Journalisation

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

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'. Cette valeur est toujours .
Level (Niveau)	0 à 7. 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

Le tableau suivant répertorie les niveaux de gravité des messages du journal 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**	Système inutilisable.
1	**alerte**	Action immédiate requise.
2	**critique**	Conditions critiques.
3	**erreur**	Conditions d'erreur.
4	**avertissement**	Conditions de mise en garde.
5	**notification**	Condition normale, mais pouvant être grave
6	**renseignements**	Messages informatifs seulement.
7	**débogage**	Messages de débogage uniquement Ne journalisez à ce niveau que temporairement, lors du débogage des problèmes. Ce niveau de journalisation peut générer tant de messages que les performances du système peuvent en être affectées.

Remarque ASA et ne génèrent pas de messages syslog avec un niveau de gravité de zéro (urgences).

Filtrage des messages Syslog

Vous pouvez filtrer les messages syslog générés de sorte que seuls certains messages syslog soient envoyés vers une destination de sortie particulière. Par exemple, vous pouvez configurer ASA pour envoyer tous les messages syslog vers une destination de sortie et pour envoyer un sous-ensemble de ces messages syslog vers une autre destination de sortie.

Plus précisément, vous pouvez diriger les messages du 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 personnalisez ces critères en créant une liste de messages que vous pouvez préciser lorsque vous définissez la destination de sortie. 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.

Classe de messages Syslog

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. Utilisez la commande **logging class**.
- Créez une liste de messages qui spécifie la classe du message. Utilisez la commande **logging list**.

La classe de messages syslog fournit une méthode de catégorisation des messages syslog par type, ce qui équivaut à une fonctionnalité ou à une fonction du périphérique. Par exemple, la classe rip désigne 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, tous les ID de message syslog qui commencent par les chiffres 611 sont associés à la classe vpnc (client VPN). Les messages syslog associés à la fonctionnalité de client VPN vont de 611101 à 611323.

En outre, la plupart des messages syslog ISAKMP ont un ensemble commun d'objets ajoutés au début pour aider à identifier le tunnel. Ces objets précèdent le texte descriptif d'un message syslog lorsqu'ils sont disponibles. Si l'objet est inconnu au moment de la génération du message syslog, la combinaison en-tête = valeur ne s'affiche pas.

Les objets portent le préfixe suivant :

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

Lorsque le groupe est le groupe de tunnels, le nom d'utilisateur est le nom d'utilisateur de la base de données locale ou du serveur AAA et l'adresse IP est 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

Classe	Définition	Numéros d'ID des messages Syslog
—	Mise en grappe	747
—	Gestion des cartes	323
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

Classe	Définition	Numéros d'ID des messages Syslog
np	Processeur de réseau	319
—	NP SSL	725
ospf	Routage OSPF	318, 409, 503, 613
—	Chiffrement de mot de passe	742
—	Serveur mandataire téléphonique	337
protocole 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

Classe	Définition	Numéros d'ID des messages Syslog
—	VXLAN	778
webfo	Basculement WebVPN	721
webvpn	WebVPN et Secure Client (services client sécurisés)	716

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.

Lignes directrices relatives à la journalisation

Cette section comprend des consignes et des limites que vous devez consulter avant de configurer la journalisation.

Directives IPv6

- IPv6 est pris en charge. Les journaux système peuvent être envoyés en utilisant les protocoles TCP ou 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.
- La journalisation sécurisée sur IPv6 n'est pas prise en charge.

Directives supplémentaires

- 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. Ces fichiers ne sont pas compatibles avec le périphérique. Leur utilisation entraînera une erreur d'analyse et, éventuellement, le processus syslog-ng échouera.
- 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, saisissez une nouvelle commande pour chaque serveur 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.
- Il n'est pas possible d'affecter deux listes ou classes différentes à des serveurs syslog différents ou aux mêmes emplacements.
- Vous pouvez configurer jusqu'à seize serveurs de journaux système. Cependant, en mode contexte multiple, la limitation est de 4 serveurs par contexte.
- Le serveur syslog doit être accessible au moyen de 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. Assurez-vous d'avoir activé 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.
- 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. Il s'agit du comportement attendu. 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.

- 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 n'inclut pas 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
  ```

- 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).
- 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.

Configurer la journalisation

Cette section décrit comment configurer la journalisation.

Activer la journalisation

Pour activer la journalisation, procédez comme suit :

Procédure

Activer la journalisation

logging enable

Exemple :

```
ciscoasa(config)# logging enable
```

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'interface que vous configurez dispose d'un accès de gestion uniquement désactivé.

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 Configurez l'ASA pour envoyer des messages aux serveurs de journal système.

Vous pouvez configurer l'ASA pour envoyer des messages aux serveurs de journal système IPv4 ou IPv6.

logging host *interface_name syslog_ip* [**tcp**[/*port*] | **udp** [/*port*] [**format emblem**]]

Exemple :

```
ciscoasa(config)# logging host dmz1 192.168.1.5 udp/1026
ciscoasa(config)# logging host dmz1 2002::1:1 udp/2020
```

Le mot clé **format emblem** active la journalisation au format EMBLEM pour le serveur de journal système avec UDP uniquement. L'argument *interface_name* spécifie l'interface par laquelle vous accédez au serveur de journal système. L'argument *syslog_ip* spécifie l'adresse IP du serveur de journal système. La paire mot clé-argument **tcp**[/*port*] ou **udp**[/*port*] spécifie que l'ASA doit utiliser TCP ou UDP pour envoyer des messages de journal système au serveur de journal système.

Vous pouvez configurer l'ASA pour envoyer des données à un serveur de journal système en utilisant UDP ou TCP, mais pas les deux. 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 les nouvelles connexions, quelle que soit la connectivité à un serveur de journal système TCP, consultez l'étape 3.

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.

Étape 2 Spécifiez les messages de journal système qui doivent être envoyés au serveur de journal système.

logging trap {*severity_level* | *message_list*}

Exemple :

```
ciscoasa(config)# logging trap errors
```

Vous pouvez spécifier le numéro du niveau de gravité (1 à 7) ou le nom. Par exemple, si vous définissez le niveau de gravité 3, l'ASA envoie des messages de journal système pour les niveaux de gravité 3, 2 et 1. Vous pouvez spécifier une liste de messages sur mesure qui identifie les messages de journal système à envoyer au serveur de journal système.

Étape 3 (Facultatif) Désactivez la fonction pour bloquer les nouvelles connexions lorsqu'un serveur de journal système connecté au TCP est en panne.

logging permit-hostdown

Exemple :

```
ciscoasa(config)# logging permit-hostdown
```

Lorsque l'ASA est configuré pour envoyer des messages de journal système à un serveur de journal système basé sur TCP, et si le serveur de journal système est en panne ou la file d'attente du journal est pleine, les nouvelles connexions à l'ASA sont bloquées. Les nouvelles connexions sont à nouveau autorisées une fois que le serveur de journal système est de nouveau opérationnel et que la file d'attente du journal n'est plus pleine. À l'aide de cette commande, vous pouvez autoriser les nouvelles connexions même si le serveur de journal système n'est pas opérationnel.

Étape 4 (Facultatif) Définissez la fonction de journalisation sur une valeur autre que 20, qui est celle attendue par la plupart des systèmes UNIX.

logging facility *number*

Exemple :

```
ciscoasa(config)# logging facility 21
```

Activer la journalisation sécurisée

Procédure

Activez la journalisation sécurisée en spécifiant le mot clé **secure** dans la commande de l'hôte de journalisation. En outre, saisissez éventuellement la commande **reference-identity**.

logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**[**reference-identity** *reference_identity_name*]]

Lieu :

- **logging host** *interface_name syslog_ip* spécifie l'interface sur laquelle se trouve le serveur de journal système et l'adresse IP du serveur de journal système.
- [**tcp**/*port* | **udp**/*port*] spécifie le port (TCP ou UDP) que le serveur de journal système écoute pour les messages du journal système. Le mot clé **tcp** indique que l'ASA doit utiliser TCP pour envoyer des messages du journal système au serveur de journal système. Le mot clé **udp** indique que l'ASA doit utiliser UDP pour envoyer des messages du journal système au serveur de journal système.
- Le mot clé **format emblem** active la journalisation au format EMBLEM pour le serveur de journal système.
- Le mot clé **secure** indique que la connexion à l'hôte de journalisation distant doit utiliser SSL/TLS pour TCP uniquement. La journalisation sécurisée ne prend pas en charge UDP; une erreur se produit si vous essayez d'utiliser ce protocole.
- [**reference-identity** *reference_identity_name*] active les vérifications d'identité de référence RFC 6125 sur le certificat en fonction de l'objet d'identité de référence précédemment configuré. Consultez Configurer les identités de référence pour en savoir plus sur l'objet d'identité de référence.

Exemple :

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure  reference-identity
syslogServer
```

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

Envoyez des messages de journal système au format EMBLEM à un serveur de journal système sur UDP en utilisant le port 514.

logging host *interface_name ip_address*{**tcp** [/*port*] | **udp** [/ *port*]] [**format emblem**]

Exemple :

```
ciscoasa(config)# logging host interface_1 127.0.0.1 udp format emblem
ciscoasa(config)# logging host interface_1 2001::1 udp format emblem
```

Vous pouvez configurer des serveurs de journal système IPv4 ou IPv6.

Le mot clé **format emblem** active la journalisation au format EMBLEM pour le serveur de journal système (UDP uniquement). L'argument *interface_name* spécifie l'interface par laquelle vous accédez au serveur de journal système. L'argument *ip_address* spécifie l'adresse IP du serveur de journal système. La paire mot clé-argument **tcp**[/*port*] or **udp**[/*port*] spécifie que l'ASA doit utiliser TCP ou UDP pour envoyer des messages de journal système au serveur de journal système.

Vous pouvez configurer l'ASA 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.

Vous pouvez utiliser plusieurs commandes **logging host** pour spécifier des serveurs supplémentaires qui recevront tous des messages de journal système. Si vous configurez au moins deux serveurs de journalisation, veillez à limiter le niveau de gravité de la journalisation aux avertissements pour tous les serveurs de journalisation.

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 3 de Envoyer des messages du journal système à un serveur externe de journal système, à la page 11.

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

Envoyez des messages de journal système au format EMBLEM à des destinations de sortie autres qu'un serveur de journal système, comme des sessions Telnet ou SSH.

logging emblem

Exemple :

```
ciscoasa(config)# logging emblem
```

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 Spécifiez quels messages de journal système doivent être envoyés au tampon du journal interne, qui sert d'emplacement de stockage temporaire.

logging buffered {*severity_level* | *message_list*}

Exemple :

```
ciscoasa(config)# logging buffered critical
ciscoasa(config)# logging buffered level 2
ciscoasa(config)# logging buffered notif-list
```

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 vider le tampon du journal interne, saisissez la commande **clear logging buffer**.

Étape 2 Modifiez la taille du tampon du journal interne. La taille du tampon par défaut est de 4 Ko.

logging buffer-size *bytes*

Exemple :

```
ciscoasa(config)# logging buffer-size 16384
```

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.

Étape 3 Choisissez une des options suivantes :

- Enregistrez les nouveaux messages dans le tampon du journal interne et enregistrez le contenu complet de ce tampon dans la mémoire flash interne.

  logging flash-bufferwrap

  Exemple :

  ```
  ciscoasa(config)# logging flash-bufferwrap
  ```

  Remarque
  Si la taille de tampon est supérieure à 2 Mo, cette commande arrête d'écrire des données dans la mémoire flash, sans avertissement.

- Enregistrez les nouveaux messages dans le tampon du journal interne et enregistrez le contenu complet du tampon du journal sur un serveur FTP.

  logging ftp-bufferwrap

  Exemple :

  ```
  ciscoasa(config)# logging ftp-bufferwrap
  ```

  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.

- Identifiez le serveur FTP sur lequel vous souhaitez stocker le contenu du tampon du journal.

  logging ftp-server *server pathusername password*

  Exemple :

  ```
  ciscoasa(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
  ```

  L'argument *server* spécifie l'adresse IP du serveur FTP externe. L'argument *path* spécifie le chemin d'accès au répertoire sur le serveur FTP où les données du tampon du journal doivent être enregistrées. Ce chemin est relatif au répertoire racine FTP. L'argument *username* spécifie un nom d'utilisateur valide pour la connexion au serveur FTP. L'argument *password* indique le mot de passe pour le nom d'utilisateur spécifié.

- Enregistrez le contenu actuel du tampon du journal dans la mémoire flash interne.

  logging savelog [*savefile*]

  Exemple :

```
ciscoasa(config)# logging savelog latest-logfile.txt
```

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 Spécifiez la quantité maximum de mémoire flash interne disponible pour l'enregistrement des fichiers journaux.

logging flash-maximum-allocation *kbytes*

Exemple :

```
ciscoasa(config)# logging flash-maximum-allocation 1200
```

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. La limite maximum de la valeur flash-maximum-allocation est de 2 Go.

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.

Étape 2 Spécifiez la quantité minimum de mémoire flash interne qui doit être libre pour que l'ASA enregistre un fichier journal.

logging flash-minimum-free *kbytes*

Exemple :

```
ciscoasa(config)# logging flash-minimum-free 4000
```

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 Spécifiez quels messages de journal système doivent être envoyés à une adresse courriel.

logging mail {*severity_level* | *message_list*}

Exemple :

```
ciscoasa(config)# logging mail high-priority
```

Lors de l'envoi par courriel, un message de journal système s'affiche dans la ligne d'objet du courriel. Pour cette raison, nous vous conseillons de configurer cette option pour informer les administrateurs des messages de journal système de niveau de gravité élevé, tels que critique, alerte et urgence.

Étape 2 Spécifiez l'adresse courriel source à utiliser lors de l'envoi des messages de journal système à une adresse courriel.

logging from-address *email_address*

Exemple :

```
ciscoasa(config)# logging from-address xxx-001@example.com
```

Étape 3 Spécifiez l'adresse courriel du destinataire à utiliser lors de l'envoi des messages de journal système à une adresse courriel.

logging recipient-address *e-mail_address*[*severity_level*]

Exemple :

```
ciscoasa(config)# logging recipient-address admin@example.com
```

Étape 4 Spécifiez le serveur SMTP à utiliser lors de l'envoi des messages de journal système à une adresse courriel. Vous pouvez fournir une adresse de serveur principal et secondaire pour assurer le service de messagerie du journal sans défaillance. Vous pouvez également associer une interface et le serveur pour identifier la table de routage à utiliser pour la journalisation. Si aucune interface n'est fournie, l'ASA fera référence à la table de routage de gestion et, en l'absence d'entrée de route, il examinera la table de routage des données.

smtp-server [*primary-interface*] *primary-smpt-server-ip-address* [[*backup-interface*]*backup-smpt-server-ip-address*]

Exemple :

```
ciscoasa(config)# smtp-server 10.1.1.24 10.1.1.34
ciscoasa(config)# smtp-server 10.1.1.24
ciscoasa(config)# smtp-server management 10.1.1.24 outside 10.1.1.34
ciscoasa(config)# smtp-server management 10.1.1.24
```

Envoyer les messages du journal système au gestionnaire ASDM

Pour envoyer des messages de journal système à ASDM, procédez comme suit :

Procédure

Étape 1 Spécifiez les messages de journal système qui doivent être envoyés à ASDM.

logging asdm {*severity_level* | *message_list*}

Exemple :

```
ciscoasa(config)# logging asdm 2
```

L'ASA réserve une zone de tampon pour les messages de journal système en attente d'envoi à ASDM et enregistre les messages dans le tampon au fur et à mesure qu'ils apparaissent. Le tampon du journal ASDM est un tampon différent de celui du tampon interne. Lorsque le tampon du journal ASDM est plein, l'ASA supprime le message de journal système le plus ancien afin de libérer de l'espace dans le tampon pour les nouveaux messages. La suppression du message de journal système le plus ancien pour faire de la place aux nouveaux messages est le paramètre par défaut dans ASDM. Pour contrôler le nombre de messages de journal système conservés dans le tampon du journal ASDM, vous pouvez modifier la taille de ce tampon.

Étape 2 Spécifiez le nombre de messages de journal système à conserver dans le tampon du journal ASDM.

logging asdm-buffer-size *num_of_msgs*

Exemple :

```
ciscoasa(config)# logging asdm-buffer-size 200
```

Saisissez la commande **clear logging asdm** pour vider le contenu actuel du tampon du journal ASDM.

Configurer la file d'attente de journalisation

Pour configurer la file d'attente de journalisation, procédez comme suit :

Procédure

Spécifiez le nombre de messages de journal système que l'ASA peut contenir dans sa file d'attente avant de les envoyer à la destination de sortie configurée.

logging queue *message_count*

Exemple :

```
ciscoasa(config)# logging queue 300
```

Les ASA ont un nombre fixe de blocs en mémoire qui peuvent être alloués pour la mise en mémoire tampon des messages du journal système en attente d'envoi à la destination de sortie configurée. Le nombre de blocs requis dépend de la longueur de la file d'attente des messages de journal système et du nombre de serveurs de journal système spécifié. La taille de la file d'attente par défaut est de 512 messages de journal système. La taille de la file d'attente n'est limitée que par la disponibilité de la mémoire de blocage. Les valeurs valides vont de 0 à 8 192 messages, selon la plateforme. Si la file d'attente de journalisation est fixée à zéro, la file d'attente a la taille configurable maximale (8 192 messages).

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

Spécifiez quels messages de journal système doivent être envoyés au port de console.

logging console { *severity_level* | *message_list*}

Exemple :

```
ciscoasa(config)# logging console errors
```

Envoyer les messages du journal système au serveur SNMP

Pour activer la journalisation sur un serveur SNMP, procédez comme suit.

Procédure

Activez la journalisation SNMP et spécifiez les messages à envoyer aux serveurs SNMP.

logging history [*logging_list* | *level*]

Exemple :

```
ciscoasa(config)# logging history errors
```

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 Spécifiez quels messages de journal système doivent être envoyés à une session Telnet ou SSH.

logging monitor {*severity_level* | *message_list*}

Exemple :

```
ciscoasa(config)# logging monitor 6
```

Étape 2 Activez la journalisation pour la session en cours uniquement.

terminal monitor

Exemple :

```
ciscoasa(config)# terminal monitor
```

Si vous vous déconnectez puis vous reconnectez, vous devrez saisir à nouveau cette commande. Saisissez la commande **terminal no monitor** pour désactiver la journalisation pour la session en cours.

Configurer les messages du journal système

Afficher ou masquer les noms d'utilisateur non valides dans les journaux système

Vous pouvez afficher ou masquer 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.

Procédure

Étape 1 Afficher les noms d'utilisateur non valides :

no logging hide username

Étape 2 Masquer les noms d'utilisateur non valides :

logging hide username

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

Précisez que les messages du journal système doivent inclure la date et l'heure auxquelles ils ont été générés.

logging timestamp

Exemple :

```
ciscoasa(config)# logging timestamp
LOG-2008-10-24-081856.TXT
```

Pour supprimer la date et l'heure des messages du journal système, saisissez la commande **no logging timestamp**.

Désactiver un message du journal système

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

Procédure

Empêchez l'ASA de générer un message de journal système particulier.

no logging message *syslog_id*

Exemple :

```
ciscoasa(config)# no logging message 113019
```

Pour réactiver un message du journal système désactivé, saisissez la commande **logging message** *syslog_id* (par exemple, **logging message 113019**). Pour réactiver la journalisation de tous les messages du journal système désactivés, saisissez la commande **clear configure logging disabled**.

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

Spécifiez le niveau de gravité d'un message du journal système.

logging message *syslog_id* **level** *severity_level*

Exemple :

```
ciscoasa(config)# logging message 113019 level 5
```

Pour réinitialiser le niveau de gravité d'un message du journal système à ses paramètres, saisissez la commande **no logging message** *syslog_id* **level** *severity_level* (par exemple, **no logging message 113019 level 5**). Pour réinitialiser le niveau de gravité de tous les messages du journal système modifiés à leurs paramètres, saisissez la commande **clear configure logging level**.

Bloquer les messages du journal système sur une unité de secours

Procédure

Utilisez la commande suivante pour bloquer la génération d'un message de journal système spécifique sur une unité de secours.

no logging message *syslog-id* **standby**

Exemple :

```
ciscoasa(config)# no logging message 403503 standby
```

Débloquez un message du journal système donné pour vous assurer que les messages de journal système de l'ASA de secours pour le basculement restent synchronisés si le basculement se produit. Utilisez la commande **logging standby** pour débloquer la génération d'un message de journal système spécifique qui a précédemment été bloqué et ne peut pas être généré sur une unité de secours.

Remarque
Dans un état stable, lorsque les ASA actifs et en veille enregistrent les journaux, le trafic double sur les destinations de journalisation partagées, telles que les serveurs de journal système, les serveurs SNMP et les serveurs FTP. Cependant, en cas de basculement, pendant la phase de commutation, l'ASA de secours génère plus d'événements, y compris les intrusions de basculement et les événements de connexion de l'unité active.

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

Configurez l'ASA pour inclure un ID de périphérique dans les messages du journal système au format non EMBLEM. Vous ne pouvez spécifier qu'un seul type d'ID de périphérique pour les messages du journal système.

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

Exemple :

```
ciscoasa(config)# logging device-id hostname
ciscoasa(config)# logging device-id context-name
```

Le mot clé **context-name** indique que le nom du contexte actuel doit être utilisé comme ID de périphérique (s'applique au mode de contexte multiple uniquement). Si vous activez l'ID de périphérique de journalisation pour le contexte d'administration en mode de contexte multiple, les messages provenant de l'espace d'exécution du système utilisent un ID de périphérique de **system** et les messages provenant du contexte d'administration utilisent le nom du contexte d'administration comme ID de périphérique.

Remarque
Dans une grappe ASA, utilisez toujours l'adresse IP de l'unité de contrôle pour l'interface sélectionnée.

Le mot clé **cluster-id** spécifie le nom unique dans la configuration de démarrage d'une unité ASA individuelle dans la grappe en tant qu'ID de périphérique. Le mot clé **hostname** spécifie que le nom d'hôte de l'ASA doit être utilisé comme ID de périphérique. La paire mot clé-argument **ipaddress** *interface_name* précise que l'adresse IP de l'interface spécifiée comme *interface_name* doit être utilisée comme ID de périphérique. Si vous utilisez le mot clé **ipaddress**, l'ID de périphérique devient l'adresse IP de l'interface ASA spécifiée, quelle que soit l'interface à partir de laquelle le message de journal système est envoyé. Dans l'environnement de grappe, le mot clé **system** détermine que l'ID de périphérique devient l'adresse IP système sur l'interface. Ce mot clé fournit un ID de périphérique unique et cohérent pour tous les messages de journal système envoyés à partir du périphérique. La paire mot clé-argument **string** *text* spécifie que la chaîne de texte doit être utilisée comme ID de périphérique. La chaîne peut inclure jusqu'à 16 caractères.

Vous ne pouvez pas utiliser d'espaces ni l'un des caractères suivants :

- & (esperluette)
- ‘ (guillemets simples)
- “ (guillemets doubles)
- < (inférieur à)
- > (supérieur à)
- ? (point d'interrogation)

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.

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 personnalisées à envoyer à une destination de journalisation spécifique (par exemple, un serveur SNMP), procédez comme suit :

Procédure

Étape 1 Spécifiez les critères de sélection des messages à enregistrer dans le tampon du journal interne. Par exemple, si vous définissez le niveau de gravité 3, l'ASA envoie des messages de journal système pour les niveaux de gravité 3, 2 et 1.

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

Exemple :

```
ciscoasa(config)# logging list list-notif level 3
```

L'argument *name* spécifie le nom de la liste. La paire mot clé-argument **level** *level* spécifie le niveau de gravité. La paire mot clé-argument **class** *message_class* spécifie une classe de messages particulière. La paire mot clé-argument **message** *start_id* [*-end_id*] spécifie un numéro de message de journal système individuel ou une plage de numéros.

Remarque
N'utilisez pas les noms des niveaux de gravité comme nom d'une liste de messages de journal système. Les noms interdits comprennent les urgences, les alertes, les critiques, les erreurs, les avertissements, les notifications, les renseignements et le débogage. De même, n'utilisez pas les trois premiers caractères de ces mots au début d'un nom de liste d'événements. Par exemple, n'utilisez pas un nom de liste d'événements commençant par le caractère « err ».

Étape 2 (Facultatif) Ajoutez d'autres critères de sélection des messages à la liste.

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

Exemple :

```
ciscoasa(config)# logging list list-notif message 104024-105999
ciscoasa(config)# logging list list-notif level critical
ciscoasa(config)# logging list list-notif level warning class ha
```

Saisissez la même commande qu'à l'étape précédente, en précisant le nom de la liste de messages existante et le critère supplémentaire. Saisissez une nouvelle commande pour chaque critère que vous souhaitez ajouter à la liste. Par exemple, vous pouvez spécifier les critères pour les messages de journal système à inclure dans la liste comme suit :

- ID des messages du journal système compris entre 104 024 et 105 999.
- Tous les messages du journal système de niveau de gravité Critique ou supérieur (urgence, alerte ou critique).
- Tous les messages du journal système de classe ha avec un niveau de gravité d'avertissement ou supérieur (urgence, alerte, critique, erreur ou avertissement).

Remarque
Un message de journal système est journalisé s'il satisfait à l'une de ces conditions. Si un message de journal système satisfait à plusieurs conditions, le message est journalisé une seule fois.

Configurer les filtres de journalisation

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

Remplacez la configuration dans la commande de destination de sortie indiquée. 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.

logging class *message_class* {**buffered** | **console** | **history** | **mail** | **monitor** | **trap**} [*severity_level*]

Exemple :

```
ciscoasa(config)# logging class ha buffered alerts
```

Les mots clés **buffered**, **history**, **mail**, **monitor** et **trap** spécifient la destination de sortie à laquelle les messages du journal système de cette classe doivent être envoyés. Le mot clé **history** active la journalisation SNMP. Le mot clé **monitor** active la journalisation Telnet et SSH. Le mot clé **trap** active la journalisation du serveur de journal système. Sélectionnez une destination par entrée de ligne de commande. Pour spécifier qu'une classe doit être envoyée à plusieurs destinations, saisissez une nouvelle commande 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

Appliquez un niveau de gravité spécifié (1 à 7) à un ensemble de messages ou à un message en particulier (et non à la destination) dans une période donnée.

logging rate-limit {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

Exemple :

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

Les limites de débit ont une incidence sur le volume de messages envoyés à toutes les destinations configurées. Pour réinitialiser la limite de débit de journalisation à la valeur par défaut, saisissez la commande **clear running-config logging rate-limit**. Pour réinitialiser la limite de débit de journalisation, saisissez la commande **clear configure logging rate-limit**.

Supervision des journaux

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

- **show logging**

  Cette commande affiche les messages du journal système, y compris le niveau de gravité.

Remarque

- Le nombre maximum de messages de journal système pouvant être affichés est de 1 000, ce qui correspond au paramètre par défaut. Le nombre maximum de messages de journal système pouvant être affichés est de 2 000.
- Le compteur Host TX dans la sortie de la commande **show logging** s'affiche même après l'exécution de la commande **clear logging counters all**.

- **show logging message**

  Cette commande affiche une liste des messages de journal système avec les niveaux de gravité modifiés et des messages de journal système désactivés.

- **show logging message** *message_ID*

  Cette commande affiche le niveau de gravité d'un message de journal système spécifique.

- **show logging queue**

  Cette commande affiche la file d'attente de journalisation et les statistiques de la file d'attente.

- **show running-config logging rate-limit**

  Cette commande affiche le paramètre de limite de débit de journalisation actuel.

- **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).

Exemples de journalisation

Les exemples suivants montrent les renseignements de journalisation qui s'affichent pour la commande **show logging** :

```
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address "10.1.1.1"
    Mail logging: disabled
    ASDM logging: disabled
```

```
ciscoasa (config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: enabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 330272 messages logged
    Trap logging: level debugging, facility 20, 325464 messages logged
        Logging to inside 2001:164:5:1::123
    Permit-hostdown logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

Les exemples suivants montrent comment contrôler l'activation d'un message de journal système et le niveau de gravité du message de journal système spécifié :

```
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)

ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (disabled)

ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)
```

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.
Limite de débit	7.0(4)	Limite le débit auquel les messages de journal système sont générés. Nous avons introduit la commande suivante : **logging rate-limit**.

Nom de la caractéristique	Versions de plateforme	Description
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 introduit la commande suivante : **logging list**.
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 la commande suivante : **logging host**.
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 la commande suivante : **logging class**.
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. Nous avons modifié la commande suivante : **logging class**. Ajout de prise en charge pour effacer les tampons de journalisation enregistrés (ASDM, internes, FTP et flash). Nous avons introduit la commande suivante : **clear logging queue bufferwrap**.
Chiffrement de mot de passe	8.3(1)	Ajout de la prise en charge du chiffrement de mot de passe. Nous avons modifié la commande suivante : **logging ftp server**.
Visionneuses de journaux	8.3(1)	Les adresses IP sources et de destination ont été ajoutées aux visionneuses de journaux.
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 utiliser la commande **logging permit-hostdown**. Nous avons introduit les messages de journal système suivants : 414005, 414006, 414007 et 414008. Nous avons modifié la commande suivante : **show logging**.

Nom de la caractéristique	Versions de plateforme	Description
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.
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 la commande suivante : **logging device-id**.
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 introduit la commande suivante : **logging message** *syslog-id* **standby**.
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 ajouté ou modifié les commandes suivantes : **[no] crypto ca reference-identity**, **logging host**.
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 la commande suivante : **logging host**
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 la commande suivante : **logging class**.
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**

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.