Configurer les destinations des messages d'audit et des journaux

StorageGRID 11.8

NetApp
March 19, 2024

Sommaire

Configurer les destinations des messages d’audit et des journaux 1
Considérations relatives à l’utilisation d’un serveur syslog externe 1
Configurer les messages d’audit et le serveur syslog externe 6

Configurer les destinations des messages d'audit et des journaux

Considérations relatives à l'utilisation d'un serveur syslog externe

Un serveur syslog externe est un serveur hors de StorageGRID que vous pouvez utiliser pour collecter les informations d'audit système sur un emplacement unique. L'utilisation d'un serveur syslog externe vous permet de réduire le trafic réseau sur vos nœuds d'administration et de gérer les informations plus efficacement. Pour StorageGRID, le format de paquet de messages syslog sortants est conforme à la norme RFC 3164.

Les types d'informations d'audit que vous pouvez envoyer au serveur syslog externe sont les suivants :

- Journaux d'audit contenant les messages d'audit générés pendant le fonctionnement normal du système
- Événements liés à la sécurité tels que les connexions et la remontée à la racine
- Fichiers journaux d'application pouvant être demandés s'il est nécessaire d'ouvrir un dossier d'assistance pour résoudre un problème rencontré

Quand utiliser un serveur syslog externe

Un serveur syslog externe est particulièrement utile si vous disposez d'une grande grille, utilisez plusieurs types d'applications S3 ou souhaitez conserver toutes les données d'audit. L'envoi d'informations d'audit à un serveur syslog externe vous permet de :

- Collectez et gérez plus efficacement les informations d'audit telles que les messages d'audit, les journaux d'applications et les événements de sécurité.
- Réduisez le trafic réseau sur vos nœuds d'administration, car les informations d'audit sont transférées directement depuis les différents nœuds de stockage vers le serveur syslog externe, sans devoir passer par un nœud d'administration.

> Lorsque les journaux sont envoyés à un serveur syslog externe, les journaux uniques supérieurs à 8,192 octets sont tronqués à la fin du message pour se conformer aux limitations communes des implémentations de serveur syslog externe.

> Pour optimiser les options de restauration complète des données en cas de défaillance du serveur syslog externe, jusqu'à 20 Go de journaux locaux d'enregistrements d'audit (`localaudit.log`) sont gérés sur chaque nœud.

Comment configurer un serveur syslog externe

Pour savoir comment configurer un serveur syslog externe, reportez-vous à la section "Configurer les messages d'audit et le serveur syslog externe".

Si vous prévoyez de configurer l'utilisation du protocole TLS ou RELP/TLS, vous devez disposer des certificats suivants :

- **Certificats d'autorité de certification du serveur** : un ou plusieurs certificats d'autorité de certification de confiance pour vérifier le serveur syslog externe dans le codage PEM. Si omis, le certificat d'autorité de certification de la grille par défaut sera utilisé.
- **Certificat client** : certificat client pour l'authentification au serveur syslog externe dans le codage PEM.
- **Clé privée client** : clé privée pour le certificat client dans le codage PEM.

> Si vous utilisez un certificat client, vous devez également utiliser une clé privée client. Si vous fournissez une clé privée chiffrée, vous devez également fournir la phrase de passe. L'utilisation d'une clé privée chiffrée n'est pas un avantage majeur en matière de sécurité, car la clé et la phrase de passe doivent être stockées. Si elles sont disponibles, il est recommandé de recourir à une clé privée non chiffrée pour plus de simplicité.

Comment estimer la taille du serveur syslog externe

En principe, la taille de la grille est adaptée au débit requis, défini en termes d'opérations S3 par seconde ou d'octets par seconde. Par exemple, votre grid peut être capable de gérer 1,000 opérations S3 par seconde ou 2,000 Mo par seconde, d'ingales et de récupérations d'objets. Il est conseillé de dimensionner votre serveur syslog externe en fonction des besoins de votre grid.

Cette section fournit des formules heuristiques qui vous aident à estimer le taux et la taille moyenne des messages de journal de différents types requis par votre serveur syslog externe en termes de caractéristiques de performance connues ou souhaitées de la grille (opérations S3 par seconde).

Utilisez des opérations S3 par seconde dans les formules d'estimation

Si votre grille a été dimensionnée pour un débit exprimé en octets par seconde, vous devez convertir ce dimensionnement en opérations S3 par seconde afin d'utiliser les formules d'estimation. Pour convertir le débit du grid, vous devez d'abord déterminer la taille d'objet moyenne que vous pouvez utiliser les informations des journaux d'audit et des mesures existants (le cas échéant), ou en utilisant vos connaissances des applications qui utilisent StorageGRID. Par exemple, si la taille du grid a été dimensionnée pour atteindre un débit de 2,000 Mo/seconde, et que la taille d'objet moyenne est de 2 Mo, votre grille a été dimensionnée pour traiter 1,000 opérations S3 par seconde (2,000 Mo/2 Mo).

> Les formules de dimensionnement externe du serveur syslog présentées dans les sections suivantes fournissent des estimations communes (plutôt que des estimations de cas les plus défavorables). Selon votre configuration et votre charge de travail, un taux plus élevé ou moins élevé de messages syslog ou de données syslog peut être constaté que les formules le prévoient. Les formules sont destinées à être utilisées uniquement comme directives.

Formules d'estimation pour les journaux d'audit

Si vous ne disposez d'aucune information concernant votre charge de travail S3 autre que le nombre d'opérations S3 par seconde que votre grille doit prendre en charge, vous pouvez estimer le volume des journaux d'audit que votre serveur syslog externe devra gérer à l'aide des formules suivantes : Dans l'hypothèse où vous laissez les niveaux d'audit définis sur les valeurs par défaut (toutes les catégories sont définies sur Normal, sauf Storage, qui est défini sur erreur) :

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, votre serveur syslog externe doit être dimensionné pour prendre en charge 2,000 messages syslog par seconde et doit être capable de recevoir (et généralement stocker) les données du journal d'audit à un taux de 1.6 Mo par seconde.

Si vous en savez plus sur votre charge de travail, des estimations plus précises sont possibles. Pour les journaux d'audit, les variables supplémentaires les plus importantes sont le pourcentage d'opérations S3 PUT (par rapport à) et la taille moyenne, en octets, des champs S3 suivants (les abréviations de 4 caractères utilisées dans le tableau sont des noms de champs du journal d'audit) :

Code	Champ	Description
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Touche S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.

Nous allons utiliser P pour représenter le pourcentage d'opérations S3 qui sont PUT, où 0 ≤ P ≤ 1 (pour une charge de travail PUT de 100 %, P = 1, et pour une charge DE travail GET de 100 %, P = 0).

Utilisons K pour représenter la taille moyenne de la somme des noms des comptes S3, du compartiment S3 et de la clé S3. Supposons que le nom de compte S3 soit toujours mon compte s3 (13 octets), que les compartiments ont des noms de longueur fixe comme /my/application/catg-12345 (28 octets) et que les objets ont des clés à longueur fixe comme 5733a5d7-f069-41ef-8fbd-132449c69c (36 octets). La valeur de K est alors de 90 (13+13+28+36).

Si vous pouvez déterminer les valeurs P et K, vous pouvez estimer le volume des journaux d'audit que votre serveur syslog externe doit traiter à l'aide des formules suivantes, en supposant que vous laissez les niveaux d'audit par défaut (toutes les catégories définies sur Normal, sauf Storage, Qui est défini sur erreur) :

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, le workload est PUT à 50 %, et les noms de compte S3, les noms de compartiment, Et les noms d'objet utilisent une moyenne de 90 octets. Votre serveur syslog externe doit être dimensionné pour prendre en charge 1,500 messages syslog par seconde et doit être capable de recevoir (et généralement stocker) les données du journal d'audit à un taux d'environ 1 Mo par seconde.

Formules d’estimation pour les niveaux d’audit non par défaut

Les formules fournies pour les journaux d’audit supposent l’utilisation des paramètres par défaut du niveau d’audit (toutes les catégories sont définies sur Normal, sauf Storage, qui est défini sur erreur). Les formules détaillées d’estimation du taux et de la taille moyenne des messages d’audit pour les paramètres de niveau d’audit non par défaut ne sont pas disponibles. Toutefois, le tableau suivant peut être utilisé pour faire une estimation approximative du taux; vous pouvez utiliser la formule de taille moyenne fournie pour les journaux d’audit, mais sachez qu’elle risque de générer une surestimation car les messages d’audit « supplémentaires » sont, en moyenne, inférieurs aux messages d’audit par défaut.

Condition	Formule
Réplication : niveaux d’audit tous définis sur débogage ou Normal	Débit du journal d’audit = 8 x taux d’opérations S3
Codage d’effacement : les niveaux d’audit sont tous définis sur débogage ou Normal	Utiliser la même formule que pour les paramètres par défaut

Formules d’estimation pour les événements de sécurité

Les événements de sécurité ne sont pas corrélés avec les opérations S3 et produisent généralement un volume négligeable de journaux et de données. Pour ces raisons, aucune formule d’estimation n’est fournie.

Formules d’estimation pour les journaux d’application

Si vous ne disposez d’aucune information concernant votre charge de travail S3 autre que le nombre d’opérations S3 par seconde que que votre grid est censé prendre en charge, vous pouvez estimer le volume des journaux d’applications que votre serveur syslog externe devra gérer à l’aide des formules suivantes :

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, votre serveur syslog externe doit être dimensionné pour prendre en charge 3,300 journaux d’application par seconde et être capable de recevoir (et de stocker) les données de journaux d’application à un taux de 1.2 Mo par seconde environ.

Si vous en savez plus sur votre charge de travail, des estimations plus précises sont possibles. Pour les journaux d’application, les variables supplémentaires les plus importantes sont la stratégie de protection des données (réplication contre Le code d’effacement), le pourcentage d’opérations S3 PUT (par rapport à Et la taille moyenne, en octets, des champs S3 suivants (les abréviations de 4 caractères utilisées dans le tableau sont des noms de champs du journal d’audit) :

Code	Champ	Description
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l’utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.

Code	Champ	Description
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Touche S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.

Exemples d'estimations de dimensionnement

Cette section explique des exemples d'utilisation des formules d'estimation pour les grilles avec les méthodes de protection des données suivantes :

- La réplication
- Le code d'effacement

Si vous utilisez la réplication pour la protection des données

La p représente le pourcentage d'opérations S3 qui sont PUT, 0 ≤ P ≤ 1 (pour une charge de travail PUT de 100 %, P = 1 et POUR une charge DE travail GET de 100 %, P = 0).

K représente la taille moyenne de la somme des noms de compte S3, du compartiment S3 et de la clé S3. Supposons que le nom de compte S3 soit toujours mon compte s3 (13 octets), que les compartiments ont des noms de longueur fixe comme /my/application/catg-12345 (28 octets) et que les objets ont des clés à longueur fixe comme 5733a5d7-f069-41ef-8fbd-132449c69c (36 octets). Ensuite K a une valeur de 90 (13+13+28+36).

Si vous pouvez déterminer des valeurs pour P et K, vous pouvez estimer le volume des journaux d'application que votre serveur syslog externe devra traiter à l'aide des formules suivantes.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, le workload est utilisé à 50 % et les noms de comptes S3, de compartiments et de noms d'objet moyenne à 90 octets, votre serveur syslog externe doit être dimensionné pour prendre en charge 1800 journaux d'applications par seconde. Et sera en mesure de recevoir (et de stocker en général) des données d'application à un taux de 0.5 Mo par seconde.

Si vous utilisez le code d'effacement pour la protection des données

La p représente le pourcentage d'opérations S3 qui sont PUT, 0 ≤ P ≤ 1 (pour une charge de travail PUT de 100 %, P = 1 et POUR une charge DE travail GET de 100 %, P = 0).

K représente la taille moyenne de la somme des noms de compte S3, du compartiment S3 et de la clé S3.

Supposons que le nom de compte S3 soit toujours mon compte s3 (13 octets), que les compartiments ont des noms de longueur fixe comme /my/application/catg-12345 (28 octets) et que les objets ont des clés à longueur fixe comme 5733a5d7-f069-41ef-8fbd-132449c69c (36 octets). Ensuite K a une valeur de 90 (13+13+28+36).

Si vous pouvez déterminer des valeurs pour P et K, vous pouvez estimer le volume des journaux d'application que votre serveur syslog externe devra traiter à l'aide des formules suivantes.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

Par exemple, si votre grid est dimensionné pour 1,000 opérations S3 par seconde, votre workload pèse 50 % du volume et vos noms de compte S3, noms de compartiment, les noms d'objets sont en moyenne de 90 octets. votre serveur syslog externe doit être dimensionné pour prendre en charge 2,250 journaux d'applications par seconde et être capable de recevoir (et généralement de stocker) des données d'application à un taux de 0.6 Mo par seconde.

Configurer les messages d'audit et le serveur syslog externe

Vous pouvez configurer un certain nombre de paramètres liés aux messages d'audit. Vous pouvez ajuster le nombre de messages d'audit enregistrés, définir les en-têtes de requête HTTP que vous souhaitez inclure dans les messages d'audit de lecture et d'écriture des clients, configurer un serveur syslog externe et spécifier l'emplacement d'envoi des journaux d'audit, des journaux d'événements de sécurité et des journaux logiciels StorageGRID.

Les messages d'audit et les journaux enregistrent les activités du système et les événements de sécurité. Ils constituent les outils essentiels de surveillance et de dépannage. Tous les nœuds StorageGRID génèrent des messages d'audit et des journaux pour suivre l'activité et les événements du système.

Vous pouvez également configurer un serveur syslog externe pour enregistrer les informations d'audit à distance. L'utilisation d'un serveur externe réduit l'impact sur les performances de la journalisation des messages d'audit sans réduire l'exhaustivité des données d'audit. Un serveur syslog externe est particulièrement utile si vous disposez d'une grande grille, utilisez plusieurs types d'applications S3 ou souhaitez conserver toutes les données d'audit. Voir "Considérations relatives au serveur syslog externe" pour plus d'informations.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Maintenance ou autorisation d'accès racine".
- Si vous prévoyez de configurer un serveur syslog externe, vous avez consulté le "considérations relatives à l'utilisation d'un serveur syslog externe" et assurez-vous que le serveur dispose de suffisamment de capacité pour recevoir et stocker les fichiers journaux.
- Si vous prévoyez de configurer un serveur syslog externe à l'aide du protocole TLS ou RELP/TLS, vous disposez des certificats CA serveur et client requis et de la clé privée client.

Modifier les niveaux des messages d'audit

Vous pouvez définir un niveau d'audit différent pour chacune des catégories de messages suivantes dans le journal d'audit :

Catégorie de vérification	Paramètre par défaut	Plus d'informations
Système	Normale	"Messages d'audit système"
Stockage	Erreur	"Messages d'audit du stockage objet"
Gestion	Normale	"Message d'audit de gestion"
Lectures du client	Normale	"Messages d'audit de lecture du client"
Écritures des clients	Normale	"Écrire des messages d'audit client"
ILM	Normale	"Messages d'audit ILM"
Réplication entre plusieurs grilles	Erreur	"CGRR : demande de réplication croisée"

Ces valeurs par défaut s'appliquent si vous avez installé StorageGRID à l'origine à l'aide de la version 10.3 ou ultérieure. Si vous avez initialement utilisé une version antérieure de StorageGRID, la valeur par défaut pour toutes les catégories est Normal.

Durant les mises à niveau, les configurations des niveaux d'audit ne seront pas effectives immédiatement.

Étapes

1. Sélectionnez **CONFIGURATION** > **surveillance** > **serveur d'audit et syslog**.
2. Pour chaque catégorie de message d'audit, sélectionnez un niveau d'audit dans la liste déroulante :

Niveau d'audit	Description
Éteint	Aucun message d'audit de la catégorie n'est enregistré.
Erreur	Seuls les messages d'erreur sont consignés—les messages d'audit pour lesquels le code de résultat n'a pas été « réussi » (CMC).
Normale	Les messages transactionnels standard sont consignés—les messages répertoriés dans ces instructions pour la catégorie.

Niveau d'audit	Description
Débogage	Obsolète. Ce niveau se comporte de la même manière que le niveau d'audit normal.

Les messages inclus pour tout niveau particulier incluent ceux qui seraient consignés aux niveaux supérieurs. Par exemple, le niveau Normal inclut tous les messages d'erreur.

> Si vous n'avez pas besoin d'un enregistrement détaillé des opérations de lecture du client pour vos applications S3, vous pouvez éventuellement définir le paramètre **lecture du client** sur **erreur** pour diminuer le nombre de messages d'audit enregistrés dans le journal d'audit.

3. Sélectionnez **Enregistrer**.

   Une bannière verte indique que votre configuration a été enregistrée.

Définissez les en-têtes de requête HTTP

Vous pouvez éventuellement définir les en-têtes de requête HTTP que vous souhaitez inclure dans les messages d'audit de lecture et d'écriture du client. Ces en-têtes de protocole s'appliquent uniquement aux requêtes S3 et Swift.

Étapes

1. Dans la section **en-têtes de protocole d'audit**, définissez les en-têtes de requête HTTP que vous souhaitez inclure dans les messages d'audit de lecture et d'écriture du client.

   Utilisez un astérisque (*) comme caractère générique pour qu'il corresponde à zéro ou à plusieurs caractères. Utilisez la séquence d'échappement (*) pour faire correspondre un astérisque littéral.

2. Sélectionnez **Ajouter un autre en-tête** pour créer des en-têtes supplémentaires, si nécessaire.

   Lorsque des en-têtes HTTP sont trouvés dans une requête, ils sont inclus dans le message d'audit sous le champ HTRH.

   > Les en-têtes de requête de protocole d'audit ne sont consignés que si le niveau d'audit pour **lecture client** ou **écriture client** n'est pas **off**.

3. Sélectionnez **Enregistrer**

   Une bannière verte indique que votre configuration a été enregistrée.

utilisez un serveur syslog externe

Vous pouvez également configurer un serveur syslog externe pour enregistrer les journaux d'audit, les journaux d'application et les journaux d'événements de sécurité dans un emplacement en dehors de votre grille.

> Si vous ne souhaitez pas utiliser de serveur syslog externe, ignorez cette étape et passez à l' Sélectionnez les destinations des informations d'audit.

Si les options de configuration disponibles dans cette procédure ne sont pas suffisamment flexibles pour répondre à vos besoins, des options de configuration supplémentaires peuvent être appliquées à l'aide du `audit-destinations` Les terminaux, qui se trouvent dans la section API privée de "API de gestion du grid". Par exemple, vous pouvez utiliser l'API si vous souhaitez utiliser différents serveurs syslog pour différents groupes de nœuds.

Entrez les informations syslog

Accédez à l'assistant configurer le serveur syslog externe et fournissez les informations dont StorageGRID a besoin pour accéder au serveur syslog externe.

Étapes

1. Sur la page Audit and syslog Server, sélectionnez **Configure External syslog Server**. Ou, si vous avez déjà configuré un serveur syslog externe, sélectionnez **Modifier le serveur syslog externe**.

   L'assistant configurer le serveur syslog externe s'affiche.

2. Pour l'étape **Entrez les informations syslog** de l'assistant, entrez un nom de domaine complet valide ou une adresse IPv4 ou IPv6 pour le serveur syslog externe dans le champ **Host**.
3. Entrez le port de destination sur le serveur syslog externe (doit être un entier compris entre 1 et 65535). Le port par défaut est 514.
4. Sélectionnez le protocole utilisé pour envoyer les informations d'audit au serveur syslog externe.

   Il est recommandé d'utiliser **TLS** ou **RELP/TLS**. Vous devez télécharger un certificat de serveur pour utiliser l'une de ces options. L'utilisation de certificats permet de sécuriser les connexions entre votre grille et le serveur syslog externe. Pour plus d'informations, voir "Gérer les certificats de sécurité".

   Toutes les options de protocole requièrent la prise en charge par le serveur syslog externe ainsi que sa configuration. Vous devez choisir une option compatible avec le serveur syslog externe.

   Le protocole RELP (fiable Event Logging Protocol) étend la fonctionnalité du protocole syslog afin de fournir des messages d'événement fiables. L'utilisation de RELP peut aider à éviter la perte d'informations d'audit si votre serveur syslog externe doit redémarrer.

5. Sélectionnez **Continuer**.
6. si vous avez sélectionné **TLS** ou **RELP/TLS**, téléchargez les certificats de l'autorité de certification du serveur, le certificat du client et la clé privée du client.
   a. Sélectionnez **Parcourir** pour le certificat ou la clé que vous souhaitez utiliser.
   b. Sélectionnez le certificat ou le fichier de clé.
   c. Sélectionnez **Ouvrir** pour charger le fichier.

      Une coche verte s'affiche en regard du nom du fichier de certificat ou de clé, vous informant qu'il a été téléchargé avec succès.

7. Sélectionnez **Continuer**.

Gérer le contenu du journal système

Vous pouvez sélectionner les informations à envoyer au serveur syslog externe.

Étapes

1. Pour l'étape **gérer le contenu syslog** de l'assistant, sélectionnez chaque type d'informations d'audit que vous souhaitez envoyer au serveur syslog externe.

   - **Envoyer les journaux d'audit** : envoie les événements StorageGRID et les activités système
   - **Envoyer des événements de sécurité** : envoie des événements de sécurité tels qu'une tentative d'ouverture de session par un utilisateur non autorisé ou une ouverture de session par un utilisateur en tant que root
   - **Envoyer les journaux d'application** : envoie les fichiers journaux utiles pour le dépannage, notamment :
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` (Nœuds d'administration uniquement)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`

   Pour plus d'informations sur les journaux du logiciel StorageGRID, reportez-vous à la section "Journaux du logiciel StorageGRID".

2. Utilisez les menus déroulants pour sélectionner la gravité et l'établissement (type de message) pour chaque catégorie d'informations d'audit que vous souhaitez envoyer.

   La définition de la gravité et des valeurs de l'établissement peut vous aider à regrouper les journaux de manière personnalisable pour une analyse plus facile.

   a. Pour **gravité**, sélectionnez **passe-système** ou sélectionnez une valeur de gravité comprise entre 0 et 7.

      Si vous sélectionnez une valeur, la valeur sélectionnée sera appliquée à tous les messages de ce type. Les informations sur les différentes gravité seront perdues si vous remplacez la gravité par une valeur fixe.

Gravité	Description
Passe-système	Chaque message envoyé au syslog externe a la même valeur de gravité que lorsqu'il a été connecté localement au nœud : • Pour les journaux d'audit, la gravité est « info ». • Pour les événements de sécurité, les valeurs de gravité sont générées par la distribution Linux sur les nœuds. • Pour les journaux d'application, les niveaux de gravité varient entre « info » et « avis », selon le problème. Par exemple, l'ajout d'un serveur NTP et la configuration d'un groupe HA donnent la valeur « INFO », tandis que l'arrêt délibéré du service SSM ou RSM donne la valeur « notification ».
0	Urgence : le système est inutilisable

Gravité	Description
1	Alerte : une action doit être effectuée immédiatement
2	Critique : conditions critiques
3	Erreur : conditions d'erreur
4	Avertissement : conditions d'avertissement
5	Remarque : condition normale mais significative
6	Information : messages d'information
7	Débogage : messages de niveau débogage

b. Pour **facilty**, sélectionnez **Passthrough** ou sélectionnez une valeur d'installation comprise entre 0 et 23.

   Si vous sélectionnez une valeur, elle sera appliquée à tous les messages de ce type. Les informations concernant les différents sites seront perdues si vous remplacez l'établissement par une valeur fixe.

Installation	Description
Passe-système	Chaque message envoyé au syslog externe a la même valeur d'installation que lorsqu'il a été connecté localement au nœud : • Pour les journaux d'audit, la fonction envoyée au serveur syslog externe est « local7 ». • Pour les événements de sécurité, les valeurs d'installation sont générées par la distribution linux sur les nœuds. • Pour les journaux d'application, les journaux d'application envoyés au serveur syslog externe ont les valeurs suivantes : ◦ `bycast.log`: utilisateur ou démon ◦ `bycast-err.log`: utilisateur, démon, local3 ou local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6
0	kern (messages du noyau)
1	utilisateur (messages de niveau utilisateur)

Installation	Description
2	e-mail
3	démon (démons système)
4	auth (messages de sécurité/d'autorisation)
5	syslog (messages générés en interne par syslogd)
6	lpr (sous-système d'imprimante ligne)
7	news (sous-système d'informations réseau)
8	UCP
9	cron (démon d'horloge)
10	sécurité (messages de sécurité/d'autorisation)
11	FTP
12	NTP
13	audit journal (audit du journal)
14	alerte journal (alerte de journal)
15	horloge (démon d'horloge)
16	localis0
17	local1
18	localis2
19	local3
20	local4
21	local5
22	local6
23	localis7

3. Sélectionnez **Continuer**.

Envoyer des messages de test

Avant de commencer à utiliser un serveur syslog externe, vous devez demander à tous les nœuds de votre grille d'envoyer des messages de test au serveur syslog externe. Ces messages de test vous aideront à valider l'intégralité de votre infrastructure de collecte de journaux avant de vous engager à envoyer des données au serveur syslog externe.

> N'utilisez pas la configuration du serveur syslog externe tant que vous n'avez pas confirmé que le serveur syslog externe a reçu un message test de chaque nœud de votre grille et que le message a été traité comme prévu.

Étapes

1. Si vous ne souhaitez pas envoyer de messages de test parce que vous êtes certain que votre serveur syslog externe est correctement configuré et peut recevoir des informations d'audit de tous les nœuds de votre grille, sélectionnez **Ignorer et terminer**.

   Une bannière verte indique que la configuration a été enregistrée.

2. Sinon, sélectionnez **Envoyer les messages de test** (recommandé).

   Les résultats de test apparaissent en permanence sur la page jusqu'à ce que vous arrêiez le test. Pendant que le test est en cours, vos messages d'audit continuent d'être envoyés à vos destinations précédemment configurées.

3. Si vous recevez des erreurs, corrigez-les et sélectionnez à nouveau **Envoyer des messages de test**.

   Voir "Dépanner un serveur syslog externe" pour vous aider à résoudre toutes les erreurs.

4. Attendez qu'une bannière verte indique que tous les nœuds ont réussi le test.
5. Vérifiez votre serveur syslog pour déterminer si les messages de test sont reçus et traités comme prévu.

   > Si vous utilisez UDP, vérifiez l'ensemble de votre infrastructure de collecte de journaux. Le protocole UDP ne permet pas une détection d'erreur aussi rigoureuse que l'autre protocoles.

6. Sélectionnez **Arrêter et Terminer**.

   Vous revenez à la page **Audit and syslog Server**. Une bannière verte indique que la configuration du serveur syslog a été enregistrée.

   > Les informations d'audit StorageGRID ne sont pas envoyées au serveur syslog externe tant que vous ne sélectionnez pas une destination incluant le serveur syslog externe.

Sélectionnez les destinations des informations d'audit

Vous pouvez spécifier l'emplacement des journaux d'audit, les journaux d'événements de sécurité et "Journaux du logiciel StorageGRID" sont envoyés.

> Certaines destinations ne sont disponibles que si vous avez configuré un serveur syslog externe.

Étapes

1. Sur la page serveur d'audit et syslog, sélectionnez la destination des informations d'audit.

   Les nœuds locaux uniquement et **le serveur syslog externe** fournissent généralement de meilleures performances.

Option	Description
Nœuds locaux uniquement	Les messages d'audit, les journaux d'événements de sécurité et les journaux d'applications ne sont pas envoyés aux nœuds d'administration. Ils sont enregistrés uniquement sur les nœuds qui les ont générés (« le nœud local »). Les informations d'audit générées sur chaque nœud local sont stockées dans `/var/local/log/localaudit.log` **Remarque** : StorageGRID supprime périodiquement les journaux locaux dans une rotation pour libérer de l'espace. Lorsque le fichier journal d'un nœud atteint 1 Go, le fichier existant est enregistré et un nouveau fichier journal est démarré. La limite de rotation du journal est de 21 fichiers. Lorsque la 22e version du fichier journal est créée, le fichier journal le plus ancien est supprimé. En moyenne, environ 20 Go de données de journalisation sont stockés sur chaque nœud.
Nœuds d'administration/nœuds locaux	Les messages d'audit sont envoyés au journal d'audit (`/var/local/log/audit.log`) Sur les nœuds d'administration, les journaux d'événements de sécurité et les journaux d'applications sont stockés sur les nœuds qui les ont générés.
Serveur syslog externe	Les informations d'audit sont envoyées à un serveur syslog externe et enregistrées sur les nœuds locaux. Le type d'information envoyée dépend de la façon dont vous avez configuré le serveur syslog externe. Cette option n'est activée qu'après avoir configuré un serveur syslog externe.
Nœud d'administration et serveur syslog externe	Les messages d'audit sont envoyés au journal d'audit (`/var/local/log/audit.log`) Sur les nœuds d'administration, et les informations d'audit sont envoyées au serveur syslog externe et enregistrées sur le nœud local. Le type d'information envoyée dépend de la façon dont vous avez configuré le serveur syslog externe. Cette option n'est activée qu'après avoir configuré un serveur syslog externe.

2. Sélectionnez **Enregistrer**.

   Un message d'avertissement s'affiche.

3. Sélectionnez **OK** pour confirmer que vous souhaitez modifier la destination des informations d'audit.

   Une bannière verte indique que la configuration d'audit a été enregistrée.

   Les nouveaux journaux sont envoyés aux destinations que vous avez sélectionnées. Les journaux existants restent à leur emplacement actuel.