3(1)	Ajout de la prise en charge du chiffrement de mot de passe.
Visionneuses de journaux	8.3(1)	Les adresses IP sources et de destination ont été ajoutées aux visionneuses de journaux.

Nom de la caractéristique	Versions de plateforme	Description
Journalisation et blocage des connexions améliorés	8.3(2)	Lorsque vous configurez un serveur de journal système pour utiliser TCP et que ce serveur n'est pas disponible, l'ASA bloque les nouvelles connexions qui génèrent des messages de journal système jusqu'à ce que le serveur soit à nouveau disponible (par exemple, les connexions VPN, pare-feu et mandataire direct). Cette fonctionnalité a été améliorée pour bloquer également les nouvelles connexions lorsque la file d'attente de journalisation sur l'ASA est pleine; les connexions reprendront lorsque la file d'attente de journalisation sera effacée. Cette fonctionnalité a été ajoutée pour la conformité aux Common Criteria EAL4+. Sauf si nécessaire, nous avons conseillé d'autoriser les connexions lorsque les messages de journal système ne peuvent pas être envoyés ou reçus. Pour autoriser les connexions, continuez à cochez la case **Allow user traffic to pass when TCP syslog server is down** (Autoriser le trafic utilisateur à passer lorsque le serveur de journal système TCP est en panne) dans le volet Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Servers (Serveurs de journal système). Nous avons introduit les messages de journal système suivants : 414005, 414006, 414007 et 414008. Nous n'avons pas modifié d'écrans ASDM.
Filtrage et tri des messages de journal système	v 8.4(1)	Une prise en charge a été ajoutée pour les éléments suivants : • Filtrage des messages de journal système en fonction de plusieurs chaînes de texte correspondant à différentes colonnes • Création de filtres personnalisés • Tri des messages par colonne. Pour en savoir plus, consultez le guide de configuration ASDM. Cette fonctionnalité est compatible avec toutes les versions d'ASA. Nous avons modifié les écrans suivants : Monitoring (Supervision) > Logging (Journalisation) > Real-Time Log Viewer (Visionneuse de journal en temps réel) > View (Afficher). Monitoring (Supervision) > Logging (Journalisation) > Log Buffer Viewer (Visionneuse de tampon de journal) > View (Afficher).
Mise en grappe	9.0(1)	Ajout de la prise en charge de la génération de messages de journal système dans un environnement de grappe sur l'ASA 5580 et 5585-X. Nous avons modifié l'écran suivant : Configuration > Logging (Journalisation) > Syslog Setup (Configuration du journal système) > Advanced (Avancé) > Advanced Syslog Configuration (Configuration du journal système avancée).

Nom de la caractéristique	Versions de plateforme	Description
Blocage des journaux système sur une unité de secours	9.4(1)	Nous avons ajouté la prise en charge du blocage de la génération de messages de journal système spécifiques sur l'unité de secours dans une configuration de basculement. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Setup (Configuration du journal système).
Identités de référence pour les connexions au serveur de journal système sécurisé	9.6(2)	Le traitement du client TLS prend désormais en charge les règles de vérification de l'identité de serveur définies dans la RFC 6125, section 6. La vérification de l'identité sera effectuée pendant la validation PKI pour les connexions TLS au serveur de journal système. Si l'identité présentée ne correspond pas à l'identité de référence configurée, la connexion n'est pas établie. Nous avons modifié les pages suivantes : **ASDM Configuration (Configuration ASDM) > Remote Access VPN (VPN d'accès à distance) > Advanced (Avancé)** et **Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Servers (Serveurs de journal système) -> Add (Ajouter) ou Edit (Modifier).**
Prise en charge des adresses IPv6 pour les serveurs de journal système	9.7(1)	Vous pouvez maintenant configurer des serveurs de journal système avec des adresses IPv6 pour enregistrer, envoyer et recevoir des journaux système sur TCP et UDP. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Servers (Serveurs de journal système)** > **Add Syslog Server (Ajouter un serveur de journal système)**
Classe de journalisation	9.12(1)	Ajout de la prise en charge de la BFD, du BGP, de l'interface, de l'IPv6, de la multidiffusion, de la commande Object-Group-Search, du PBR, du routage et de la classe SLA des messages de journalisation. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**.
Prise en charge de l'interface de boucle avec retour pour le journal système	9.18(2)	Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour le journal système. Commandes nouvelles/modifiées : **interface loopback**, **logging host** Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add Loopback Interface (ajouter une interface de bouclage)**. La prise en charge d'ASDM a été ajoutée dans la version 7.19.

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.