Surveillance des événements, des performances et de l'état du système

ONTAP 9

NetApp
April 13, 2024

Sommaire

Surveillance des événements, des performances et de l'état du système

Contrôle des performances du cluster avec System Manager

Contrôle des performances du cluster à l'aide de System Manager

Les sections de cette section permettent de gérer l'état et les performances des clusters à l'aide de System Manager dans ONTAP 9.7 et versions ultérieures.

Vous pouvez contrôler les performances du cluster en affichant les informations sur votre système dans le tableau de bord de System Manager. Le tableau de bord affiche des informations sur les alertes et notifications importantes, l'efficacité et la capacité des tiers et des volumes de stockage, les nœuds disponibles dans un cluster, l'état des nœuds d'une paire HA, les applications et objets les plus actifs, et les metrics de performance d'un cluster ou d'un nœud.

Le tableau de bord vous permet de déterminer les informations suivantes :

- **Santé**: La grappe est-elle saine?
- **Capacité** : quelle est la capacité disponible sur le cluster ?
- **Performance** : quel est le niveau de performances du cluster, en fonction de la latence, des IOPS et du débit ?
- **Network** : comment le réseau est-il configuré avec des hôtes et des objets de stockage, tels que des ports, des interfaces et des machines virtuelles de stockage ?

Dans les présentations Santé et capacité, vous pouvez cliquer sur → pour afficher des informations supplémentaires et effectuer des tâches.

Dans la vue d'ensemble des performances, vous pouvez afficher des mesures basées sur l'heure, le jour, la semaine, le mois ou l'année.

Dans la présentation réseau, le nombre de chaque objet du réseau est affiché (par exemple, « 8 ports NVMe/FC »). Vous pouvez cliquer sur les numéros pour afficher les détails de chaque objet réseau.

Affichez les performances sur le tableau de bord du cluster

Utilisez le tableau de bord pour prendre des décisions avisées sur les workloads à ajouter ou à déplacer. Vous pouvez également examiner les heures de pointe pour planifier les changements potentiels.

Les valeurs de performance sont renouvelées toutes les 3 secondes et le graphique de performances est actualisé toutes les 15 secondes.

Étapes

1. Cliquez sur **Tableau de bord**.
2. Sous **Performance**, sélectionnez l'intervalle.

Identification des volumes fortement sollicités et des autres objets

Accélérez les performances du cluster en identifiant les volumes (volumes fortement sollicités) et les données (objets fortement sollicités).

À partir de ONTAP 9.10.1, vous pouvez utiliser la fonction de suivi des activités de l'analyse du système de fichiers pour surveiller les objets actifs d'un volume.

Étapes

1. Cliquez sur **Storage > volumes**.
2. Filtrez les colonnes IOPS, latence et débit pour afficher les volumes et données fréquemment utilisés.

Modifier la QoS

À partir de ONTAP 9.8, lorsque vous provisionnez du stockage, Qualité de service (QoS) est activé par défaut. Vous pouvez désactiver QoS ou choisir une règle de qualité de services personnalisée lors du processus de provisionnement. Vous pouvez également modifier la QoS une fois le stockage provisionné.

Étapes

1. Dans System Manager, sélectionnez **Storage** puis **volumes**.
2. En regard du volume pour lequel vous souhaitez modifier la QoS, sélectionnez ⋮ Puis **Modifier**.

Surveiller les risques

Depuis ONTAP 9.10.0, System Manager permet de surveiller les risques signalés par le conseiller digital Active IQ. Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour prendre en compte les risques.

Le conseiller digital NetApp Active IQ crée des opportunités de réduction des risques et d'amélioration des performances et de l'efficacité de votre environnement de stockage. Avec System Manager, vous découvrez les risques signalés par Active IQ et bénéficiez d'informations exploitables pour la gestion du stockage, une disponibilité accrue, une sécurité renforcée et des performances de stockage supérieures.

Lien vers votre compte Active IQ

Pour recevoir des informations sur les risques Active IQ, vous devez d'abord créer un lien vers votre compte Active IQ de System Manager.

Étapes

1. Dans System Manager, cliquez sur **Cluster > Paramètres**.
2. Sous **Active IQ Registration**, cliquez sur **Register**.
3. Saisissez vos identifiants pour Active IQ.
4. Une fois vos informations d'identification authentifiées, cliquez sur **confirmer pour lier Active IQ à System Manager**.

Afficher le nombre de risques

Depuis ONTAP 9.10.0, vous pouvez consulter le tableau de bord dans System Manager le nombre de risques signalé par Active IQ.

Avant de commencer

Vous devez établir une connexion depuis System Manager vers votre compte Active IQ. Reportez-vous à la section Lien vers votre compte Active IQ.

Étapes

1. Dans System Manager, cliquez sur **Dashboard**.
2. Dans la section **Santé**, consultez le nombre de risques signalés.

> Vous pouvez afficher des informations plus détaillées sur chaque risque en cliquant sur le message indiquant le nombre de risques. Voir Afficher les détails des risques.

Afficher les détails des risques

Depuis ONTAP 9.10.0, vous pouvez visualiser dans System Manager la façon dont les risques signalés par Active IQ sont classés par zone d'impact. Vous pouvez également consulter des informations détaillées sur chaque risque signalé, son impact potentiel sur votre système et les actions correctives que vous pouvez prendre.

Avant de commencer

Vous devez établir une connexion depuis System Manager vers votre compte Active IQ. Reportez-vous à la section Lien vers votre compte Active IQ.

Étapes

1. Cliquez sur **Evénements > tous les événements**.
2. Dans la section **Aperçu**, sous **suggestions de Active IQ**, consultez le nombre de risques dans chaque catégorie de zone d'impact. Les catégories de risque sont les suivantes :
   - Performances et efficacité
   - Disponibilité et protection des données
   - Puissance
   - Configuration
   - Sécurité
3. Cliquez sur l'onglet **suggestions** de Active IQ pour afficher des informations sur chaque risque, notamment :
   - Niveau d'impact sur votre système
   - Catégorie du risque
   - Nœuds affectés
   - Type d'atténuation nécessaire
   - Actions correctives possibles

Reconnaître les risques

À partir de ONTAP 9.10.1, vous pouvez utiliser System Manager pour prendre en compte les risques ouverts.

Étapes

1. Dans System Manager, affichez la liste des risques en exécutant la procédure dans Afficher les détails des risques.
2. Cliquez sur le nom du risque d'un risque ouvert que vous souhaitez reconnaître.
3. Entrez les informations dans les champs suivants :
   - Rappel (date)
   - Justification
   - Commentaires
4. Cliquez sur **Acknowledge**.

> Une fois que vous avez reconnu un risque, ce changement ne prend que quelques minutes et se reflète dans la liste des suggestions de Active IQ.

Prendre en compte les risques

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour annuler le risque reconnu précédemment.

Étapes

1. Dans System Manager, affichez la liste des risques en exécutant la procédure dans Afficher les détails des risques.
2. Cliquez sur le nom du risque d'un risque reconnu que vous souhaitez annuler.
3. Entrez les informations dans les champs suivants :
   - Justification
   - Commentaires
4. Cliquez sur **UnAcknowledge**.

> Une fois que vous reconnaissez un risque, ce changement prend quelques minutes. Il faut que ce changement soit reflété dans la liste des suggestions de Active IQ.

Informations sur System Manager

Depuis ONTAP 9.11.1, System Manager affiche *Insights* qui vous aide à optimiser les performances et la sécurité de votre système.

> Pour afficher, personnaliser et répondre aux informations, reportez-vous à la section "Obtenez des informations exploitables pour optimiser votre système"

Informations sur la capacité

System Manager peut afficher les informations suivantes en fonction des conditions de capacité de votre système :

Visibilité	Gravité	Condition	Correctifs
Les tiers locaux manquent d'espace	Remédier aux risques	Un ou plusieurs niveaux locaux sont pleins à plus de 95 % et connaissent une croissance rapide. Il se peut que les workloads existants ne puissent pas croître ou, dans des cas extrêmes, que l'espace disponible des workloads existants soit insuffisant pour échouer.	**Correctif recommandé** : effectuez l'une des options suivantes. • Effacez la file d'attente de restauration du volume. • Activez le provisionnement fin sur des volumes à provisionnement lourd pour libérer du stockage piégé. • Déplacez les volumes vers un autre niveau local. • Supprimer les copies Snapshot inutiles • Supprimez les répertoires ou fichiers inutiles des volumes. • Activez FabricPool pour hiérarchiser les données dans le cloud.
Et l'espace est insuffisant pour les applications	A besoin d'attention	Un ou plusieurs volumes sont remplis à plus de 95 %, mais leur croissance automatique n'est pas activée.	**Recommandé** : activez la croissance automatique jusqu'à 150 % de la capacité actuelle. **Autres options** : • Pour gagner de l'espace, supprimez les copies Snapshot. • Redimensionner les volumes. • Supprimez des répertoires ou des fichiers.
La capacité du volume FlexGroup est déséquilibrée	Optimisez le stockage	La taille des volumes constitutifs d'un ou plusieurs volumes FlexGroup a augmenté de façon inégale au fil du temps, entraînant un déséquilibre dans l'utilisation de la capacité. Si les volumes constitutifs sont pleins, des défaillances d'écriture peuvent se produire.	**Recommandé** : rééquilibrer les volumes FlexGroup.

Les machines virtuelles de stockage sont à court de capacité	Optimisez le stockage	Une ou plusieurs machines virtuelles de stockage sont proches de leur capacité maximale. Vous ne pourrez pas provisionner davantage d'espace pour les volumes nouveaux ou existants si les VM de stockage atteignent leur capacité maximale.	**Recommandé** : si possible, augmentez la limite de capacité maximale de la machine virtuelle de stockage.

Informations de sécurité

System Manager peut afficher les informations suivantes en réponse à des conditions susceptibles de compromettre la sécurité de vos données ou de votre système.

Visibilité	Gravité	Condition	Correctifs
Les volumes sont toujours en mode de formation anti-ransomware	A besoin d'attention	Un ou plusieurs volumes sont en mode de formation anti-ransomware depuis 90 jours.	**Recommandé** : activez le mode actif anti-ransomware pour ces volumes.
La suppression automatique des copies Snapshot est activée sur les volumes	A besoin d'attention	La suppression automatique des snapshots est activée sur un ou plusieurs volumes.	**Recommandé** : désactivez la suppression automatique des copies Snapshot. Sinon, en cas d'attaque par ransomware, il n'est pas toujours possible de restaurer les données de ces volumes.
Les volumes n'ont pas de règles Snapshot	A besoin d'attention	Une règle Snapshot adéquate n'est pas associée à un ou plusieurs volumes.	**Recommandé** : rattachez une règle Snapshot à des volumes qui n'en ont pas. Sinon, en cas d'attaque par ransomware, il n'est pas toujours possible de restaurer les données de ces volumes.
FPolicy natif n'est pas configuré	Et des meilleures pratiques	Le système natif FPolicy n'est pas configuré sur une ou plusieurs machines virtuelles de stockage NAS.	**Recommandé**: **IMPORTANT**: Le blocage des extensions peut entraîner des résultats inattendus. À partir de la version 9.11.1, vous pouvez activer la fonctionnalité FPolicy native pour les machines virtuelles de stockage, qui bloque plus de 3000 extensions de fichier connues pour être utilisées dans le cadre d'attaques par ransomware. "Configuration de FPolicy natif" Dans les machines virtuelles de stockage NAS pour contrôler les extensions de fichiers qui sont autorisées ou non à être écrites sur des volumes de votre environnement.

Telnet est activé	Et des meilleures pratiques	Secure Shell (SSH) doit être utilisé pour sécuriser l'accès à distance.	**Recommandé** : désactivez Telnet et utilisez SSH pour un accès distant sécurisé.
Trop peu de serveurs NTP sont configurés	Et des meilleures pratiques	Le nombre de serveurs configurés pour NTP est inférieur à 3.	**Recommandé** : associez au moins trois serveurs NTP au cluster. Sinon, des problèmes peuvent se produire lors de la synchronisation de l'heure du cluster.
Le shell distant (RSH) est activé	Et des meilleures pratiques	Secure Shell (SSH) doit être utilisé pour sécuriser l'accès à distance.	**Recommandé** : désactivez RSH et utilisez SSH pour un accès distant sécurisé.
La bannière de connexion n'est pas configurée	Et des meilleures pratiques	Les messages de connexion ne sont pas configurés ni pour le cluster, ni pour la machine virtuelle de stockage, ni pour les deux.	**Recommandé** : configurez les bannières de connexion pour le cluster et la machine virtuelle de stockage et activez leur utilisation.
AutoSupport utilise un protocole non sécurisé	Et des meilleures pratiques	AutoSupport n'est pas configuré pour communiquer via HTTPS.	**Recommandé** : il est fortement recommandé d'utiliser HTTPS comme protocole de transport par défaut pour envoyer des messages AutoSupport au support technique.
L'utilisateur admin par défaut n'est pas verrouillé	Et des meilleures pratiques	Personne n'a ouvert de session à l'aide d'un compte d'administration par défaut (admin ou diag), et ces comptes ne sont pas verrouillés.	**Recommandé**: Verrouiller les comptes d'administration par défaut lorsqu'ils ne sont pas utilisés.
Secure Shell (SSH) utilise des chiffrements non sécurisés	Et des meilleures pratiques	La configuration actuelle utilise des chiffrements CBC non sécurisés.	**Recommandé**: Vous devez autoriser uniquement les chiffrements sécurisés sur votre serveur Web pour protéger les communications sécurisées avec vos visiteurs. Supprimer les chiffriers qui ont des noms contenant "cbc", tels que "ais128-cbc", "aes192-cbc", "aes256-cbc" et "3des-cbc".
La conformité à la norme FIPS 140-2 globale est désactivée	Et des meilleures pratiques	La conformité à la norme FIPS 140-2 est désactivée sur le cluster.	**Recommandé** : pour des raisons de sécurité, vous devez activer la cryptographie conforme à la norme FIPS 140-2 pour garantir que ONTAP peut communiquer en toute sécurité avec des clients externes ou des clients serveur.

Les attaques par ransomware ne font pas l'objet d'une surveillance des volumes	A besoin d'attention	La protection contre les ransomware est désactivée sur un ou plusieurs volumes.	**Recommandé** : activez la protection contre les ransomware sur les volumes. Sinon, vous ne remarquerez peut-être pas si des volumes sont menacés ou en cours d'attaque.
Les machines virtuelles de stockage ne sont pas configurées pour lutter contre les ransomware	Et des meilleures pratiques	Une ou plusieurs machines virtuelles de stockage ne sont pas configurées pour la protection contre les ransomware.	**Recommandé** : activez la protection contre les ransomware sur les machines virtuelles de stockage. Sinon, vous ne remarquerez peut-être pas la menace ou l'attaque des machines virtuelles de stockage.

Informations de configuration

System Manager peut afficher les informations suivantes en réponse à des problèmes de configuration de votre système.

Visibilité	Gravité	Condition	Correctifs
Le cluster n'est pas configuré pour les notifications	Et des meilleures pratiques	Les e-mails, les webhooks ou les traphost SNMP ne sont pas configurés pour vous permettre de recevoir des notifications sur les problèmes rencontrés avec le cluster.	**Recommandé** : configurer les notifications pour le cluster.
Le cluster n'est pas configuré pour les mises à jour automatiques.	Et des meilleures pratiques	Le cluster n'a pas été configuré pour recevoir les mises à jour automatiques des derniers fichiers de qualification de disque, de firmware de disque, de firmware de tiroir et de firmware SP/BMC lorsqu'ils sont disponibles.	**Recommandé** : activez cette fonction.

Le firmware du cluster n'est pas à jour	Et des meilleures pratiques	Votre système ne dispose pas de la dernière mise à jour du micrologiciel qui pourrait avoir des améliorations, des correctifs de sécurité ou de nouvelles fonctionnalités qui aident à sécuriser le cluster pour de meilleures performances.	**Recommandé** : mettre à jour le micrologiciel ONTAP.

Obtenez des informations exploitables pour optimiser votre système

Avec System Manager, vous pouvez afficher des informations exploitables qui vous aident à optimiser votre système.

Description de la tâche

Depuis ONTAP 9.11.0, vous pouvez voir une vue d'ensemble de System Manager qui vous aide à optimiser la capacité et la conformité de sécurité de votre système.

Depuis ONTAP 9.11.1, vous pouvez afficher des informations supplémentaires pour optimiser la capacité, la conformité de sécurité et la configuration de votre système.

Le blocage des extensions peut entraîner des résultats inattendus. à partir de ONTAP 9.11.1, vous pouvez activer FPolicy natif pour les machines virtuelles de stockage à l'aide de System Manager. Il se peut que vous receviez un message System Manager Insight vous recommandant "Configuration de FPolicy natif" Pour une VM de stockage.

Avec le mode natif FPolicy, vous pouvez autoriser ou interdire des extensions de fichiers spécifiques. System Manager recommande plus de 3000 extensions de fichiers interdites utilisées dans les attaques par ransomware précédentes. Certaines de ces extensions peuvent être utilisées par des fichiers légitimes dans votre environnement et leur blocage peut entraîner des problèmes inattendus.

Par conséquent, il est fortement conseillé de modifier la liste des extensions pour répondre aux besoins de votre environnement. Reportez-vous à la section "Comment supprimer une extension de fichier d'une configuration FPolicy native créée par System Manager à l'aide de System Manager pour recréer la règle".

Pour en savoir plus sur FPolicy natif, reportez-vous à la section "Types de configuration FPolicy".

En fonction des meilleures pratiques, ces informations sont affichées sur une page à partir de laquelle vous pouvez lancer des actions immédiates pour optimiser votre système. Pour plus de détails sur chaque information, reportez-vous à la section "Informations sur System Manager".

Affichez les informations exploitables concernant l'optimisation

Étapes

1. Dans System Manager, cliquez sur **Insights** dans la colonne de navigation de gauche.

   La page **Insights** affiche des groupes de vues. Chaque groupe d'informations peut contenir une ou plusieurs informations. Les groupes suivants sont affichés :

   - A votre attention
   - Remédier aux risques
   - Optimisez le stockage

2. (Facultatif) filtrez les informations affichées en cliquant sur ces boutons dans le coin supérieur droit de la page :

   -  Affiche les informations relatives à la sécurité.
   -  Affiche les informations relatives à la capacité.
   -  Affiche les informations relatives à la configuration.
   -  Affiche toutes les informations.

Répondez aux informations exploitables pour optimiser votre système

Dans System Manager, vous pouvez répondre à des analyses en les rejetant, en explorant différentes façons de résoudre les problèmes ou en initiant le processus pour les résoudre.

Étapes

1. Dans System Manager, cliquez sur **Insights** dans la colonne de navigation de gauche.
2. Passez le curseur sur un aperçu pour afficher les boutons permettant d'effectuer les opérations suivantes :
   - **Rejeter** : supprimez l'aperçu de la vue. Pour « rejeter » les avis, reportez-vous à [customize-settings-insights].
   - **Explorer**: Découvrez différentes façons de résoudre le problème mentionné dans la perspicacité. Ce bouton apparaît uniquement si plusieurs méthodes de correction sont possibles.
   - **Fix** : lancer le processus de résolution du problème mentionné dans l'InSight. Il vous sera demandé de confirmer si vous souhaitez prendre les mesures nécessaires pour appliquer le correctif.

> Certaines de ces actions peuvent être lancées à partir d'autres pages de System Manager, mais la page **Insights** vous aide à rationaliser vos tâches quotidiennes en vous permettant de lancer ces actions à partir de cette page.

Personnalisez les paramètres pour obtenir des informations exploitables

Vous pouvez personnaliser les informations dont vous recevrez des notifications dans System Manager.

Étapes

1. Dans System Manager, cliquez sur **Insights** dans la colonne de navigation de gauche.

2. Dans le coin supérieur droit de la page, cliquez sur ⋮, Puis sélectionnez **Paramètres**.
3. Sur la page **Paramètres**, assurez-vous que les cases à cocher situées en regard des informations que vous souhaitez en être averti. Si vous avez précédemment rejeté une idée, vous pouvez la « rejeter » en vous assurant qu'une case à cocher est cochée.
4. Cliquez sur **Enregistrer**.

Exportez les informations sous forme de fichier PDF

Vous pouvez exporter toutes les informations applicables sous forme de fichier PDF.

Étapes

1. Dans System Manager, cliquez sur **Insights** dans la colonne de navigation de gauche.
2. Dans le coin supérieur droit de la page, cliquez sur ⋮, Puis sélectionnez **Exporter**.

Configuration de FPolicy natif

Depuis ONTAP 9.11.1, lorsque vous recevez une vue System Manager qui suggère d'implémenter FPolicy natif, vous pouvez la configurer sur vos machines virtuelles et volumes de stockage.

Avant de commencer

Lorsque vous accédez à System Manager Insights, sous **appliquer les meilleures pratiques**, vous pouvez recevoir un message indiquant que FPolicy natif n'est pas configuré.

Pour en savoir plus sur les types de configuration FPolicy, reportez-vous à la section "Types de configuration FPolicy".

Étapes

1. Dans System Manager, cliquez sur **Insights** dans la colonne de navigation de gauche.
2. Sous **appliquer les meilleures pratiques**, localisez **le système natif FPolicy n'est pas configuré**.
3. Lisez le message suivant avant de prendre des mesures :

> **Le blocage des extensions peut entraîner des résultats inattendus.** à partir de ONTAP 9.11.1, vous pouvez activer FPolicy natif pour les machines virtuelles de stockage à l'aide de System Manager.
> Avec le mode natif FPolicy, vous pouvez autoriser ou interdire des extensions de fichiers spécifiques. System Manager recommande plus de 3000 extensions de fichiers interdites utilisées dans les attaques par ransomware précédentes. Certaines de ces extensions peuvent être utilisées par des fichiers légitimes dans votre environnement et leur blocage peut entraîner des problèmes inattendus.
>
> Par conséquent, il est fortement conseillé de modifier la liste des extensions pour répondre aux besoins de votre environnement. Reportez-vous à la section "Comment supprimer une extension de fichier d'une configuration FPolicy native créée par System Manager à l'aide de System Manager pour recréer la règle".

4. Cliquez sur **fixer**.
5. Sélectionnez les machines virtuelles de stockage auxquelles vous souhaitez appliquer la fonctionnalité FPolicy native.

6. Pour chaque VM de stockage, sélectionnez les volumes qui recevront la FPolicy native.
7. Cliquez sur **configurer**.

Contrôlez et gérez les performances du cluster à l'aide de l'interface de ligne de commandes

Contrôle des performances et présentation de la gestion

Vous pouvez également définir des tâches de base de contrôle et de gestion des performances, et identifier et résoudre des problèmes courants de performance.

Vous pouvez utiliser ces procédures pour contrôler et gérer les performances du cluster si les hypothèses suivantes s'appliquent à votre situation :

- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.
- Vous pouvez afficher l'état du système et les alertes, surveiller les performances du cluster et effectuer une analyse de la source des problèmes à l'aide de Active IQ Unified Manager (anciennement OnCommand Unified Manager) en plus de l'interface de ligne de commandes de ONTAP.
- Vous utilisez l'interface de ligne de commandes ONTAP pour configurer la qualité de service (QoS) du stockage.

  La QoS est également disponible dans System Manager, NSLM, WFA, VSC (plug-in VMware) et les API.
- Vous souhaitez installer Unified Manager à l'aide d'une appliance virtuelle au lieu d'une installation Linux ou Windows.
- Vous êtes prêt à utiliser une configuration statique plutôt que DHCP pour installer le logiciel.
- Vous pouvez accéder aux commandes ONTAP au niveau de privilège avancé.
- Vous êtes un administrateur de cluster ayant le rôle « admin ».

Informations associées

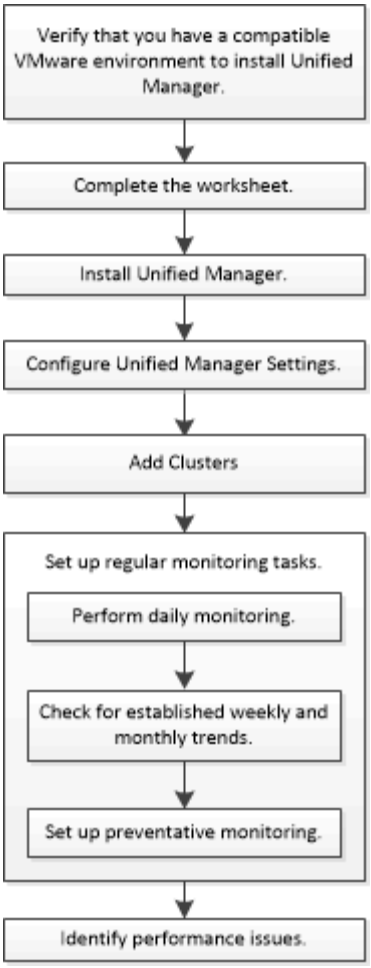
Si ces hypothèses ne sont pas correctes pour votre situation, vous devez consulter les ressources suivantes :

- "Installation de Active IQ Unified Manager 9.8"
- "Administration du système"

Contrôle des performances

Présentation du workflow de surveillance des performances et de maintenance

Le contrôle et la maintenance des performances du cluster impliquent l'installation du logiciel Active IQ Unified Manager, la configuration des tâches de surveillance de base, l'identification des problèmes de performances et les ajustements nécessaires.



Vérifiez que votre environnement VMware est pris en charge

Pour installer correctement Active IQ Unified Manager, vous devez vérifier que votre environnement VMware répond aux exigences requises.

Étapes

1. Vérifiez que votre infrastructure VMware répond aux exigences de dimensionnement pour l'installation de Unified Manager.
2. Accédez au "Matrice d'interopérabilité" pour vérifier que vous disposez d'une combinaison prise en charge des composants suivants :
   - Version ONTAP
   - Version du système d'exploitation ESXi
   - Version de VMware vCenter Server
   - Version des outils VMware
   - Type et version du navigateur

   Le "Matrice d'interopérabilité" Le répertorie les configurations prises en charge pour Unified Manager.
3. Cliquez sur le nom de la configuration sélectionnée.

   Les détails de cette configuration s'affichent dans la fenêtre Détails de la configuration.

4. Vérifiez les informations dans les onglets suivants :
    - Remarques

      Le répertorie les alertes et informations importantes spécifiques à votre configuration.

    - Politiques et lignes directrices

      Présente des recommandations d'ordre général pour toutes les configurations.

Fiche technique Active IQ Unified Manager

Avant d'installer, de configurer et de connecter Active IQ Unified Manager, vous devez disposer facilement d'informations spécifiques sur votre environnement. Vous pouvez enregistrer les informations dans la fiche.

Informations sur l'installation de Unified Manager

Machine virtuelle sur laquelle le logiciel est déployé	Votre valeur
Adresse IP du serveur ESXi	
Nom de domaine complet de l'hôte	
Adresse IP de l'hôte	
Masque de réseau	
Adresse IP de la passerelle	
Adresse DNS principale	
Adresse DNS secondaire	
Domaines de recherche	
Nom d'utilisateur de maintenance	
Mot de passe utilisateur de maintenance	

Informations sur la configuration de Unified Manager

Réglage	Votre valeur
Adresse e-mail de l'utilisateur de maintenance	
Serveur NTP	

Nom d’hôte ou adresse IP du serveur SMTP	
Nom d’utilisateur SMTP	
Mot de passe SMTP	
Port SMTP par défaut	25 (valeur par défaut)
E-mail à partir duquel les notifications d’alerte sont envoyées	
Nom distinctif de la liaison LDAP	
Mot de passe de liaison LDAP	
Nom d’administrateur Active Directory	
Mot de passe Active Directory	
Nom distinctif de la base du serveur d’authentification	
Nom d’hôte ou adresse IP du serveur d’authentification	

Informations sur le cluster

Capturer les informations suivantes pour chaque cluster sur Unified Manager.

Cluster 1 de N	Votre valeur
Nom d’hôte ou adresse IP de gestion du cluster	
Nom d’utilisateur de l’administrateur ONTAP L’administrateur doit avoir reçu le rôle « admin ».	
Mot de passe administrateur ONTAP	
Protocole (HTTP ou HTTPS)	

Informations associées

"Authentification de l’administrateur et RBAC"

Installez Active IQ Unified Manager

Téléchargez et déployez Active IQ Unified Manager

Pour installer le logiciel, vous devez télécharger le fichier d'installation de l'appliance virtuelle (va), puis utiliser un client VMware vSphere pour déployer le fichier sur un serveur VMware ESXi. Le va est disponible dans un fichier OVA.

Étapes

1. Accédez à la page **NetApp support site Software Download** (Téléchargement de logiciels) et recherchez Active IQ Unified Manager.

   https://mysupport.netapp.com/products/index.html

2. Sélectionnez **VMware vSphere** dans le menu déroulant **Select Platform** et cliquez sur **Go!**
3. Enregistrez le fichier « OVA » dans un emplacement local ou réseau accessible à votre client VMware vSphere.
4. Dans VMware vSphere client, cliquez sur **fichier** > **déployer le modèle OVF**.
5. Localisez le fichier « OVA » et utilisez l'assistant pour déployer l'appliance virtuelle sur le serveur ESXi.

   Vous pouvez utiliser l'onglet **Propriétés** de l'assistant pour saisir vos informations de configuration statique.

6. Mise sous tension de la machine virtuelle
7. Cliquez sur l'onglet **Console** pour afficher le processus de démarrage initial.
8. Suivez l'invite pour installer VMware Tools sur la machine virtuelle.
9. Configurer le fuseau horaire.
10. Entrez un nom d'utilisateur et un mot de passe de maintenance.
11. Accédez à l'URL affichée par la console de la machine virtuelle.

Configurez les paramètres Active IQ Unified Manager initiaux

La boîte de dialogue Configuration initiale du Active IQ Unified Manager s'affiche lorsque vous accédez pour la première fois à l'interface utilisateur Web, qui vous permet de configurer certains paramètres initiaux et d'ajouter des clusters.

Étapes

1. Acceptez le paramètre AutoSupport activé par défaut.
2. Entrez les détails du serveur NTP, l'adresse e-mail de l'utilisateur de maintenance, le nom d'hôte du serveur SMTP et les options SMTP supplémentaires, puis cliquez sur **Enregistrer**.

Une fois que vous avez terminé

Une fois la configuration initiale terminée, la page sources de données du cluster s'affiche, dans laquelle vous pouvez ajouter les détails du cluster.

Spécifiez les clusters à surveiller

Vous devez ajouter un cluster à un serveur Active IQ Unified Manager pour surveiller le

cluster, afficher l'état de détection du cluster et contrôler ses performances.

Ce dont vous avez besoin

- Vous devez disposer des informations suivantes :
  - Nom d'hôte ou adresse IP de gestion du cluster

    Le nom d'hôte est le nom de domaine complet (FQDN) ou le nom court que Unified Manager utilise pour se connecter au cluster. Ce nom d'hôte doit être résolu sur l'adresse IP de gestion du cluster.

  L'adresse IP de gestion du cluster doit être la LIF de gestion du cluster du serveur virtuel de stockage administratif (SVM). Si vous utilisez une LIF node-management, l'opération échoue.

  - Nom d'utilisateur et mot de passe de l'administrateur ONTAP
  - Type de protocole (HTTP ou HTTPS) pouvant être configuré sur le cluster et le numéro de port du cluster
- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- L'administrateur ONTAP doit disposer des rôles d'administrateur ONTAPI et SSH.
- Le FQDN de Unified Manager doit pouvoir exécuter ONTAP.

  Vous pouvez le vérifier à l'aide de la commande ONTAP `ping -node` *`node_name`* `-destination` *`Unified_Manager_FQDN`*.

Description de la tâche

Dans le cas d'une configuration MetroCluster, vous devez ajouter les clusters locaux et distants, et les clusters doivent être configurés correctement.

Étapes

1. Cliquez sur **Configuration** > **sources de données de cluster**.
2. Sur la page clusters, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un cluster**, spécifiez les valeurs requises, telles que le nom d'hôte ou l'adresse IP (IPv4 ou IPv6) du cluster, le nom d'utilisateur, le mot de passe, le protocole de communication et le numéro de port.

   Par défaut, le protocole HTTPS est sélectionné.

   Vous pouvez modifier l'adresse IP de gestion du cluster d'IPv6 au format IPv4 ou d'IPv4 à IPv6. La nouvelle adresse IP est reflétée dans la grille du cluster et la page de configuration du cluster, une fois le cycle de surveillance suivant terminé.
4. Cliquez sur **Ajouter**.
5. Si HTTPS est sélectionné, effectuez les opérations suivantes :
   a. Dans la boîte de dialogue **Authorise Host** , cliquez sur **View Certificate** pour afficher les informations de certificat relatives au cluster.
   b. Cliquez sur **Oui**.

      Unified Manager vérifie le certificat uniquement lors de l'ajout initial du cluster, mais ne le vérifie pas pour chaque appel d'API à ONTAP.

Si le certificat a expiré, vous ne pouvez pas ajouter le cluster. Vous devez renouveler le certificat SSL, puis ajouter le cluster.

6. **Facultatif** : affichez l'état de la détection du cluster :

   a. Vérifiez l'état de la détection du cluster à partir de la page **Configuration du cluster**.

   Le cluster est ajouté à la base de données Unified Manager après l'intervalle de contrôle par défaut d'environ 15 minutes.

Configurer les tâches de surveillance de base

Effectuer un contrôle quotidien

Vous pouvez effectuer une surveillance quotidienne afin de vous assurer que vous n'avez aucun problème de performance immédiat à laquelle vous devez vous préoccuper.

Étapes

1. Dans l'interface utilisateur Active IQ Unified Manager, accédez à la page **Inventaire des événements** pour afficher tous les événements actuels et obsolètes.
2. Dans l'option **View**, sélectionnez `Active Performance Events` et déterminer quelle action est nécessaire.

Utilisez les tendances de performances hebdomadaires et mensuelles pour identifier les problèmes de performances

L'identification des tendances de performances permet de déterminer si le cluster est sur-utilisé ou sous-utilisé en analysant la latence du volume. Vous pouvez utiliser des étapes similaires pour identifier les goulets d'étranglement du processeur, du réseau ou d'autres systèmes.

Étapes

1. Identifiez le volume que vous pensez être sous-utilisé ou sur-utilisé.
2. Dans l'onglet **Détails du volume**, cliquez sur **30 d** pour afficher les données historiques.
3. Dans le menu déroulant « données de pause par », sélectionnez **latence**, puis cliquez sur **Envoyer**.
4. Désélectionnez **agrégat** dans le tableau comparatif des composants du cluster, puis comparez la latence du cluster avec celle du tableau de latence du volume.
5. Sélectionnez **agrégat** et désélectionnez tous les autres composants dans le tableau comparatif des composants du cluster, puis comparez la latence globale avec celle du graphique de latence du volume.
6. Comparez le graphique de latence de lecture/écriture sur le tableau de latence du volume.
7. Identifiez si les charges d'application client ont provoqué des conflits au niveau de la charge de travail et rééquilibrez les charges de travail en fonction des besoins.
8. Déterminez si l'agrégat est sur-utilisé et source de conflits, et rééquilibrez les charges de travail si nécessaire.

Utilisez des seuils de performances pour générer des notifications d'événements

Les événements sont des notifications que la Active IQ Unified Manager génère automatiquement lorsqu'une condition prédéfinie se produit ou lorsqu'une valeur de compteur de performances franchit un seuil. Les événements vous aident à identifier les

problèmes de performance dans les clusters que vous surveillez. Vous pouvez configurer des alertes pour envoyer automatiquement une notification par e-mail lorsque des événements de certains types de gravité se produisent.

Définissez des seuils de performances

Vous pouvez définir des seuils de performance pour contrôler les problèmes de performance stratégiques. Des seuils définis par l'utilisateur déclenchent une notification d'avertissement ou d'événement critique lorsque le système approche ou dépasse le seuil défini.

Étapes

1. Créez les seuils d'avertissement et d'événement critique :
   a. Sélectionnez **Configuration** > **seuils de performances**.
   b. Cliquez sur **Créer**.
   c. Sélectionnez le type d'objet et spécifiez un nom et une description de la règle.
   d. Sélectionnez la condition de compteur d'objets et spécifiez les valeurs limites qui définissent les événements Avertissement et critique.
   e. Sélectionnez la durée pendant laquelle les valeurs limites doivent être enfreintes pour un événement à envoyer, puis cliquez sur **Enregistrer**.
2. Attribuez la politique de seuil à l'objet de stockage.
   a. Accédez à la page Inventaire pour le même type d'objet de cluster que vous avez précédemment sélectionné et choisissez **Performance** dans l'option Afficher.
   b. Sélectionnez l'objet auquel vous souhaitez affecter la stratégie de seuil, puis cliquez sur **affecter stratégie de seuil**.
   c. Sélectionnez la stratégie que vous avez créée précédemment, puis cliquez sur **affecter stratégie**.

Exemple

Vous pouvez définir des seuils définis par l'utilisateur pour en savoir plus sur les problèmes de performance stratégiques. Par exemple, si vous disposez d'un serveur Microsoft Exchange et que vous savez qu'il tombe en panne si la latence du volume dépasse 20 millisecondes, vous pouvez définir un seuil d'avertissement à 12 millisecondes et un seuil critique à 15 millisecondes. Avec ce paramètre de seuil, vous pouvez recevoir des notifications lorsque la latence du volume dépasse la limite.

Ajouter des alertes

Vous pouvez configurer des alertes pour vous avertir lorsqu'un événement particulier est généré. Vous pouvez configurer les alertes pour une seule ressource, pour un groupe de ressources ou pour les événements d'un type de sévérité particulier. Vous pouvez spécifier la fréquence à laquelle vous souhaitez être averti et associer un script à l'alerte.

Ce dont vous avez besoin

- Vous devez avoir configuré des paramètres de notification tels que l'adresse e-mail de l'utilisateur, le

serveur SMTP et l'hôte d'interruption SNMP pour permettre au serveur Active IQ Unified Manager d'utiliser ces paramètres pour envoyer des notifications aux utilisateurs lorsqu'un événement est généré.

- Vous devez connaître les ressources et les événements pour lesquels vous souhaitez déclencher l'alerte, ainsi que les noms d'utilisateur ou adresses e-mail des utilisateurs que vous souhaitez notifier.
- Si vous souhaitez que le script soit exécuté en fonction de l'événement, vous devez l'avoir ajouté à Unified Manager à l'aide de la page scripts.
- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Description de la tâche

Vous pouvez créer une alerte directement à partir de la page Détails de l'événement après avoir reçu un événement en plus de créer une alerte à partir de la page Configuration de l'alerte, comme décrit ici.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.
2. Dans la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom**, puis entrez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources**, puis sélectionnez les ressources à inclure ou à exclure de l'alerte.

   Vous pouvez définir un filtre en spécifiant une chaîne de texte dans le champ **Nom contient** pour sélectionner un groupe de ressources. En fonction de la chaîne de texte que vous spécifiez, la liste des ressources disponibles n'affiche que les ressources qui correspondent à la règle de filtre. La chaîne de texte que vous spécifiez est sensible à la casse.

   Si une ressource est conforme à la fois aux règles inclure et exclure que vous avez spécifiées, la règle d'exclusion est prioritaire sur la règle inclure et l'alerte n'est pas générée pour les événements liés à la ressource exclue.

5. Cliquez sur **Evénements**, puis sélectionnez les événements en fonction du nom de l'événement ou du type de gravité de l'événement pour lequel vous souhaitez déclencher une alerte.

   Pour sélectionner plusieurs événements, appuyez sur la touche Ctrl pendant que vous effectuez vos sélections.

6. Cliquez sur **actions** et sélectionnez les utilisateurs que vous souhaitez notifier, choisissez la fréquence de notification, choisissez si une interruption SNMP sera envoyée au récepteur d'interruption et affectez un script à exécuter lorsqu'une alerte est générée.

   Si vous modifiez l'adresse e-mail spécifiée pour l'utilisateur et rouvrez l'alerte pour modification, le champ Nom apparaît vide car l'adresse e-mail modifiée n'est plus mappée à l'utilisateur qui a été précédemment sélectionné. En outre, si vous avez modifié l'adresse e-mail de l'utilisateur sélectionné à partir de la page utilisateurs, l'adresse e-mail modifiée n'est pas mise à jour pour l'utilisateur sélectionné.

   Vous pouvez également choisir de notifier les utilisateurs via les interruptions SNMP.

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

Dans cet exemple, vous apprendrez à créer une alerte conforme aux exigences suivantes :

- Nom de l'alerte : HealthTest
- Ressources : inclut tous les volumes dont le nom contient « abc » et exclut tous les volumes dont le nom contient « xyz »
- Événements : inclut tous les événements de santé critiques
- Actions : inclut « sample@domain.com », un script « Test » et l'utilisateur doit être averti toutes les 15 minutes

Effectuez les opérations suivantes dans la boîte de dialogue Ajouter une alerte :

1. Cliquez sur **Nom** et saisissez `HealthTest` Dans le champ **Nom d'alerte**.
2. Cliquez sur **Ressources** et, dans l'onglet inclure, sélectionnez **volumes** dans la liste déroulante.
   a. Entrez `abc` Dans le champ **Name contient** pour afficher les volumes dont le nom contient "abc".
   b. Sélectionnez **<<All Volumes whose name contains 'abc'>>** dans la zone Ressources disponibles, et déplacez-la dans la zone Ressources sélectionnées.
   c. Cliquez sur **exclure**, puis saisissez `xyz` Dans le champ **Name contient**, puis cliquez sur **Add**.
3. Cliquez sur **Evénements**, puis sélectionnez **critique** dans le champ gravité de l'événement.
4. Sélectionnez **tous les événements critiques** dans la zone événements de correspondance et déplacez-le dans la zone événements sélectionnés.
5. Cliquez sur **actions**, puis saisissez `sample@domain.com` Dans le champ Alert ces utilisateurs.
6. Sélectionnez **rappeler toutes les 15 minutes** pour avertir l'utilisateur toutes les 15 minutes.

   Vous pouvez configurer une alerte pour qu'elle envoie régulièrement des notifications aux destinataires pendant une heure donnée. Vous devez déterminer l'heure à laquelle la notification d'événement est active pour l'alerte.
7. Dans le menu Select script to Execute, sélectionnez **Test** script.
8. Cliquez sur **Enregistrer**.

Configurez les paramètres d'alerte

Vous pouvez spécifier les événements provenant de Active IQ Unified Manager qui déclenchent des alertes, les destinataires de ces alertes et la fréquence des alertes.

Ce dont vous avez besoin

Vous devez avoir le rôle Administrateur d'applications.

Description de la tâche

Vous pouvez configurer des paramètres d'alerte uniques pour les types d'événements de performance suivants :

- Événements critiques déclenchés par des violations des seuils définis par l'utilisateur
- Événements d'avertissement déclenchés par des violations des seuils définis par l'utilisateur, des seuils définis par le système ou des seuils dynamiques

Par défaut, des alertes par e-mail sont envoyées aux utilisateurs d'administration de Unified Manager pour tous les nouveaux événements. Vous pouvez envoyer des alertes par e-mail à d'autres utilisateurs en ajoutant les adresses e-mail de ces utilisateurs.

Pour désactiver l'envoi d'alertes pour certains types d'événements, vous devez décocher toutes les cases d'une catégorie d'événement. Cette action n'arrête pas l'apparition des événements dans l'interface utilisateur.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Storage Management** > **Alert Setup**.

   La page Configuration des alertes s'affiche.

2. Cliquez sur **Ajouter** et configurez les paramètres appropriés pour chaque type d'événement.

   Pour envoyer des alertes par e-mail à plusieurs utilisateurs, entrez une virgule entre chaque adresse e-mail.

3. Cliquez sur **Enregistrer**.

Identification des problèmes de performances dans Active IQ Unified Manager

Si un événement de performance se produit, vous pouvez localiser la source du problème dans Active IQ Unified Manager et utiliser d'autres outils pour le résoudre. Vous recevrez peut-être une notification par e-mail d'un événement ou une notification de cet événement pendant le suivi quotidien.

Étapes

1. Cliquez sur le lien de la notification par e-mail, qui vous mène directement à l'objet de stockage ayant un événement de performances.

Si…	Alors…
Recevoir une notification par e-mail d'un événement	Cliquez sur le lien pour accéder directement à la page des détails de l'événement.
Remarquez l'événement lors de l'analyse de la page Inventaire des événements	Sélectionnez l'événement pour accéder directement à la page des détails de l'événement.

2. Si l'événement a franchi un seuil défini par le système, suivez les actions suggérées dans l'interface utilisateur pour résoudre le problème.
3. Si l'événement a franchi un seuil défini par l'utilisateur, analysez l'événement pour déterminer si vous devez agir.
4. Si le problème persiste, vérifiez les paramètres suivants :
   - Paramètres de protocole sur le système de stockage
   - Paramètres réseau sur n'importe quel commutateur Ethernet ou Fabric
   - Paramètres réseau sur le système de stockage
   - Disposition des disques et metrics des agrégats sur le système de stockage
5. Si le problème persiste, contactez le support technique pour obtenir de l'aide.

Utilisez le conseiller numérique Active IQ pour consulter les performances du système

Pour tous les systèmes ONTAP qui envoient la télémétrie AutoSupport à NetApp, vous pouvez afficher des données étendues de performances et de capacité. Active IQ affiche les performances du système sur une période plus longue que ce que vous pouvez voir dans System Manager.

Vous pouvez afficher les graphiques de l'utilisation du CPU, de la latence, des opérations d'entrée/sortie par seconde, des opérations d'entrée/sortie par protocole et du débit du réseau. Vous pouvez également télécharger ces données au format .csv pour les analyser avec d'autres outils.

Outre ces données de performances, Active IQ affiche l'efficacité du stockage par charge de travail et compare cette efficacité à celle attendue pour ce type de charge de travail. Vous pouvez consulter les tendances en matière de capacité et obtenir une estimation de la quantité de stockage supplémentaire à ajouter dans une période donnée.

- L'efficacité du stockage est disponible au niveau du client, du cluster et des nœuds, à gauche du tableau de bord principal.
- La performance est disponible au niveau du cluster et du nœud sur la gauche du tableau de bord principal.

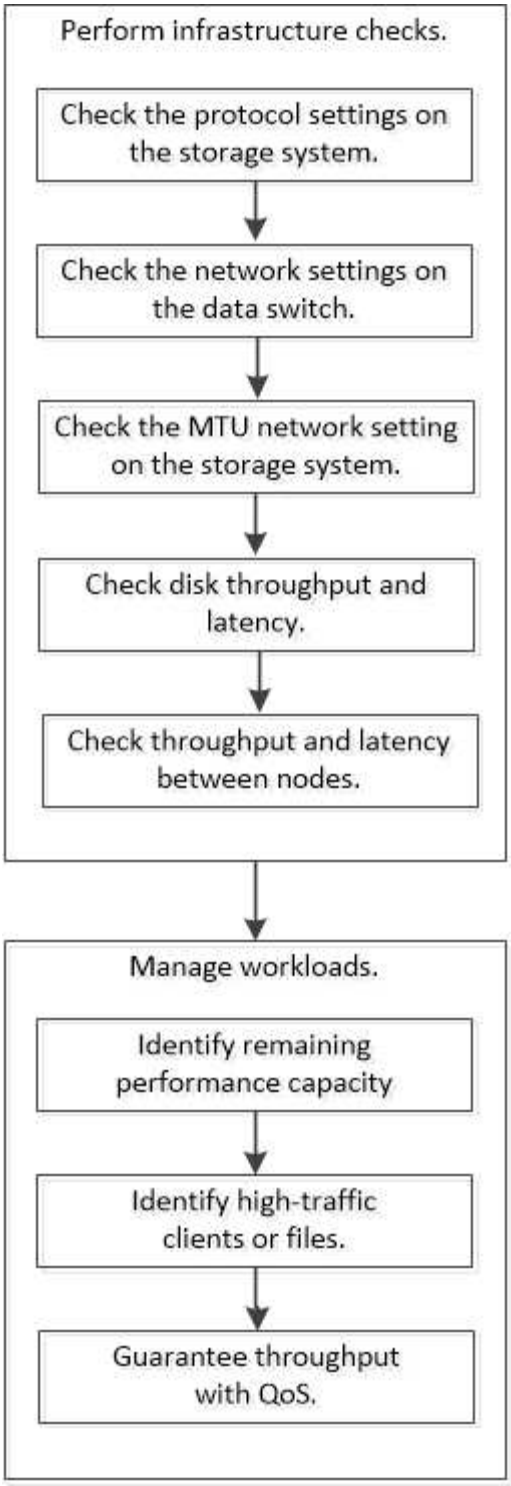
Informations associées

- "Documentation du conseiller digital Active IQ"
- "Liste de lecture vidéo conseiller numérique Active IQ"
- "Portail Web Active IQ"

Gérez les problèmes de performance

Workflow de gestion des performances

Une fois que vous avez identifié un problème de performance, vous pouvez procéder à quelques vérifications de diagnostic de base de votre infrastructure pour éliminer les erreurs de configuration évidentes. Si ceux qui ne identifient pas le problème, vous pouvez commencer par examiner les problèmes liés à la gestion des charges de travail.



Effectuer des vérifications de base de l'infrastructure

Vérifiez les paramètres de protocole sur le système de stockage

Vérifiez la taille maximale du transfert TCP NFS

Pour NFS, vous pouvez vérifier si la taille maximale du transfert TCP pour les lectures et les écritures peut provoquer un problème de performances. Si vous pensez que la taille ralentit les performances, vous pouvez l'augmenter.

Ce dont vous avez besoin

- Pour effectuer cette tâche, vous devez disposer des privilèges d'administrateur de cluster.
- Vous devez utiliser des commandes de niveau de privilège avancé pour cette tâche.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Vérifiez la taille maximale du transfert TCP :

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

3. Si la taille maximale du transfert TCP est trop faible, augmentez la taille :

   ```
   vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
   ```

4. Revenir au niveau de privilège administratif :

   ```
   set -privilege admin
   ```

Exemple

L'exemple suivant modifie la taille maximale de transfert TCP de `SVM1` à 1048576 :

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

Vérifiez la taille de lecture/écriture TCP iSCSI

Pour iSCSI, vous pouvez vérifier la taille de lecture/écriture TCP pour déterminer si le paramètre de taille crée un problème de performances. Si la taille est la source d'un problème, vous pouvez le corriger.

Ce dont vous avez besoin

Des commandes de niveau de privilège avancé sont requises pour cette tâche.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Vérifiez le paramètre de taille de la fenêtre TCP :

   ```
   vserver iscsi show -vserv,er vserver_name -instance
   ```

3. Modifiez le paramètre de taille de la fenêtre TCP :

   ```
   vserver iscsi modify -vserver vserver_name -tcp-window-size integer
   ```

4. Revenir au privilège administratif :

```
set -privilege admin
```

Exemple

L'exemple suivant modifie la taille de la fenêtre TCP de `SVM1` à 131,400 octets :

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

Contrôler les réglages multiplexés CIFS

Si des performances réseau CIFS lentes sont à l'origine d'un problème de performances, vous pouvez modifier les paramètres multiplexés pour les améliorer et les corriger.

Étapes

1. Contrôler le réglage multiplexé CIFS :

   ```
   vserver cifs options show -vserver -vserver_name -instance
   ```

2. Modifier le paramètre multiplexé CIFS :

   ```
   vserver cifs options modify –vserver -vserver_name –max-mpx integer
   ```

Exemple

L'exemple suivant modifie le nombre maximal de multiplexage activé `SVM1` à 255 :

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

Vérifiez la vitesse du port de l'adaptateur FC

La vitesse du port cible de l'adaptateur doit correspondre à la vitesse du périphérique auquel il se connecte, afin d'optimiser les performances. Si le port est défini sur négociation automatique, il peut prendre plus de temps pour vous reconnecter après un basculement et un rétablissement ou une autre interruption.

Ce dont vous avez besoin

Toutes les LIFs qui utilisent cet adaptateur comme port de home port doivent être hors ligne.

Étapes

1. Mettez l'adaptateur hors ligne :

   ```
   network fcp adapter modify -node nodename -adapter adapter -state down
   ```

2. Vérifiez la vitesse maximale de l'adaptateur de port :

   ```
   fcp adapter show -instance
   ```

3. Modifiez la vitesse du port, si nécessaire :

```
network fcp adapter modify -node nodename -adapter adapter -speed
{1|2|4|8|10|16|auto}
```

4. Mettez la carte en ligne :

```
network fcp adapter modify -node nodename -adapter adapter -state up
```

5. Mettre en ligne toutes les LIFs sur l'adaptateur :

```
network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }
-status-admin up
```

Exemple

L'exemple suivant modifie la vitesse du port de l'adaptateur `0d` marche `node1` Jusqu'à 2 Gbits/s :

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

Vérifiez les paramètres réseau sur les commutateurs de données

Bien que vous deviez conserver les mêmes paramètres MTU sur vos clients, serveurs et systèmes de stockage (c'est-à-dire les points de terminaison réseau), les périphériques réseau intermédiaires tels que les cartes réseau et les commutateurs doivent être définis sur leurs valeurs MTU maximales pour garantir que les performances ne sont pas affectées.

Pour des performances optimales, tous les composants du réseau doivent être en mesure de transférer des trames Jumbo (IP de 9000 octets, 9022 octets y compris Ethernet). Les commutateurs de données doivent être réglés sur au moins 9022 octets, mais une valeur typique de 9216 est possible avec la plupart des commutateurs.

Procédure

Pour les commutateurs de données, vérifiez que la taille de MTU est définie sur 9022 ou plus.

Pour plus d'informations, consultez la documentation du fournisseur du commutateur.

Vérifiez le paramètre réseau MTU sur le système de stockage

Vous pouvez modifier les paramètres réseau sur le système de stockage s'ils ne sont pas identiques à ceux du client ou d'autres terminaux réseau. Alors que le paramètre MTU du réseau de gestion est défini sur 1500, la taille MTU du réseau de données doit être de 9000.

Description de la tâche

Tous les ports d'un broadcast-domain ont la même taille de MTU, à l'exception du trafic de gestion du port e0M. Si le port fait partie d'un domaine de diffusion, utilisez le `broadcast-domain modify` Commande permettant de modifier la MTU de tous les ports du broadcast-domain modifié.

Notez que les périphériques réseau intermédiaires tels que les cartes réseau et les commutateurs de données peuvent être configurés sur des MTU plus élevés que les noeuds finaux réseau. Pour plus d'informations, voir

"Vérifiez les paramètres réseau sur les commutateurs de données".

Étapes

1. Vérifiez le paramètre du port MTU sur le système de stockage :

   ```
   network port show -instance
   ```

2. Modifier la MTU sur le domaine de diffusion utilisé par les ports :

   ```
   network port broadcast-domain modify -ipspace ipspace -broadcast-domain
   broadcast_domain -mtu new _mtu
   ```

Exemple

L'exemple suivant modifie le paramètre du port MTU sur 9000 :

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain
Cluster -mtu 9000
```

Vérifiez le débit et la latence des disques

Vous pouvez vérifier les mesures de débit et de latence des disques pour les nœuds de cluster afin de vous aider à effectuer le dépannage.

Description de la tâche

Des commandes de niveau de privilège avancé sont requises pour cette tâche.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Vérifiez le débit du disque et les mesures de latence :

   ```
   statistics disk show -sort-key latency
   ```

Exemple

L'exemple suivant affiche les totaux de chaque opération de lecture ou d'écriture de l'utilisateur pour `node2` marche `cluster1`:

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                    Busy Total Read  Write  Read    Write   *Latency
  Disk       Node   (%)   Ops   Ops   Ops   (Bps)    (Bps)       (us)
------------ ----   ---- ----   ----- ----- ------   -----     -----

1.10.20      node2     4    5       3     2  95232  367616    23806
1.10.8       node2     4    5       3     2 138240  386048    22113

1.10.6       node2     3    4       2     2  48128  371712    19113
1.10.19      node2     4    6       3     2 102400  443392    19106

1.10.11      node2     4    4       2     2 122880  408576    17713
```

Vérifiez le débit et la latence entre les nœuds

Vous pouvez utiliser le `network test-path` commande permettant d'identifier les goulets d'étranglement réseau ou de présélectionner les chemins réseau entre les nœuds. Vous pouvez exécuter la commande entre les nœuds intercluster ou intracluster.

Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des commandes de niveau de privilège avancé sont requises pour cette tâche.
- Pour un chemin intercluster, les clusters source et destination doivent être associés.

Description de la tâche

Il arrive que les performances du réseau entre les nœuds ne répondent pas aux attentes de votre configuration de chemin. Un taux de transmission de 1 Gbit/s pour le type de transferts de données volumineux vus dans les opérations de réplication SnapMirror, par exemple, ne serait pas cohérent avec une liaison 10 GbE entre les clusters source et destination.

Vous pouvez utiliser le `network test-path` commande pour mesurer le débit et la latence entre les nœuds. Vous pouvez exécuter la commande entre les nœuds intercluster ou intracluster.

> Le test sature le chemin du réseau avec des données, vous devez donc exécuter la commande lorsque le système n'est pas occupé, et lorsque le trafic réseau entre les nœuds n'est pas excessif. Le test s'est terminé après dix secondes. La commande ne peut être exécutée qu'entre des nœuds ONTAP 9.

Le `session-type` Option identifie le type d'opération que vous exécutez sur le chemin réseau, par exemple « AsyncMirrorRemote » pour la réplication SnapMirror vers une destination distante. Le type détermine la quantité de données utilisées dans le test. Le tableau suivant définit les types de session :

Type de session	Description
AsyncMirrorlocal	Paramètres utilisés par SnapMirror entre les nœuds du même cluster

AsyncMirrorRemote	Paramètres utilisés par SnapMirror entre les nœuds dans différents clusters (type par défaut)
Transfert de données à distance	Paramètres utilisés par ONTAP pour l'accès distant aux données entre les nœuds d'un même cluster (par exemple, une requête NFS vers un nœud pour un fichier stocké dans un volume sur un autre nœud)

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Mesure du débit et de la latence entre les nœuds :

   ```
   network test-path -source-node source_nodename |local -destination-cluster
   destination_clustername -destination-node destination_nodename -session-type
   Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
   ```

   Le nœud source doit se trouver dans le cluster local. Le nœud de destination peut être situé sur le cluster local ou dans un cluster en clusters à peering. Une valeur de "local" pour `-source-node` spécifie le nœud sur lequel vous exécutez la commande.

   La commande suivante mesure le débit et la latence des opérations de réplication de type SnapMirror entre `node1` sur le cluster local et `node3` marche `cluster2`:

   ```
   cluster1::> network test-path -source-node node1 -destination-cluster
   cluster2 -destination-node node3 -session-type AsyncMirrorRemote
   Test Duration:      10.88 secs
   Send Throughput:    18.23 MB/sec
   Receive Throughput: 18.23 MB/sec
   MB sent:            198.31
   MB received:        198.31
   Avg latency in ms:  2301.47
   Min latency in ms:  61.14
   Max latency in ms:  3056.86
   ```

3. Revenir au privilège administratif :

   ```
   set -privilege admin
   ```

Une fois que vous avez terminé

Si les performances ne répondent pas aux attentes en matière de configuration du chemin, vérifiez les statistiques de performances du nœud, utilisez les outils disponibles pour isoler le problème sur le réseau, vérifiez les paramètres du commutateur, etc.

Gérer les charges de travail

Identifiez les performances de capacité restante

La capacité de performance, ou *headroom*, mesure le volume de travail que vous pouvez placer sur un nœud ou un agrégat avant que les performances des charges de travail sur la ressource ne commencent à être affectées par la latence. Connaître la capacité en termes de performances disponible sur le cluster vous aide à provisionner et à équilibrer les charges de travail.

Ce dont vous avez besoin

Des commandes de niveau de privilège avancé sont requises pour cette tâche.

Description de la tâche

Vous pouvez utiliser les valeurs suivantes pour l' `-object` option pour collecter et afficher les statistiques de marge :

- Pour les CPU, `resource_headroom_cpu`.
- Pour les agrégats, `resource_headroom_aggr`.

Vous pouvez également effectuer cette tâche à l'aide de System Manager et de Active IQ Unified Manager.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Démarrer la collecte de statistiques de marge en temps réel :

   ```
   statistics start –object resource_headroom_cpu|aggr
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

3. Afficher les informations statistiques relatives à la marge en temps réel :

   ```
   statistics show -object resource_headroom_cpu|aggr
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

4. Revenir au privilège administratif :

   ```
   set -privilege admin
   ```

Exemple

L'exemple suivant affiche les statistiques moyennes sur la marge horaire des nœuds du cluster.

Vous pouvez calculer la capacité de performances disponible d'un nœud en soustrayant la `current_utilization` compteur du `optimal_point_utilization` compteur. Dans cet exemple, la capacité d'utilisation pour `CPU_sti2520-213` Est de -14% (72%-86%), ce qui suggère que le CPU a été surexploité en moyenne au cours de la dernière heure.

Vous avez peut-être spécifié `ewma_daily`, `ewma_weekly`, ou `ewma_monthly` pour obtenir la moyenne des mêmes informations sur des périodes plus longues.

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
  (statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_hourly                                                     -
                         current_ops                             4376
                     current_latency                            37719
                 current_utilization                               86
                   optimal_point_ops                             2573
               optimal_point_latency                             3589
            optimal_point_utilization                              72
     optimal_point_confidence_factor                                1

Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_hourly                                                     -
                         current_ops                                0
                     current_latency                                0
                 current_utilization                                0
                   optimal_point_ops                                0
               optimal_point_latency                                0
            optimal_point_utilization                              71
     optimal_point_confidence_factor                                1
2 entries were displayed.
```

Identifiez les clients ou les fichiers à fort trafic

Vous pouvez utiliser la technologie Active Objects de ONTAP pour identifier les clients ou les fichiers responsables d'une quantité disproportionnée de trafic de grappe. Une fois

que vous avez identifié ces « principaux » clients ou fichiers, vous pouvez rééquilibrer les charges de travail du cluster ou prendre d'autres mesures pour résoudre le problème.

Ce dont vous avez besoin

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Afficher les principaux clients accédant au cluster :

   `statistics top client show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante affiche les principaux clients accédant à `cluster1`:

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10


                                              *Total
        Client Vserver           Node Protocol    Ops
-------------- ------- -------------- -------- ------
172.17.180.170     vs4 siderop1-vsim4      nfs    668
172.17.180.169     vs3 siderop1-vsim3      nfs    337
172.17.180.171     vs3 siderop1-vsim3      nfs    142
172.17.180.170     vs3 siderop1-vsim3      nfs    137
172.17.180.123     vs3 siderop1-vsim3      nfs    137
172.17.180.171     vs4 siderop1-vsim4      nfs     95
172.17.180.169     vs4 siderop1-vsim4      nfs     92
172.17.180.123     vs4 siderop1-vsim4      nfs     92
172.17.180.153     vs3 siderop1-vsim3      nfs      0
```

2. Afficher les principaux fichiers auxquels a accédé sur le cluster :

   `statistics top file show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante affiche les principaux fichiers auxquels vous accédez `cluster1`:

```
cluster1::> statistics top file show

cluster1 : 3/23/2016 17:59:10

                                    *Total
                     File Volume Vserver          Node    Ops
------------------------ ------ ------- -------------- ------
/vol/vol1/vm170-read.dat   vol1     vs4 siderop1-vsim4     22
/vol/vol1/vm69-write.dat   vol1     vs3 siderop1-vsim3      6
     /vol/vol2/vm171.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol2/vm169.dat   vol2     vs3 siderop1-vsim3      2
      /vol/vol2/p123.dat   vol2     vs4 siderop1-vsim4      2
      /vol/vol2/p123.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol1/vm171.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim3      2
      /vol/vol1/p123.dat   vol1     vs4 siderop1-vsim4      2
```

Débit garanti avec la QoS

Débit garanti avec les QoS

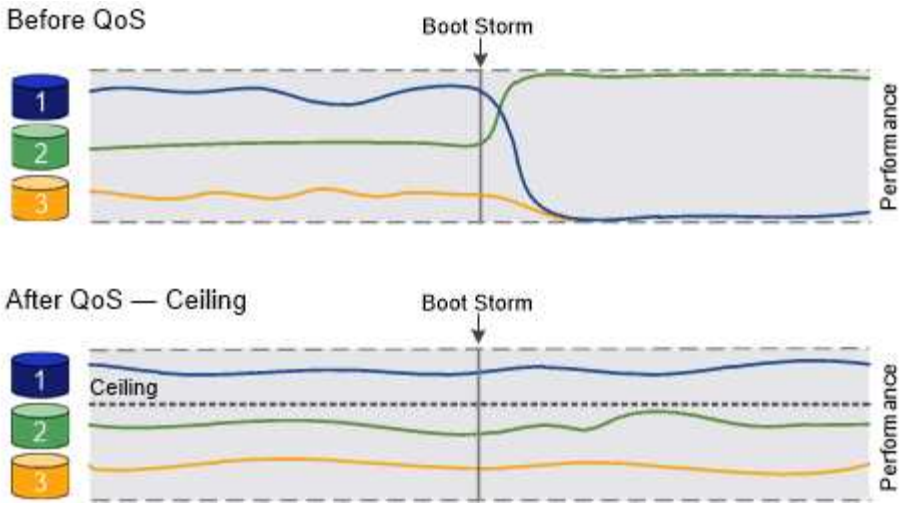
Grâce à la qualité de service (QoS) du stockage, vous pouvez garantir que les performances des workloads stratégiques ne sont pas dégradées par des charges de travail concurrentes. Vous pouvez fixer un plafond de débit sur une charge de travail concurrente pour limiter son impact sur les ressources système, ou définir un débit *sol* pour une charge de travail critique, afin de garantir qu'il répond aux objectifs de débit minimum, indépendamment de la demande des charges de travail concurrentes. Vous pouvez même fixer un plafond et un sol pour la même charge de travail.

À propos des plafonds de débit (QoS Max)

Le débit limite le débit pour une charge de travail jusqu'à un nombre maximal d'IOPS ou de Mbit/s, ainsi que les IOPS et les Mbit/s. Dans la figure ci-dessous, le plafond de débit pour la charge de travail 2 garantit qu'il ne « traite » pas les charges de travail 1 et 3.

Un *policy group* définit le plafond de débit pour une ou plusieurs charges de travail. Une charge de travail représente les opérations d'E/S d'un objet *stockage :* un volume, un fichier, qtree ou une LUN, ou l'ensemble des volumes, fichiers, qtrees ou LUN d'un SVM. Vous pouvez spécifier le plafond lorsque vous créez le groupe de règles ou attendre jusqu'à ce que vous contrôdiez les charges de travail pour les spécifier.

> Le débit des charges de travail peut dépasser jusqu'à 10 % le plafond défini, en particulier si le débit d'une charge de travail change rapidement. Le plafond peut être dépassé de 50 % pour gérer les rafales. Les rafales se produisent sur des nœuds uniques lorsque les jetons s'accumulent jusqu'à 150 %



À propos du débit au sol (QoS min)

Un plancher de débit garantit que le débit d'une charge de travail ne passe pas en dessous d'un nombre minimal d'IOPS ou de Mo/sec, ou d'IOPS et de Mo/sec. Dans la figure ci-dessous, les niveaux de débit pour la charge de travail 1 et la charge de travail 3 s'assurent qu'ils répondent aux objectifs de débit minimum, indépendamment de la demande par charge de travail 2.

Comme le suggèrent les exemples, un plafond de débit accélère directement le débit. Un plancher de débit accélère indirectement le débit en donnant la priorité aux charges de travail pour lesquelles le sol a été défini.

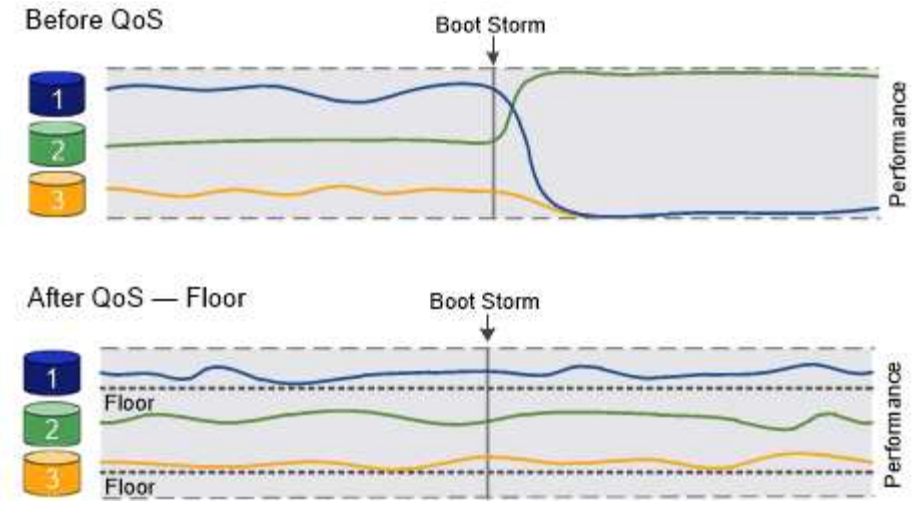
Vous pouvez spécifier l'étage lors de la création du groupe de règles ou attendre jusqu'à ce que vous surveilliez les charges de travail pour le spécifier.

À partir de la version ONTAP 9.13.1, vous pouvez définir des étages de débit au niveau de l'étendue du SVM avec [adaptive-qos-templates]. Dans les versions ONTAP antérieures à 9.13.1, un groupe de règles qui définit un plancher de débit ne peut pas être appliqué à une SVM.

Dans les versions antérieures à ONTAP 9.7, le débit est garanti lorsque la capacité de performance est suffisante.

Dans la ONTAP 9.7 et versions ultérieures, le débit au sol peut être garanti même en cas de capacité de performance insuffisante. Ce nouveau comportement de plancher s'appelle planchers v2. Pour respecter les garanties, au sol v2, peut offrir une plus grande latence sur les charges de travail sans débit ni travail dépassant les paramètres au sol. Au sol v2 s'applique à la QoS et à la qualité de service adaptative.

L'option d'activation/désactivation du nouveau comportement des étages v2 est disponible dans ONTAP 9.7P6 et versions ultérieures. Une charge de travail peut tomber sous le plancher spécifié pendant des opérations critiques comme `volume move trigger-cutover`. Même lorsque vous disposez d'une capacité suffisante et que vos opérations stratégiques n'ont pas lieu, le débit d'une charge de travail peut tomber en dessous du seuil spécifié de 5 %. Si les étages sont surprovisionnés et que la capacité de performance n'est pas disponible, certaines charges de travail peuvent tomber en dessous de l'étage spécifié.



À propos des groupes de règles de qualité de service partagés et non partagés

À partir de ONTAP 9.4, vous pouvez utiliser un groupe de règles QoS *non-partagé* pour spécifier que le plafond ou le sol de débit défini s'applique à chaque charge de travail membre individuellement. Le comportement des groupes de règles *shared* dépend du type de stratégie :

- Pour les plafonds de débit, le débit total des charges de travail affectées au groupe de règles partagées ne peut dépasser le plafond spécifié.
- Pour les étages de débit, le groupe de règles partagées ne peut être appliqué qu'à une seule charge de travail.

À propos de la QoS adaptative

En principe, la valeur du groupe de règles que vous attribuez à un objet de stockage est fixe. Vous devez modifier la valeur manuellement lorsque la taille de l'objet de stockage change. Une augmentation de l'espace utilisé sur un volume, par exemple, nécessite généralement une augmentation correspondante du plafond de débit spécifié pour le volume.

Adaptive QoS ajuste automatiquement la valeur du groupe de règles en fonction de la taille de la charge de travail, en maintenant le rapport IOPS/To|Go en fonction de la taille des modifications de la charge de travail. C'est un avantage significatif pour la gestion de centaines, voire de milliers de charges de travail dans un déploiement à grande échelle.

Généralement, vous utilisez la QoS adaptative pour ajuster les plafonds de débit, mais vous pouvez également l'utiliser pour gérer le débit (en cas d'augmentation de la taille des charges de travail). La taille du workload est exprimée en espace alloué à l'objet de stockage ou en espace utilisé par l'objet de stockage.

> L'espace utilisé est disponible pour les étages de débit dans ONTAP 9.5 et versions ultérieures. Elle n'est pas prise en charge pour les étages de débit dans ONTAP 9.4 et les versions antérieures.

- Une politique *Alocated space* maintient le ratio IOPS/To|Go en fonction de la taille nominale de l'objet de stockage. Si le rapport est de 100 IOPS/Go, un volume de 150 Go plafonné à 15,000 IOPS, tant que la taille du volume reste celle-ci. Si le volume a été redimensionné de façon à 300 Go, la QoS adaptative ajuste le débit au plafond à 30,000 000 IOPS.
- Une règle *Used space* (par défaut) maintient le ratio IOPS/To|Go en fonction de la quantité de données réelles stockées avant le stockage efficace. Si le rapport est de 100 IOPS/Go, un volume de 150 Go contenant 100 Go de données stockées aurait un débit plafond de 10,000 000 IOPS. À mesure que la

quantité d'espace utilisée change, la QoS adaptative ajuste le plafond de débit en fonction du rapport.

Depuis ONTAP 9.5, vous pouvez spécifier une taille de bloc d'E/S pour votre application afin d'indiquer une limite de débit en IOPS et en Mbit/s. La limite de Mbit/s est calculée à partir de la taille de bloc multipliée par la limite d'IOPS. Par exemple, une taille de bloc d'E/S de 32 Ko pour une limite d'IOPS de 6144 IOPS/To permet d'obtenir une limite de 192 Mbit/s en Mbit/s.

Vous pouvez vous attendre à ce que le comportement suivant soit à la fois pour les plafonds de rendement et pour les planchers :

- Lorsqu'une charge de travail est affectée à un groupe de règles QoS adaptative, le plafond ou le sol est immédiatement mis à jour.
- Lorsqu'une charge de travail d'un groupe de règles de QoS adaptative est redimensionnée, la limite ou le sol est mis à jour en cinq minutes environ.

Le débit doit augmenter d'au moins 10 000 IOPS avant la mise à jour.

Les groupes de règles de QoS adaptative sont toujours non partagés : le plafond ou l'étage de débit défini s'applique à chaque charge de travail membre individuellement.

À partir de la version ONTAP 9.6, les niveaux de débit sont pris en charge par ONTAP Select Premium avec SSD.

Modèle de groupe de règles adaptatif

À partir de la version ONTAP 9.13.1, vous pouvez définir un modèle de QoS adaptative sur une SVM. Les modèles de groupes de règles adaptatifs vous permettent de définir des seuils et des plafonds de débit pour tous les volumes d'une SVM.

Les modèles de groupes de règles adaptatives ne peuvent être définis qu'après la création du SVM. Utilisez le `vserver modify` commande avec `-qos-adaptive-policy-group-template` paramètre permettant de définir la règle.

Lorsque vous définissez un modèle de groupe de règles adaptatives, les volumes créés ou migrés après avoir défini la règle héritent automatiquement de la règle. L'affectation du modèle de règle n'a aucun impact sur les volumes existants du SVM. Si vous désactivez la policy sur le SVM, tout volume ultérieurement migré vers ou créé sur le SVM ne recevra pas la policy. La désactivation du modèle de groupe de règles adaptatives n'a pas d'impact sur les volumes qui ont hérité du modèle de règles car ils conservent le modèle de règles.

Pour plus d'informations, voir Définissez un modèle de groupe de règles adaptatives.

Assistance générale

Le tableau ci-dessous présente les différences en matière de prise en charge des plafonds de débit, des étages de débit et de la QoS adaptative.

Ressource ou fonctionnalité	Plafond de débit	Plancher de débit	Débit au sol v2	La QoS adaptative
Version ONTAP 9	Tout	9.2 et versions ultérieures	9.7 et versions ultérieures	9.3 et versions ultérieures

Ressource ou fonctionnalité	Plafond de débit	Plancher de débit	Débit au sol v2	La QoS adaptative
Plateformes	Tout	• AFF • C190 * • ONTAP Select Premium avec SSD *	• AFF • C190 • ONTAP Select Premium avec SSD	Tout
Protocoles	Tout	Tout	Tout	Tout
FabricPool	Oui.	Oui, si la règle de Tiering est définie sur « none » et si aucun bloc n'est dans le cloud.	Oui, si la règle de Tiering est définie sur « none » et si aucun bloc n'est dans le cloud.	Non
SnapMirror synchrone	Oui.	Non	Non	Oui.

La prise en charge des baies ONTAP Select et C190 a débuté avec la version ONTAP 9.6.

Charges de travail prises en charge pour les plafonds de débit

Le tableau ci-dessous présente la prise en charge des charges de travail pour les plafonds de débit dans la version ONTAP 9. Les volumes root, les miroirs de partage de charge et les miroirs de protection des données ne sont pas pris en charge.

Support de charge de travail - plafond	ONTAP 9.0	ONTAP 9.1	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4 - 9.7	ONTAP 9.8 et versions ultérieures
Volumétrie	oui	oui	oui	oui	oui	oui
Fichier	oui	oui	oui	oui	oui	oui
LUN	oui	oui	oui	oui	oui	oui
SVM	oui	oui	oui	oui	oui	oui
Volume FlexGroup	non	non	non	oui	oui	oui
qtrees*	non	non	non	non	non	oui

Support de charge de travail - plafond	ONTAP 9.0	ONTAP 9.1	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4 - 9.7	ONTAP 9.8 et versions ultérieures
Plusieurs charges de travail par groupe de règles	oui	oui	oui	oui	oui	oui
Groupes de stratégies non partagés	non	non	non	non	oui	oui

Depuis la version ONTAP 9.8, l'accès NFS est pris en charge dans les qtrees des volumes FlexVol et FlexGroup sur lesquels NFS est activé. Depuis la version ONTAP 9.9.1, l'accès SMB est également pris en charge dans les qtrees des volumes FlexVol et FlexGroup sur lesquels SMB est activé.

Charges de travail prises en charge pour le débit au sol

Le tableau ci-dessous présente la prise en charge des charges de travail pour les débits par la version ONTAP 9. Les volumes root, les miroirs de partage de charge et les miroirs de protection des données ne sont pas pris en charge.

Soutien de la charge de travail - plancher	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4 - 9.7	ONTAP 9.8 - 9.13.0	ONTAP 9.13.1 et versions ultérieures
Volumétrie	oui	oui	oui	oui	oui
Fichier	non	oui	oui	oui	oui
LUN	oui	oui	oui	oui	oui
SVM	non	non	non	non	oui
Volume FlexGroup	non	non	oui	oui	oui
qtrees *	non	non	non	oui	oui
Plusieurs charges de travail par groupe de règles	non	non	oui	oui	oui
Groupes de stratégies non partagés	non	non	oui	oui	oui

*à partir de ONTAP 9.8, l'accès NFS est pris en charge dans les qtrees des volumes FlexVol et FlexGroup sur lesquels NFS est activé. Depuis la version ONTAP 9.9.1, l'accès SMB est également pris en charge dans les qtrees des volumes FlexVol et FlexGroup sur lesquels SMB est activé.

Prise en charge de workloads pour la QoS adaptative

Le tableau ci-dessous présente la prise en charge des workloads pour la QoS adaptative par la version ONTAP 9. Les volumes root, les miroirs de partage de charge et les miroirs de protection des données ne sont pas pris en charge.

Prise en charge des workloads : QoS adaptative	ONTAP 9.3	ONTAP 9.4 - 9.13.0	ONTAP 9.13.1 et versions ultérieures
Volumétrie	oui	oui	oui
Fichier	non	oui	oui
LUN	non	oui	oui
SVM	non	non	oui
Volume FlexGroup	non	oui	oui
Plusieurs charges de travail par groupe de règles	oui	oui	oui
Groupes de stratégies non partagés	oui	oui	oui

Nombre maximal de charges de travail et de groupes de règles

Le tableau ci-dessous indique le nombre maximal de charges de travail et de groupes de règles par la version ONTAP 9.

Prise en charge des workloads	ONTAP 9.3 et versions antérieures	ONTAP 9.4 et versions ultérieures
Charges de travail maximales par cluster	12,000	40,000
Nombre maximal de workloads par nœud	12,000	40,000
Nombre maximal de stratégies groupes	12,000	12,000

Activer ou désactiver le débit planchers v2

Vous pouvez activer ou désactiver le débit planchers v2 sur AFF. La valeur par défaut est activée. Lorsque la technologie planchers v2 est activée, le débit au sol peut être atteint lorsque les contrôleurs sont utilisés de façon intensive, au détriment d’une latence plus élevée sur d’autres charges de travail. Au niveau de la QoS et de la QoS adaptative.

Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Entrez l'une des commandes suivantes :

Les fonctions que vous recherchez…	Utilisez cette commande :
Désactiver les étages v2	`qos settings throughput-floors-v2 -enable false`
Activation de la version 2	`qos settings throughput-floors-v2 -enable true`

Pour désactiver le débit planchers v2 dans un cluster MetroCluster, vous devez exécuter le `qos settings throughput-floors-v2 -enable false` contrôlez à la fois les clusters source et de destination.

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

Flux de travail de QoS du stockage

Si vous connaissez déjà les exigences de performance des workloads que vous souhaitez gérer avec QoS, vous pouvez définir la limite de débit lors de la création du groupe de règles. Sinon, vous pouvez attendre jusqu'à ce que vous contrôlons les charges de travail pour spécifier la limite.

Fixer un plafond de débit avec la QoS

Vous pouvez utiliser le `max-throughput` Champ permettant à un groupe de règles de définir une limite de débit pour les workloads d'objets de stockage (QoS max). Vous pouvez appliquer le groupe de règles lors de la création ou de la modification de l'objet de stockage.

Ce dont vous avez besoin

- Pour créer une « policy group » il faut être un administrateur de cluster.
- Vous devez être un administrateur de cluster pour appliquer une « policy group » à un SVM.

Description de la tâche

- Depuis ONTAP 9.4, vous pouvez utiliser un groupe de règles QoS *non-partagé* pour spécifier que le plafond de débit défini s'applique à chaque charge de travail membre individuellement. Sinon, le groupe de règles est *Shared:* le débit total des charges de travail affectées au groupe de règles ne peut pas dépasser le plafond spécifié.

  Réglez `-is-shared=false` pour le `qos policy-group create` commande permettant de spécifier un groupe de polices non partagé.

- Vous pouvez spécifier la limite de débit pour le plafond en IOPS, Mo/s ou IOPS, Mo/s. Si vous spécifiez les IOPS et Mo/s, la première limite atteinte est appliquée.

> Si vous définissez une limite et un sol pour la même charge de travail, vous pouvez spécifier la limite de débit pour le plafond des IOPS uniquement.

- Un objet de stockage faisant l'objet d'une limite QoS doit être contenu par le SVM auquel appartient le groupe de règles. Plusieurs « policy group » peuvent appartenir à la même SVM.
- Vous ne pouvez pas affecter un objet de stockage à un groupe de règles si son objet contenant ou ses objets enfants appartiennent à ce groupe.
- Il s'agit d'une meilleure pratique de QoS pour appliquer un groupe de règles au même type d'objets de stockage.

Étapes

1. Création d'une « policy group » :

   `qos policy-group create -policy-group` *`policy_group`* `-vserver` *`SVM`* `-max -throughput` *`number_of_iops`*`|Mb/S|iops,Mb/S -is-shared true|false`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man. Vous pouvez utiliser le `qos policy-group modify` commande permettant d'ajuster les plafonds de débit.

   La commande suivante crée la « policy group » partagée `pg-vs1` Avec un débit maximum de 5,000 000 IOPS :

   ```
   cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
   -max-throughput 5000iops -is-shared true
   ```

   La commande suivante crée le « policy group » non partagé `pg-vs3` Avec un débit maximum de 100 400 IOPS et 80 Ko/S :

   ```
   cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
   -max-throughput 100iops,400KB/s -is-shared false
   ```

   La commande suivante crée le « policy group » non partagé `pg-vs4` sans limite de débit :

   ```
   cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
   -is-shared false
   ```

2. Appliquer une « policy group » à un SVM, fichier, volume ou LUN :

   `storage_object` `create -vserver` *`SVM`* `-qos-policy-group` *`policy_group`*

   Pour connaître la syntaxe complète des commandes, consultez les pages de manuels. Vous pouvez utiliser le *`storage_object`* `modify` commande pour appliquer un autre groupe de règles à l'objet de stockage.

La commande suivante applique la « policy group » `pg-vs1` À la SVM `vs1`:

```
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
```

Les commandes suivantes appliquent la « policy group » `pg-app` aux volumes `app1` et `app2`:

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

3. Surveillance des performances des groupes de règles :

   `qos statistics performance show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Contrôle des performances depuis le cluster. N'utilisez pas d'outil sur l'hôte pour surveiller les performances.

   La commande suivante affiche les performances de « policy group » :

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_vs1                   5008       19.56MB/s     2.45ms
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

4. Contrôle de la performance des charges de travail :

   `qos statistics workload performance show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Contrôle des performances depuis le cluster. N'utilisez pas d'outil sur l'hôte pour surveiller les performances.

   La commande suivante indique les performances des workloads :

```
cluster1::> qos statistics workload performance show
Workload           ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-             -    12320        47.84MB/s  1215.00us
app1-wid7967     7967     7219        28.20MB/s   319.00us
vs1-wid12279    12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS    14       55        10.92KB/s   236.00us
_Scan_Backgro..  5688       20            0KB/s        0ms
```

Vous pouvez utiliser le `qos statistics workload latency show` Commande pour afficher les statistiques de latence détaillées pour les workloads de QoS.

Définissez un seuil de débit avec la QoS

Vous pouvez utiliser le `min-throughput` Champ permettant à un groupe de règles de définir un étage de débit pour les workloads d'objets de stockage (QoS min). Vous pouvez appliquer le groupe de règles lors de la création ou de la modification de l'objet de stockage. Depuis la version ONTAP 9.8, vous pouvez spécifier le seuil de débit en IOPS ou Mbit/s, ou IOPS et Mbit/s.

Avant de commencer

- Vous devez exécuter ONTAP 9.2 ou version ultérieure. Les étages de débit sont disponibles à partir de ONTAP 9.2.
- Pour créer une « policy group » il faut être un administrateur de cluster.
- À partir de la version ONTAP 9.13.1, vous pouvez appliquer des planchers de débit au niveau de la SVM en utilisant une modèle de groupe de règles adaptatif. Vous ne pouvez pas définir de modèle de « policy group » adaptatif sur une SVM disposant d'une « policy group » QoS.

Description de la tâche

- Depuis ONTAP 9.4, vous pouvez utiliser un groupe de règles QoS *non-partagé* pour spécifier que le niveau de débit défini soit appliqué individuellement à chaque charge de travail membre. C'est la seule condition dans laquelle un groupe de règles pour un étage de débit peut être appliqué à plusieurs charges de travail.

  Réglez `-is-shared=false` pour le `qos policy-group create` commande permettant de spécifier une « policy group » non partagée.

- Le débit d'une charge de travail peut tomber en dessous du seuil spécifié si la capacité de performance est insuffisante (marge) sur le nœud ou l'agrégat.
- Un objet de stockage faisant l'objet d'une limite QoS doit être contenu par le SVM auquel appartient le groupe de règles. Plusieurs « policy group » peuvent appartenir à la même SVM.
- Il s'agit d'une meilleure pratique de QoS pour appliquer un groupe de règles au même type d'objets de stockage.
- Un groupe de règles qui définit un étage de débit ne peut pas être appliqué à un SVM.

Étapes

1. Vérifier que la capacité de performance sur le nœud ou l'agrégat est appropriée, comme décrit dans

"Identification de la capacité de performance restante".

2. Création d'une « policy group » :

   `qos policy-group create -policy group` *`policy_group`* `-vserver` *`SVM`* `-min -throughput` *`qos_target`* `-is-shared true|false`

   Pour connaître la syntaxe complète de la commande, consultez la page man de votre version de ONTAP. Vous pouvez utiliser le `qos policy-group modify` commande permettant de régler les étages de débit.

   La commande suivante crée la « policy group » partagée `pg-vs2` Avec un débit minimal de 1,000 000 IOPS :

   ```
   cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2
   -min-throughput 1000iops -is-shared true
   ```

   La commande suivante crée le « policy group » non partagé `pg-vs4` sans limite de débit :

   ```
   cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4
   -is-shared false
   ```

3. Appliquer une « policy group » à un volume ou une LUN :

   `storage_object` `create -vserver` *`SVM`* `-qos-policy-group` *`policy_group`*

   Pour connaître la syntaxe complète des commandes, consultez les pages de manuels. Vous pouvez utiliser le `_storage_object_modify` commande pour appliquer un autre groupe de règles à l'objet de stockage.

   La commande suivante applique la « policy group » `pg-app2` au volume `app2`:

   ```
   cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
   -qos-policy-group pg-app2
   ```

4. Surveillance des performances des groupes de règles :

   `qos statistics performance show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Contrôle des performances depuis le cluster. N'utilisez pas d'outil sur l'hôte pour surveiller les performances.

   La commande suivante affiche les performances de « policy group » :

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_app2                  7216       28.19MB/s   420.00us
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

5. Contrôle de la performance des charges de travail :

   `qos statistics workload performance show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Contrôle des performances depuis le cluster. N'utilisez pas d'outil sur l'hôte pour surveiller les performances.

   La commande suivante indique les performances des workloads :

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app2-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

   > Vous pouvez utiliser le `qos statistics workload latency show` Commande pour afficher les statistiques de latence détaillées pour les workloads de QoS.

Utilisez les groupes de règles de QoS adaptatifs

Vous pouvez utiliser un groupe de règles *Adaptive QoS* pour dimensionner automatiquement un plafond de débit ou une taille de sol en fonction du volume, tout en maintenant le rapport IOPS/To|GBs lorsque la taille du volume change. C'est un avantage significatif pour la gestion de centaines, voire de milliers de charges de travail dans un déploiement à grande échelle.

Avant de commencer

- Vous devez exécuter ONTAP 9.3 ou une version ultérieure. Les groupes de règles de QoS adaptative sont disponibles à partir de la version ONTAP 9.3.
- Pour créer une « policy group » il faut être un administrateur de cluster.

Description de la tâche

Un objet de stockage peut être membre d'un groupe de règles adaptative ou d'un groupe de règles non adaptatif, mais pas des deux à la fois. Le SVM de l'objet de stockage et la politique doivent être identiques. L'objet de stockage doit être en ligne.

Les groupes de règles de QoS adaptative sont toujours non partagés : le plafond ou l'étage de débit défini s'applique à chaque charge de travail membre individuellement.

Le rapport entre les limites de débit et la taille de l'objet de stockage est déterminé par l'interaction des champs suivants :

- `expected-iops` Correspond au nombre minimal d'IOPS prévu par To|Go alloué.

> `expected-iops` Est garanti sur les plateformes AFF uniquement. `expected-iops` La garantie pour FabricPool est uniquement si la règle de Tiering est définie sur « aucune » et qu'aucun bloc n'est présent dans le cloud. `expected-iops` Est garanti pour les volumes qui ne font pas partie d'une relation SnapMirror synchrone.

- `peak-iops` Est le nombre maximal d'IOPS possible par To alloué ou utilisé|Go.
- `expected-iops-allocation` indique si l'espace alloué (par défaut) ou utilisé est utilisé pour les iops attendues.

> `expected-iops-allocation` Est disponible dans ONTAP 9.5 et versions ultérieures. Elle n'est pas prise en charge par ONTAP 9.4 et les versions antérieures.

- `peak-iops-allocation` indique si l'espace alloué ou l'espace utilisé (par défaut) est utilisé pour `peak-iops`.
- `absolute-min-iops` Correspond au nombre minimal d'IOPS absolu. Vous pouvez utiliser ce champ avec de très petits objets de stockage. Elle remplace les deux `peak-iops` et/ou `expected-iops` quand `absolute-min-iops` est supérieur au calcul `expected-iops`.

  Par exemple, si vous définissez `expected-iops` À 1,000 000 IOPS/To et la taille du volume est inférieure à 1 Go, le calcul est effectué `expected-iops` Il s'agit d'une IOP fractionnaires. Le calculé `peak-iops` sera une fraction encore plus petite. Vous pouvez éviter cela en définissant le paramètre `absolute-min-iops` à une valeur réaliste.

- `block-size` Spécifie la taille du bloc d'E/S de l'application. La valeur par défaut est 32 Ko. Les valeurs valides sont de 8 Ko, 16 Ko, 32 K, 64 Ko, N'IMPORTE QUEL. TOUTE signifie que la taille de bloc n'est pas appliquée.

Trois groupes de règles de QoS adaptative par défaut sont disponibles, comme illustré dans le tableau ci-dessous. Vous pouvez appliquer ces « policy group » directement à un volume.

Groupe de règles par défaut	IOPS/To attendu	Pic d'IOPS/To	IOPS min. Absolu
`extreme`	6,144	12,288	1000

`performance`	2,048	4,096	500
`value`	128	512	75

Vous ne pouvez pas affecter un objet de stockage à un groupe de règles si son objet contenant ou ses objets enfants appartiennent à un groupe de règles. Le tableau suivant répertorie les restrictions.

Si vous attribuez…	**Vous ne pouvez alors pas affecter…**
SVM vers une « policy group »	Tout objet de stockage contenu par la SVM vers une « policy group »
Volume vers une « policy group »	Le volume contenant un SVM ou toute LUN enfant vers un « policy group »
LUN vers une « policy group »	La LUN contenant le volume ou le SVM à une « policy group »
Fichier dans une « policy group »	Fichier contenant le volume ou SVM vers une « policy group »

Étapes

1. Création d'une « policy group » QoS adaptative :

   `qos adaptive-policy-group create -policy group` *`policy_group`* `-vserver` *`SVM`* `-expected-iops` *`number_of_iops`*`/TB|GB -peak-iops` *`number_of_iops`*`/TB|GB -expected -iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-space -absolute-min-iops` *`number_of_iops`* `-block-size 8K|16K|32K|64K|ANY`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > `-expected-iops-allocation` et `-block-size` Est disponible dans ONTAP 9.5 et versions ultérieures. Ces options ne sont pas prises en charge par ONTAP 9.4 et les versions antérieures.

   La commande suivante crée une « policy group » QoS adaptative `adpg-app1` avec `-expected-iops` Défini sur 300 IOPS/To, `-peak-iops` Définis sur 1,000 IOPS/To, `-peak-iops-allocation` réglez sur `used-space`, et `-absolute-min-iops` Définissez sur 50 IOPS :

   ```
   cluster1::> qos adaptive-policy-group create -policy group adpg-app1
   -vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
   -allocation used-space -absolute-min-iops 50iops
   ```

2. Appliquer une « policy group » QoS adaptative à un volume :

   `volume create -vserver SVM -volume` *`volume`* `-aggregate` *`aggregate`* `-size` *`number_of`* `TB|GB -qos-adaptive-policy-group` *`policy_group`*

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

La commande suivante applique la « policy group » de QoS adaptative `adpg-app1` au volume `app1`:

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

Les commandes suivantes appliquent le groupe de règles de QoS adaptative par défaut `extreme` au nouveau volume `app4` et au volume existant `app5`. Le plafond de débit défini pour le groupe de règles s'applique aux volumes `app4` et `app5` chaque participant :

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

Définissez un modèle de groupe de règles adaptatives

À partir de la ONTAP 9.13.1, vous pouvez appliquer des seuils et des plafonds de débit au niveau des SVM en utilisant un modèle de groupe de règles adaptatif.

Description de la tâche

- Le modèle de groupe de règles adaptatives est une règle par défaut `apg1`. La règle peut être modifiée à tout moment. Elle peut uniquement être définie avec l'interface de ligne de commandes ou l'API REST de ONTAP et s'applique uniquement aux SVM existants.
- Le modèle de groupe de règles adaptatives n'a d'impact que sur les volumes créés sur le SVM ou migrés vers celui-ci une fois la règle définie. Les volumes existants de la SVM conservent leur état existant.

  Si vous désactivez le modèle de « Adaptive policy group », les volumes de la SVM conservent leurs règles existantes. Seuls les volumes créés ou migrés vers le SVM seront affectés par l'interruption.

- Vous ne pouvez pas définir de modèle de « policy group » adaptatif sur une SVM disposant d'une « policy group » QoS.
- Les modèles de groupes de règles adaptatifs sont conçus pour les plateformes AFF. Un modèle de groupe de règles adaptatives peut être défini sur d'autres plates-formes, mais la stratégie peut ne pas imposer un débit minimal. De même, vous pouvez ajouter un modèle de groupe de règles adaptatives à un SVM dans un agrégat FabricPool ou dans un agrégat ne prenant pas en charge un débit minimal, mais le débit ne sera pas appliqué.
- Si le SVM se trouve dans une configuration MetroCluster ou une relation SnapMirror, le modèle de groupe de règles adaptatives sera appliqué sur le SVM en miroir.

Étapes

1. Modifier le SVM pour appliquer le modèle Adaptive policy group :
   `vserver modify -qos-adaptive-policy-group-template apg1`

2. Vérifiez que la règle a été définie :
   `vserver show -fields qos-adaptive-policy-group`

Surveillez les performances des clusters avec Unified Manager

Avec Active IQ Unified Manager, vous optimisez la disponibilité et gardez le contrôle de votre infrastructure de stockage NetApp AFF et FAS pour améliorer l'évolutivité, la prise en charge, les performances et la sécurité.

Active IQ Unified Manager surveille en permanence l'état du système et envoie des alertes pour permettre à votre entreprise de libérer des ressources IT. Vous pouvez consulter les informations sur l'état du stockage à partir d'un seul tableau de bord et résoudre rapidement les problèmes à l'aide d'actions recommandées.

La gestion des données est simplifiée grâce aux fonctionnalités de détection, de contrôle et de notification vous permettant de gérer le stockage de manière proactive et de résoudre rapidement les problèmes. L'administration est plus efficace, car elle permet de surveiller plusieurs pétaoctets de données à partir d'un même tableau de bord et de gérer vos données à grande échelle.

Grâce à Active IQ Unified Manager, vous pouvez vous adapter à l'évolution des besoins de votre business tout en optimisant les performances à l'aide des données de performance et des fonctionnalités d'analytique avancée. Les fonctionnalités de création de rapports vous permettent d'accéder à des rapports standard ou de créer des rapports opérationnels personnalisés afin de répondre aux besoins spécifiques de votre entreprise.

Liens connexes :

- "En savoir plus sur Active IQ Unified Manager"
- "Lancez-vous avec Active IQ Unified Manager"
- "Découvrez Active IQ Unified Manager pour Linus"
- "Lancez-vous avec Active IQ Unified Manager pour Windows"

Contrôle des performances du cluster avec Cloud Insights

NetApp Cloud Insights est un outil de surveillance qui permet d'avoir une grande visibilité sur l'ensemble de l'infrastructure. Avec Cloud Insights, vous pouvez surveiller toutes les ressources, les optimiser et résoudre les problèmes, y compris dans les clouds publics et dans vos data centers privés.

Cloud Insights est disponible en deux éditions

La version de base de Cloud Insights a été spécialement conçue pour contrôler et optimiser les ressources NetApp Data Fabric. Ce logiciel assure une analytique avancée pour établir des connexions entre toutes les ressources NetApp, y compris les systèmes FAS AFF et HCI dans l'environnement.

L'édition Standard de Cloud Insights est axée non seulement sur les composants d'infrastructure NetApp Data Fabric, mais aussi sur les environnements multifournisseurs et multicloud. Grâce à ses fonctionnalités enrichies, vous pouvez accéder à plus de 100 services et ressources.

Dans le monde actuel, avec des ressources en jeu entre vos data centers sur site et plusieurs clouds publics, il est essentiel d'avoir une vue d'ensemble de l'application elle-même et du disque interne de la baie de

stockage. La prise en charge supplémentaire de la surveillance des applications (comme Kafka, MongoDB et Nginx) vous fournit les informations et les connaissances nécessaires pour fonctionner au niveau optimal d'utilisation ainsi qu'avec le tampon à risques idéal.

Ces deux éditions (de base et standard) peuvent s'intégrer avec NetApp Active IQ Unified Manager. Les clients qui utilisent Active IQ Unified Manager peuvent voir les informations de jointure dans l'interface utilisateur de Cloud Insights. Les notifications publiées sur Active IQ Unified Manager ne sont pas négligées et peuvent être corrélées aux événements dans Cloud Insights. En d'autres termes, vous bénéficiez du meilleur des deux mondes.

Surveillance, dépannage et optimisation de toutes vos ressources

Cloud Insights vous aide à réduire considérablement le délai de résolution des problèmes et à éviter qu'ils n'impactent les utilisateurs finaux. Mais les coûts de l'infrastructure cloud sont également réduits. L'exposition aux menaces internes est réduite en protégeant les données à l'aide d'informations exploitables.

Avec Cloud Insights, vous disposez d'une visibilité complète sur l'ensemble de votre infrastructure hybride à un seul emplacement, du cloud public à votre data Center. Vous pouvez créer instantanément des tableaux de bord pertinents qui peuvent être personnalisés en fonction de vos besoins spécifiques. Vous pouvez également créer des alertes ciblées et conditionnelles spécifiques aux besoins de votre entreprise.

La détection avancée des anomalies vous aide à résoudre les problèmes de manière préventive et proactive. Vous pouvez visualiser automatiquement les conflits et la dégradation des ressources pour restaurer rapidement les workloads impactés. La résolution des problèmes est plus rapide grâce à la hiérarchisation automatique des relations entre les différents composants de votre pile.

Vous pouvez identifier les ressources inutilisées ou orphelines dans votre environnement. Elles vous indiquent comment dimensionner correctement votre infrastructure et optimiser toutes vos dépenses.

Cloud Insights visualise votre topologie système pour mieux comprendre l'architecture Kubernetes. Vous pouvez contrôler l'état des clusters Kubernetes, y compris les nœuds susceptibles de rencontrer des problèmes, puis zoomer en cas de problème.

Cloud Insights vous aide à protéger les données de l'entreprise contre les activités abusives ou les usurpations d'identité à l'aide de fonctionnalités avancées de machine learning et de détection des anomalies qui vous fournissent des informations exploitables sur les menaces internes.

Cloud Insights vous aide à visualiser les metrics Kubernetes de façon à comprendre pleinement les relations entre vos pods, vos nœuds et vos clusters. Vous pouvez évaluer l'état d'un cluster ou d'un module de travail, ainsi que la charge en cours de traitement, ce qui vous permet de prendre le contrôle de votre cluster K8S et de contrôler à la fois l'état de santé et le coût de votre déploiement.

Liens connexes

- "En savoir plus sur Cloud Insights"
- "Lancez-vous avec Cloud Insights"

Consignation des audits

Mise en œuvre de la journalisation des audits par ONTAP

Les activités de gestion enregistrées dans le journal d'audit sont incluses dans les rapports AutoSupport standard et certaines activités de consignation sont incluses dans

les messages EMS. Vous pouvez également transférer le journal d'audit aux destinations que vous spécifiez et afficher les fichiers journaux d'audit à l'aide de l'interface de ligne de commande ou d'un navigateur Web.

Depuis ONTAP 9.11.1, vous pouvez afficher le contenu des journaux d'audit à l'aide de System Manager.

Depuis ONTAP 9.12.1, ONTAP fournit des alertes de falsification pour les journaux d'audit. ONTAP exécute une tâche d'arrière-plan quotidienne pour vérifier l'altération des fichiers audit.log et envoie une alerte EMS s'il trouve des fichiers journaux qui ont été modifiés ou falsifiés.

ONTAP consigne les activités de gestion qui sont effectuées sur le cluster, par exemple la requête émise, l'utilisateur qui a déclenché la demande, la méthode d'accès de l'utilisateur et l'heure de la demande.

Les activités de gestion peuvent être de l'un des types suivants :

- DÉFINIR les demandes, qui s'appliquent généralement aux commandes ou opérations non affichées
  - Ces demandes sont émises lorsque vous exécutez un `create`, `modify`, ou `delete` commande, par exemple.
  - Les demandes de série sont consignées par défaut.
- OBTENIR les demandes, qui récupèrent les informations et les affichent dans l'interface de gestion
  - Ces demandes sont émises lorsque vous exécutez un `show` commande, par exemple.
  - Les demandes GET ne sont pas consignées par défaut, mais vous pouvez contrôler si LES demandes GET sont envoyées depuis l'interface de ligne de commande ONTAP (`-cliget`), à partir de l'API ONTAP (`-ontapiget`), ou à partir de l'API REST (`-httpget`) sont consignés dans le fichier.

ONTAP enregistre les activités de gestion dans `/mroot/etc/log/mlog/audit.log` fichier d'un nœud. Les commandes des trois shells pour les commandes CLI—le clustershell, le nodeshell et le systemshell non-interactif (les commandes du systemshell interactives ne sont pas consignées)--ainsi que les commandes d'API sont consignées ici. Les journaux d'audit incluent des horodatages pour indiquer si tous les nœuds d'un cluster sont synchronisés.

Le `audit.log` Le fichier est envoyé par l'outil AutoSupport aux destinataires spécifiés. Vous pouvez également transférer le contenu en toute sécurité vers des destinations externes que vous spécifiez (par exemple, un serveur Splunk ou syslog).

Le `audit.log` le fichier fait l'objet d'une rotation quotidienne. La rotation se produit également lorsqu'elle atteint 100 Mo et que les 48 copies précédentes sont conservées (avec un total maximum de 49 fichiers). Lorsque le fichier d'audit effectue sa rotation quotidienne, aucun message EMS n'est généré. Si le fichier d'audit tourne parce que sa taille limite de fichier est dépassée, un message EMS est généré.

Modifications de la journalisation des audits dans ONTAP 9

À partir de ONTAP 9, le `command-history.log` le fichier est remplacé par `audit.log`, et le `mgwd.log` le fichier ne contient plus d'informations d'audit. Si vous effectuez une mise à niveau vers ONTAP 9, il est recommandé de consulter les scripts ou les outils qui font référence aux fichiers hérités et à leur contenu.

Après la mise à niveau vers ONTAP 9, existant `command-history.log` les fichiers sont conservés. Ils sont tournés vers l'extérieur (supprimés) comme nouveaux `audit.log` les fichiers sont pivotés dans (créés).

Outils et scripts qui vérifient le `command-history.log` le fichier peut continuer à fonctionner, car un lien logiciel de `command-history.log` à `audit.log` est créée lors de la mise à niveau. Cependant, les outils et les scripts qui vérifient le `mgwd.log` le fichier échoue, car ce fichier ne contient plus d'informations d'audit.

Les journaux d'audit dans ONTAP 9 et les versions ultérieures n'incluent plus les entrées suivantes, car elles ne sont pas considérées comme utiles et n'entraînent pas d'activité de journalisation inutile :

- Commandes internes exécutées par ONTAP (c'est-à-dire où username=root)
- Alias de commande (séparément de la commande à laquelle ils pointent)

Depuis ONTAP 9, vous pouvez transmettre les journaux d'audit de manière sécurisée vers des destinations externes à l'aide des protocoles TCP et TLS.

Afficher le contenu du journal d'audit

Vous pouvez afficher le contenu du cluster `/mroot/etc/log/mlog/audit.log` Fichiers via l'interface de ligne de commandes de ONTAP, System Manager ou un navigateur Web.

Les entrées du fichier journal du cluster sont les suivantes :

Temps
Horodatage de l'entrée du journal.

Client supplémentaire
Application utilisée pour se connecter au cluster. Voici des exemples de valeurs possibles `internal, console, ssh, http, ontapi, snmp, rsh, telnet,` et `service-processor`.

Utilisateur
Nom d'utilisateur de l'utilisateur distant.

État
État actuel de la demande d'audit, qui pourrait être `success, pending,` ou `error`.

Messagerie
Champ facultatif qui peut contenir une erreur ou des informations supplémentaires sur l'état d'une commande.

ID de session
ID de session sur lequel la demande est reçue. Un ID de session est attribué à chaque session SSH *session*, tandis que chaque HTTP, ONTAPI ou SNMP *request* se voit attribuer un ID de session unique.

VM de stockage
SVM via lequel l'utilisateur a connecté.

Portée
S'affiche `svm` Lorsque la demande se trouve sur une machine virtuelle de stockage de données ; dans le cas contraire, s'affiche `cluster`.

ID de commande

ID de chaque commande reçue lors d'une session CLI. Cela vous permet de mettre en corrélation une demande et une réponse. Les requêtes ZAPI, HTTP et SNMP ne possèdent pas d'ID de commande.

Vous pouvez afficher les entrées des journaux du cluster depuis l'interface de ligne de commandes de ONTAP, depuis un navigateur Web et depuis ONTAP 9.11.1, depuis System Manager.

System Manager

- Pour afficher l'inventaire, sélectionnez **Evénements et travaux > journaux d'audit**.
  Chaque colonne dispose de commandes pour filtrer, trier, rechercher, afficher et inventorier les catégories. Les détails de l'inventaire peuvent être téléchargés sous forme de classeur Excel.
- Pour définir des filtres, cliquez sur le bouton **Filter** en haut à droite, puis sélectionnez les champs souhaités.
  Vous pouvez également afficher toutes les commandes exécutées dans la session au cours de laquelle un échec s'est produit en cliquant sur le lien ID de session.

CLI

Pour afficher les entrées d'audit fusionnées à partir de plusieurs nœuds du cluster, entrez :
`security audit log show` *`[parameters]`*

Vous pouvez utiliser le `security audit log show` commande permettant d'afficher les entrées d'audit de nœuds individuels ou fusionnées à partir de plusieurs nœuds du cluster. Vous pouvez également afficher le contenu du `/mroot/etc/log/mlog` répertoire sur un seul nœud à l'aide d'un navigateur web.
Voir la page man pour plus de détails.

Navigateur Web

Vous pouvez afficher le contenu du `/mroot/etc/log/mlog` répertoire sur un seul nœud à l'aide d'un navigateur web. "Découvrez comment accéder aux fichiers log, core dump et MIB d'un nœud à l'aide d'un navigateur Web".

Gérer les paramètres de demande GET d'audit

Lorsque LES demandes DÉFINIES sont consignées par défaut, les demandes GET ne le sont pas. Cependant, vous pouvez contrôler si LES requêtes GET sont envoyées depuis ONTAP HTML (`-httpget`), l'interface de ligne de commande ONTAP (`-cliget`), ou à partir des API ONTAP (`-ontapiget`) sont consignés dans le fichier.

Vous pouvez modifier les paramètres de la journalisation des audits depuis l'interface de ligne de commandes de ONTAP et depuis ONTAP 9.11.1 depuis System Manager.

System Manager

1. Sélectionnez **événements et travaux > journaux d'audit**.
2. Cliquez sur dans le coin supérieur droit, choisissez les demandes à ajouter ou à supprimer.

CLI

- Pour spécifier que les demandes GET depuis l'interface de ligne de commande ou les API ONTAP doivent être enregistrées dans le journal d'audit (fichier audit.log), en plus des demandes SET par défaut, entrez :
  `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- Pour afficher les paramètres actuels, entrez :
  `security audit show`

Consultez les pages de manuel pour plus de détails.

Gérer les destinations du journal d'audit

Vous pouvez transférer le journal d'audit vers un maximum de 10 destinations. Par exemple, vous pouvez transférer le journal vers un serveur Splunk ou syslog à des fins de surveillance, d'analyse ou de sauvegarde.

Description de la tâche

Pour configurer le transfert, vous devez fournir l'adresse IP de l'hôte syslog ou Splunk, son numéro de port, un protocole de transmission et la fonction syslog à utiliser pour les journaux transférés. "En savoir plus sur les installations de syslog".

Vous pouvez sélectionner l'une des valeurs de transmission suivantes :

UDP non crypté
: Protocole de datagramme utilisateur sans sécurité (par défaut)

TCP non chiffré
: Protocole de contrôle de transmission sans sécurité

TCP chiffré
: Protocole de contrôle de transmission avec TLS (transport Layer Security)
Une option **Verify Server** est disponible lorsque le protocole TCP chiffré est sélectionné.

Vous pouvez transférer les journaux d'audit depuis l'interface de ligne de commandes de ONTAP et depuis ONTAP 9.11.1 depuis System Manager.

System Manager

- Pour afficher les destinations du journal d'audit, sélectionnez **Cluster > Paramètres**.
  Le nombre de destinations du journal s'affiche dans la mosaïque **gestion des notifications**. Cliquez sur ⋮ pour afficher les détails.
- Pour ajouter, modifier ou supprimer des destinations du journal d'audit, sélectionnez **Evénements et travaux > journaux d'audit**, puis cliquez sur **gérer destinations d'audit** dans le coin supérieur droit de l'écran.
  Cliquez sur + Add ou cliquez sur ⋮ Dans la colonne **adresse hôte** pour modifier ou supprimer des entrées.

CLI

1. Pour chaque destination vers laquelle vous souhaitez transférer le journal d'audit, spécifiez l'adresse IP ou le nom d'hôte de destination et les options de sécurité.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

   - Si le `cluster log-forwarding create` la commande ne peut pas envoyer de requête ping à l'hôte de destination pour vérifier la connectivité, la commande échoue avec une erreur. Bien qu'il ne soit pas recommandé, utiliser le `-force` le paramètre utilisé avec la commande ignore la vérification de connectivité.
   - Lorsque vous définissez le `-verify-server` paramètre à `true`, l'identité de la destination de transfert de journal est vérifiée en validant son certificat. Vous pouvez définir la valeur sur `true` uniquement lorsque vous sélectionnez `tcp-encrypted` valeur dans le `-protocol` légale.

2. Vérifiez que les enregistrements de destination sont corrects à l'aide du `cluster log-forwarding show` commande.

```
cluster1::> cluster log-forwarding show

                                                Verify Syslog
Destination Host          Port   Protocol       Server Facility
------------------------- ------ -------- ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            514    tcp-encrypted   true   user
2 entries were displayed.
```

Consultez les pages de manuel pour plus de détails.

AutoSupport

Gérez les paramètres AutoSupport avec System Manager

Vous pouvez utiliser System Manager pour gérer les paramètres de votre compte AutoSupport.

Vous pouvez effectuer les opérations suivantes :

Afficher les paramètres AutoSupport

Vous pouvez utiliser System Manager pour afficher les paramètres de votre compte AutoSupport.

Étapes

1. Dans System Manager, cliquez sur **Cluster > Paramètres**.

   Dans la section **AutoSupport**, les informations suivantes sont affichées :

   - État
   - Protocole de transport
   - Serveur proxy
   - De l'adresse e-mail
2. Dans la section **AutoSupport**, sélectionnez ⋮, Puis sélectionnez **plus d'options**.

   Des informations supplémentaires s'affichent sur la connexion AutoSupport et les paramètres de messagerie. De plus, l'historique des transferts de messages est répertorié.

Générez et envoyez des données AutoSupport

Dans System Manager, vous pouvez lancer la génération de messages AutoSupport et choisir entre le nœud de cluster ou les nœuds où les données sont collectées.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, sélectionnez ⋮, Puis sélectionnez **générer et Envoyer**.
3. Saisissez un objet.
4. Cochez la case sous **collecter les données de** pour spécifier les nœuds à partir desquels collecter les données.

Testez la connexion à AutoSupport

Depuis System Manager, vous pouvez envoyer un message de test pour vérifier la connexion à AutoSupport.

Étapes

1. Dans System Manager, cliquez sur **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, sélectionnez ⋮, Puis sélectionnez **Tester la connectivité**.
3. Saisissez un objet pour le message.

Activez ou désactivez le protocole AutoSupport

AutoSupport offre aux clients NetApp des avantages éprouvés, notamment l'identification proactive d'éventuels problèmes de configuration et l'accélération de la résolution des dossiers de support. AutoSupport est activé par défaut sur les nouveaux systèmes. Si nécessaire, vous pouvez utiliser System Manager pour désactiver la fonction AutoSupport de surveillance de l'état de santé du système de stockage et vous envoyer des messages de notification. Vous pouvez à nouveau activer AutoSupport après sa désactivation.

Description de la tâche

Avant de désactiver AutoSupport, vous devez savoir que vous désactivez le système d'appel à distance NetApp et que vous perdrez les avantages suivants :

- **Surveillance de l'état** : AutoSupport surveille l'état de santé de votre système de stockage et envoie des notifications au support technique et à votre service de support interne.
- **Automatisation** : AutoSupport automatise le reporting des dossiers de support. La plupart des dossiers de demande de support sont ouverts automatiquement avant que les clients n'aient conscience d'un problème.
- **Résolution plus rapide** : les dossiers de support des systèmes qui envoient des données AutoSupport sont résolus en deux fois moins de temps que ceux des systèmes qui n'envoient pas de données AutoSupport.
- **Mises à niveau plus rapides** : AutoSupport optimise les flux de travail en libre-service des clients, tels que les mises à niveau de version, les modules complémentaires, les renouvellements et l'automatisation des mises à jour de firmware dans System Manager.
- **Autres fonctions** : certaines fonctions d'autres outils ne fonctionnent que lorsque AutoSupport est activé, par exemple, certains flux de travail dans BlueXP.

Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, sélectionnez ⋮, Puis sélectionnez **Désactiver**.
3. Si vous souhaitez réactiver AutoSupport, dans la section **AutoSupport**, sélectionnez ⋮, Puis sélectionnez **Activer**.

Supprimez la génération des dossiers de demande de support

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour envoyer une demande à AutoSupport afin de supprimer la génération des dossiers de demande de support.

Description de la tâche

Pour supprimer la génération de dossiers de demande de support, vous spécifiez les nœuds et le nombre d'heures pour lesquels la suppression doit avoir lieu.

La suppression de dossiers de demande de support peut être particulièrement utile si vous ne souhaitez pas que AutoSupport crée des dossiers automatisés pendant que vous effectuez la maintenance de vos systèmes.

Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, sélectionnez ⋮, Puis sélectionnez **Supprimer support case Generation**.
3. Saisissez le nombre d'heures pendant lesquelles vous souhaitez que la suppression se produise.
4. Sélectionnez les nœuds pour lesquels vous souhaitez que la suppression se produise.

Reprendre la génération des dossiers de demande de support

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour reprendre la génération d'demandes de support avec AutoSupport si elles ont été supprimées.

Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, sélectionnez ⋮, Puis sélectionnez **Resume support case Generation**.
3. Sélectionnez les nœuds pour lesquels vous souhaitez que la génération reprenne.

Modifier les paramètres AutoSupport

System Manager permet de modifier les paramètres de connexion et de messagerie de votre compte AutoSupport.

Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, sélectionnez ⋮, Puis sélectionnez **plus d'options**.
3. Dans la section **connexions** ou **Courriel**, sélectionnez Edit pour modifier les paramètres de chaque section.

Gérez AutoSupport avec l'interface de ligne de commandes

Présentation de Manage AutoSupport

AutoSupport est un mécanisme qui surveille de manière proactive l'état de votre système et envoie automatiquement des messages au support technique NetApp, à votre organisation de support interne et à un partenaire de support. Bien que les messages AutoSupport au support technique soient activés par défaut, vous devez définir les options correctes et disposer d'un hôte de messagerie valide pour que les messages soient envoyés à votre service de support interne.

Seul l'administrateur du cluster peut effectuer la gestion AutoSupport. L'administrateur du SVM (Storage Virtual machine) n'a pas accès à AutoSupport.

L'option AutoSupport est activée par défaut lorsque vous configurez votre système de stockage pour la première fois. L'AutoSupport envoie des messages au support technique sous 24 heures après l'activation de AutoSupport. Vous pouvez réduire cette période de 24 heures en mettant à niveau ou en restaurer le système, en modifiant la configuration AutoSupport ou en modifiant l'heure du système pour une période différente de 24 heures.

> ⓘ Vous pouvez désactiver AutoSupport à tout moment, mais vous devez l'activer. L'activation d'AutoSupport peut considérablement accélérer l'identification et la résolution des problèmes sur votre système de stockage. Par défaut, le système collecte les informations AutoSupport et les stocke localement, même si vous désactivez AutoSupport.

Pour en savoir plus sur AutoSupport, consultez le site de support NetApp.

Informations associées

- "Support NetApp"

- "Pour en savoir plus sur les commandes AutoSupport, consultez l'interface de ligne de commandes de ONTAP"

Utilisez AutoSupport et Active IQ Digital Advisor

Le composant AutoSupport de ONTAP collecte les données de télémétrie et les envoie pour analyse. Le conseiller digital Active IQ analyse les données d'AutoSupport et fournit un support proactif et une optimisation. Avec l'intelligence artificielle, Active IQ peut identifier les problèmes potentiels et vous aider à les résoudre avant qu'ils n'affectent votre activité.

Active IQ vous permet d'optimiser votre infrastructure de données dans l'ensemble de votre cloud hybride grâce à un portail cloud et à une application mobile qui offrent des analyses prédictives et un support proactif. Les informations et les recommandations basées sur les données de Active IQ sont accessibles à tous les clients NetApp qui possèdent un contrat SupportEdge actif (les fonctionnalités varient selon le produit et le niveau de support).

Voici quelques avantages que vous pouvez faire avec Active IQ :

- Planification des mises à niveau. Active IQ identifie les problèmes qui peuvent être résolus dans votre environnement en effectuant une mise à niveau vers la plus récente version d'ONTAP et le composant Upgrade Advisor vous aide à planifier une mise à niveau réussie.
- Voir le bien-être du système. Votre tableau de bord Active IQ signale tout problème éventuel et vous aide à le corriger. Surveillez la capacité du système pour vous assurer que votre espace de stockage est insuffisant. Consultez les dossiers de demande de support de votre système.
- Gestion des performances. Active IQ affiche les performances du système sur une période plus longue que ce que vous pouvez voir dans System Manager. Identifiez les problèmes de configuration et de système qui ont un impact sur les performances.
- Optimisez l'efficacité. Affichez les mesures de l'efficacité du stockage et identifiez des moyens de stocker plus de données dans moins d'espace.
- Voir l'inventaire et la configuration. Active IQ affiche des informations complètes sur l'inventaire et la configuration logicielle et matérielle. Voyez quand les contrats de service arrivent à expiration et renouvelez-les pour vous assurer que vous restez pris en charge.

Informations associées

"Documentation NetApp : conseiller digital Active IQ"

"Lancez Active IQ"

"Services SupportEdge"

Quand et où les messages AutoSupport sont envoyés

AutoSupport envoie des messages à différents destinataires, en fonction du type de message. Savoir où et quand envoyer des messages AutoSupport peut vous aider à comprendre les messages que vous recevez par e-mail ou consultez le site Web Active IQ (anciennement My AutoSupport).

Sauf indication contraire, les paramètres dans les tableaux suivants sont des paramètres de l' `system node autosupport modify` commande.

Messages déclenchés par des événements

Lorsque des événements se produisent sur le système qui nécessitent une action corrective, AutoSupport envoie automatiquement un message déclenché par un événement.

Lorsque le message est envoyé	Où le message est envoyé
AutoSupport répond à un événement de déclenchement dans l'EMS	Adresses spécifiées dans `-to` et `-noteto`. (Seuls les événements critiques affectant le service sont envoyés.) Adresses spécifiées dans `-partner-address` Support technique, si `-support` est défini sur `enable`

Messages programmés

AutoSupport envoie automatiquement plusieurs messages selon un calendrier normal.

Lorsque le message est envoyé	Où le message est envoyé
Quotidien (par défaut, envoyé entre 12 h 00 et 1 h 00 en tant que message de journal)	Adresses spécifiées dans `-partner-address` Support technique, si `-support` est défini sur `enable`
Quotidien (par défaut, envoyé entre 12 h 00 et 1 h 00 comme un message de performance), si le `-perf` le paramètre est défini sur `true`	Adresses spécifiées dans -adresse-partenaire» Support technique, si `-support` est défini sur `enable`
Hebdomadaire (par défaut, envoyé le dimanche entre 12 h 00 et 1 h 00)	Adresses spécifiées dans `-partner-address` Support technique, si `-support` est défini sur `enable`

Messages déclenchés manuellement

Vous pouvez lancer ou renvoyer manuellement un message AutoSupport.

Lorsque le message est envoyé	Où le message est envoyé
Vous lancez manuellement un message à l'aide de `system node autosupport invoke` commande	Si un URI est spécifié à l'aide de `-uri` paramètre dans le `system node autosupport invoke` Commande, le message est envoyé à cet URI. Si `-uri` est omis, le message est envoyé aux adresses spécifiées dans `-to` et `-partner -address`. Le message est également envoyé au support technique si `-support` est défini sur `enable`.
Vous lancez manuellement un message à l'aide de `system node autosupport invoke-core-upload` commande	Si un URI est spécifié à l'aide de `-uri` paramètre dans le `system node autosupport invoke-core-upload` Commande, le message est envoyé à cet URI, et le fichier core dump est chargé sur l'URI. Si `-uri` est omis dans le `system node autosupport invoke-core-upload` commande, le message est envoyé au support technique et le fichier « core dump » est chargé sur le site du support technique. Cela est nécessaire dans les deux cas `-support` est défini sur `enable` et `-transport` est défini sur `https` ou `http`. En raison de la grande taille des fichiers core dump, le message n'est pas envoyé aux adresses spécifiées dans l' `-to` et `-partner-addresses` paramètres.
Vous lancez manuellement un message à l'aide de `system node autosupport invoke-performance-archive` commande	Si un URI est spécifié à l'aide de `-uri` paramètre dans le `system node autosupport invoke-performance-archive` Commande, le message est envoyé à cet URI, et le fichier d'archive de performances est chargé dans l'URI. Si `-uri` est omis dans le `system node autosupport invoke-performance-archive`, le message est envoyé au support technique et le fichier d'archive de performances est chargé sur le site de support technique. Cela est nécessaire dans les deux cas `-support` est défini sur `enable` et `-transport` est défini sur `https` ou `http`. En raison de la taille importante des fichiers d'archivage de performances, le message n'est pas envoyé aux adresses spécifiées dans l' `-to` et `-partner-addresses` paramètres.

Lorsque le message est envoyé	Où le message est envoyé
Vous renvoyez manuellement un message précédent à l'aide de `system node autosupport history retransmit` commande	Uniquement à l'URI que vous spécifiez dans le `-uri` paramètre du `system node autosupport history retransmit` commande

Messages déclenchés par le support technique

Le support technique peut demander des messages à AutoSupport avec la fonction AutoSupport OnDemand.

Lorsque le message est envoyé	Où le message est envoyé
Quand AutoSupport obtient les instructions de livraison pour générer de nouveaux messages AutoSupport	Adresses spécifiées dans `-partner-address` Support technique, si `-support` est défini sur `enable` et `-transport` est défini sur `https`
Quand AutoSupport obtient des instructions de livraison pour renvoyer les messages AutoSupport précédents	Support technique, si `-support` est défini sur `enable` et `-transport` est défini sur `https`
Quand AutoSupport obtient des instructions de livraison pour générer de nouveaux messages AutoSupport qui chargent des fichiers core dump ou d'archivage des performances	Support technique, si `-support` est défini sur `enable` et `-transport` est défini sur `https`. Le fichier « core dump » ou d'archivage des performances est téléchargé sur le site du support technique.

Comment AutoSupport crée et envoie des messages déclenchés par des événements

AutoSupport crée des messages AutoSupport déclenchés par les événements lorsque le système EMS traite un événement déclencheur. Un message AutoSupport déclenché par un événement alerte les destinataires des problèmes qui requièrent une action corrective et ne contient que des informations pertinentes pour le problème. Vous pouvez personnaliser le contenu à inclure et qui reçoit les messages.

AutoSupport utilise le processus suivant pour créer et envoyer des messages AutoSupport déclenchés par les événements :

1. Lorsque l'EMS traite un événement déclencheur, EMS envoie une requête à AutoSupport.

   Un événement déclencheur est un événement EMS avec une destination AutoSupport et un nom commençant par un `callhome.` préfixe.

2. AutoSupport crée un message AutoSupport déclenché par un événement.

   AutoSupport collecte des informations de base et de dépannage des sous-systèmes associés au déclencheur afin de créer un message contenant uniquement les informations pertinentes pour l'événement de déclenchement.

   Un ensemble de sous-systèmes par défaut est associé à chaque déclencheur. Cependant, vous pouvez

choisir d'associer des sous-systèmes supplémentaires à un déclencheur en utilisant le `system node autosupport trigger modify` commande.

3. AutoSupport envoie le message AutoSupport déclenché par l'événement aux destinataires définis par le `system node autosupport modify` commande avec `-to`, `-noteto`, `-partner-address`, et `-support` paramètres.

   Vous pouvez activer et désactiver la transmission de messages AutoSupport pour des déclencheurs spécifiques à l'aide de la `system node autosupport trigger modify` commande avec `-to` et `-noteto` paramètres.

Exemple de données envoyées pour un événement spécifique

Le `storage shelf PSU failed` L'événement EMS déclenche un message contenant des données de base provenant des fichiers obligatoires, journaux, stockage, RAID, HA, Sous-systèmes de plate-forme et de mise en réseau et données de dépannage des sous-systèmes obligatoire, fichiers journaux et stockage.

Vous souhaitez inclure des données à propos de NFS dans tout message AutoSupport envoyé en réponse à une future `storage shelf PSU failed` événement. Vous entrez la commande suivante pour activer les données de dépannage de NFS pour le `callhome.shlf.ps.fault` événement :

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Notez que le `callhome.` le préfixe est supprimé du `callhome.shlf.ps.fault` événement lorsque vous utilisez le `system node autosupport trigger` Commandes ou lorsqu'elles sont référencées par des événements AutoSupport et EMS dans l'interface de ligne de commande.

Types de messages AutoSupport et leur contenu

Les messages AutoSupport contiennent des informations d'état sur les sous-systèmes pris en charge. Découvrez ce que contiennent les messages AutoSupport pour vous aider à interpréter les messages que vous recevez par e-mail ou à consulter sur le site Web Active IQ (anciennement My AutoSupport).

Type de message	Type de données que le message contient
Événement déclenché	Fichiers contenant des données contextuelles sur le sous-système spécifique où l'événement s'est produit
Tous les jours	Fichiers journaux
Performance	Données de performance échantillonnées au cours des 24 heures précédentes
Hebdomadaire	Données de configuration et d'état

Type de message	Type de données que le message contient
Déclenché par le `system node autosupport invoke` commande	Dépend de la valeur spécifiée dans `-type` paramètre : • `test` envoie un message déclenché par l'utilisateur avec certaines données de base. Ce message déclenche également une réponse automatique par e-mail du support technique à toutes les adresses e-mail spécifiées, à l'aide du `-to` Pour confirmer la réception des messages AutoSupport. • `performance` envoie des données de performance. • `all` envoie un message déclenché par l'utilisateur avec un ensemble complet de données similaires au message hebdomadaire, y compris les données de dépannage de chaque sous-système. L'assistance technique demande généralement ce message.
Déclenché par le `system node autosupport invoke-core-upload` commande	Fichiers core dump d'un nœud
Déclenché par le `system node autosupport invoke-performance-archive` commande	Fichiers d'archivage des performances pendant une période donnée
Déclenché par AutoSupport OnDemand	AutoSupport OnDemand peut demander de nouveaux messages ou des messages antérieurs : • Les nouveaux messages, selon le type de collection AutoSupport, peuvent être `test`, `all`, ou `performance`. • Les messages antérieurs dépendent du type de message renvoyé. AutoSupport OnDemand peut demander la création de nouveaux messages qui chargent les fichiers suivants sur le site de support NetApp à l'adresse "mysupport.netapp.com": • « Core dump » • Archivage des performances

Nature des sous-systèmes AutoSupport

Chaque sous-système fournit des informations de base et de dépannage utilisées par AutoSupport pour ses messages. Chaque sous-système est également associé aux événements de déclenchement qui permettent à AutoSupport de collecter uniquement à partir des informations pertinentes pour l'événement de déclenchement.

AutoSupport collecte du contenu sensible au contexte. Vous pouvez afficher des informations sur les sous-systèmes et déclencher des événements à l'aide du `system node autosupport trigger show` commande.

Taille et budgets de temps des AutoSupport

AutoSupport collecte des informations, organisées par sous-système, et applique une taille et un budget consacré au contenu pour chaque sous-système. Face à la croissance des systèmes de stockage, les budgets AutoSupport assurent un contrôle de la charge utile AutoSupport, ce qui assure une livraison évolutive des données AutoSupport.

AutoSupport cesse de collecter des informations et de tronquer AutoSupport le contenu du sous-système si sa taille ou son budget. Si le contenu ne peut pas être facilement tronqué (par exemple, les fichiers binaires), AutoSupport omet le contenu.

Vous devez modifier la taille et les budgets par défaut uniquement si le support NetApp vous y invite. Vous pouvez également consulter la taille et les budgets de temps par défaut des sous-systèmes en utilisant le `autosupport manifest show` commande.

Fichiers envoyés dans des messages AutoSupport déclenchés par un événement

Les messages AutoSupport déclenchés par des événements contiennent uniquement des informations de base et de dépannage des sous-systèmes associés à l'événement qui a généré AutoSupport le message. Ses données spécifiques aident les partenaires de support et les équipes de support NetApp à résoudre le problème.

AutoSupport utilise les critères suivants pour contrôler le contenu des messages AutoSupport déclenchés par les événements :

- Quels sous-systèmes sont inclus

  Les données sont regroupées en sous-systèmes, y compris les sous-systèmes communs, tels que les fichiers journaux et certains sous-systèmes, tels que RAID. Chaque événement déclenche un message contenant uniquement les données des sous-systèmes spécifiques.

- Niveau de détail de chaque sous-système inclus

  Les données de chaque sous-système inclus sont fournies au niveau de base ou de dépannage.

Vous pouvez afficher tous les événements possibles et déterminer quels sous-systèmes sont inclus dans les messages relatifs à chaque événement à l'aide du `system node autosupport trigger show` commande avec `-instance` paramètre.

En plus des sous-systèmes inclus par défaut pour chaque événement, vous pouvez ajouter des sous-systèmes supplémentaires à un niveau de base ou de dépannage à l'aide de l' `system node autosupport`

`trigger modify` commande.

Fichiers journaux envoyés dans les messages AutoSupport

Les messages AutoSupport peuvent contenir plusieurs fichiers journaux clés qui permettent au personnel du support technique de revoir l'activité récente du système.

Tous les types de messages AutoSupport peuvent inclure les fichiers journaux suivants lorsque le sous-système fichiers journaux est activé :

Fichier journal	Quantité de données incluses dans le fichier
• Fichiers journaux à partir du `/mroot/etc/log/mlog/` répertoire • Le fichier journal DES MESSAGES	Seules les nouvelles lignes ajoutées aux journaux depuis le dernier message AutoSupport jusqu'à un maximum spécifié. Cela permet de s'assurer que les messages AutoSupport disposent de données uniques et pertinentes, sans chevauchement. (Les fichiers journaux des partenaires font exception. Pour les partenaires, le nombre maximal de données autorisé est inclus.)
• Fichiers journaux à partir du `/mroot/etc/log/shelflog/` répertoire • Fichiers journaux à partir du `/mroot/etc/log/acp/` répertoire • Données de journal du système de gestion des événements (EMS)	Les lignes de données les plus récentes jusqu'à un maximum spécifié.

Le contenu des messages AutoSupport peut changer de version d'ONTAP.

Fichiers envoyés dans des messages AutoSupport hebdomadaires

Les messages hebdomadaires AutoSupport contiennent des données supplémentaires sur la configuration et l'état, ce qui est utile pour suivre les modifications apportées à votre système au fil du temps.

Les informations suivantes sont envoyées dans des messages AutoSupport hebdomadaires :

- Informations de base sur chaque sous-système
- Contenu de sélectionné `/mroot/etc` fichiers de répertoire
- Fichiers journaux
- Résultat des commandes fournissant les informations système
- Informations supplémentaires, notamment les informations des bases de données répliquées – RDB –, les statistiques des services et bien plus encore

Comment AutoSupport OnDemand obtient des instructions de livraison auprès du support technique

AutoSupport OnDemand communique régulièrement avec le support technique pour

obtenir des instructions de livraison pour envoyer, renvoyer et refuser des messages AutoSupport, et pour télécharger des fichiers volumineux vers le site du support NetApp. AutoSupport OnDemand permet d'envoyer des messages AutoSupport à la demande au lieu d'attendre l'exécution de la tâche AutoSupport hebdomadaire.

AutoSupport OnDemand comprend les composants suivants :

- Client AutoSupport OnDemand qui s'exécute sur chaque nœud
- Service AutoSupport OnDemand qui réside dans le support technique

Le client AutoSupport OnDemand interroge régulièrement le service AutoSupport OnDemand afin d'obtenir des instructions de livraison du support technique. Par exemple, le support technique peut utiliser le service AutoSupport OnDemand pour demander la génération d'un nouveau message AutoSupport. Lorsque le client AutoSupport OnDemand interroge le service AutoSupport OnDemand, le client obtient les instructions de livraison et envoie le nouveau message AutoSupport à la demande.

AutoSupport OnDemand est activé par défaut. Cependant, AutoSupport OnDemand dépend de certains paramètres AutoSupport pour continuer à communiquer avec le support technique. AutoSupport OnDemand communique automatiquement avec le support technique lorsque les exigences suivantes sont respectées :

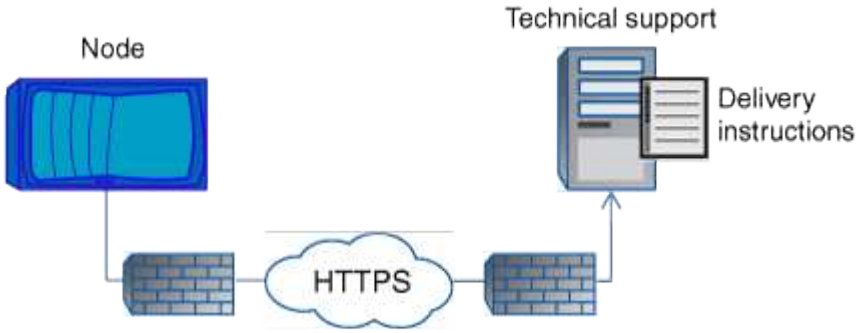
- AutoSupport est activé.
- AutoSupport est configuré pour envoyer des messages au support technique.
- AutoSupport est configuré pour utiliser le protocole de transport HTTPS.

Le client AutoSupport OnDemand envoie des demandes HTTPS au même emplacement de support technique auquel les messages AutoSupport sont envoyés. Le client AutoSupport OnDemand n'accepte pas les connexions entrantes.

AutoSupport OnDemand utilise le compte utilisateur « AutoSupport » pour communiquer avec le support technique. ONTAP vous empêche de supprimer ce compte.

Si vous souhaitez désactiver AutoSupport OnDemand, mais que AutoSupport reste activé, utilisez la commande : LINK:https://docs.netapp.com/us-en/ontap-cli-9121/system-node-autosupport-modify.html#parameters[`system node autosupport modify -ondemand-state disable`].

L'illustration suivante montre comment AutoSupport OnDemand envoie des demandes HTTPS au support technique pour obtenir des instructions de livraison.



Les instructions de livraison peuvent inclure des demandes pour que AutoSupport puisse faire ce qui suit :

- Générer de nouveaux messages AutoSupport.

Le support technique peut demander de nouveaux messages AutoSupport pour vous aider à trier les problèmes.

- Générer de nouveaux messages AutoSupport qui chargent les fichiers « core dump » ou les fichiers d'archivage des performances sur le site de support NetApp.

  Le support technique peut demander des fichiers « core dump » ou d'archivage des performances afin de gérer les problèmes urgents.

- Retransmettre les messages AutoSupport générés précédemment.

  Cette demande se produit automatiquement si aucun message n'a été reçu en raison d'un échec de livraison.

- Désactiver la distribution des messages AutoSupport pour des événements déclencheurs spécifiques.

  Le support technique peut désactiver la livraison de données non utilisées.

Structure des messages AutoSupport envoyés par e-mail

Lorsqu'un message AutoSupport est envoyé par e-mail, le message a un objet standard, un corps bref et une pièce jointe de grande taille au format de fichier 7z qui contient les données.

Si AutoSupport est configuré pour masquer les données privées, certaines informations, telles que le nom d'hôte, sont omises ou masquées dans l'en-tête, le sujet, le corps et les pièces jointes.

Objet

La ligne d'objet des messages envoyés par le mécanisme AutoSupport contient une chaîne de texte qui identifie la raison de la notification. Le format de la ligne d'objet est le suivant :

Notification de groupe HA de *System_Name* (*message*) *Severity*

- *System_Name* est le nom d'hôte ou l'ID système, selon la configuration AutoSupport

Corps

Le corps du message AutoSupport contient les informations suivantes :

- Date et heure du message
- Version de ONTAP sur le nœud qui a généré le message
- L'ID du système, le numéro de série et le nom d'hôte du nœud qui a généré le message
- Numéro de séquence AutoSupport
- Localisation et nom du contact SNMP, si spécifiés
- ID système et nom d'hôte du nœud partenaire HA

Fichiers joints

Les informations clés d'un message AutoSupport sont contenues dans des fichiers compressés dans un fichier

7z appelé `body.7z` et joints au message.

Les fichiers contenus dans la pièce jointe sont spécifiques au type de message AutoSupport.

Types de gravité AutoSupport

Les messages AutoSupport ont des types de gravité qui vous aident à comprendre l'objet de chaque message : par exemple, pour attirer l'attention immédiate sur un problème d'urgence ou uniquement pour fournir des informations.

Les messages ont l'un des niveaux de gravité suivants :

- **Alerte** : les messages d'alerte indiquent qu'un événement de niveau supérieur peut se produire si vous ne prenez pas d'action.

  Vous devez prendre une action contre les messages d'alerte dans les 24 heures.

- **Urgence** : les messages d'urgence sont affichés lorsqu'une interruption s'est produite.

  Vous devez agir immédiatement contre les messages d'urgence.

- **Erreur** : les conditions d'erreur indiquent ce qui peut se produire si vous ignorez.
- **Avis** : condition normale mais significative.
- **Info**: Message d'information fournit des détails sur le problème, que vous pouvez ignorer.
- **Debug** : les messages au niveau du débogage fournissent des instructions que vous devez effectuer.

Si votre service de support interne reçoit des messages AutoSupport par e-mail, la gravité apparaît dans l'objet de l'e-mail.

Conditions requises pour utiliser AutoSupport

Vous devez utiliser HTTPS avec TLSv1.2 ou SMTP sécurisé pour la transmission des messages AutoSupport afin de garantir une sécurité optimale et de prendre en charge toutes les fonctionnalités AutoSupport les plus récentes. Les messages AutoSupport livrés avec tout autre protocole seront rejetés.

Protocoles pris en charge

Tous ces protocoles s'exécutent sur IPv4 ou IPv6, en fonction de la famille d'adresses à laquelle le nom résout.

Protocole et port	Description
HTTPS sur le port 443	Il s'agit du protocole par défaut. Vous devez l'utiliser autant que possible. Ce protocole prend en charge AutoSupport OnDemand et les téléchargements de fichiers volumineux. Le certificat du serveur distant est validé par rapport au certificat racine, sauf si vous désactivez la validation. La livraison utilise une demande PUT HTTPS. Avec PUT, si la demande échoue pendant la transmission, la requête redémarre là où elle s'est arrêtée. Si le serveur qui reçoit la demande ne prend pas en charge PUT, la livraison utilise une requête POST HTTPS.
HTTP sur le port 80	Ce protocole est préférable à SMTP. Ce protocole prend en charge les téléchargements de fichiers volumineux, mais pas AutoSupport OnDemand. La livraison utilise une demande PUT HTTPS. Avec PUT, si la demande échoue pendant la transmission, la requête redémarre là où elle s'est arrêtée. Si le serveur qui reçoit la demande ne prend pas en charge PUT, la livraison utilise une requête POST HTTPS.
SMTP sur le port 25 ou un autre port	Vous devez utiliser ce protocole uniquement si la connexion réseau n'autorise pas HTTPS. La valeur de port par défaut est 25, mais vous pouvez configurer AutoSupport pour utiliser un autre port. Gardez à l'esprit les limitations suivantes lorsque vous utilisez SMTP : • AutoSupport OnDemand et les téléchargements de fichiers volumineux ne sont pas pris en charge. • Les données ne sont pas chiffrées. SMTP envoie des données en clair, ce qui facilite l'interception et la lecture du texte dans le message AutoSupport. • Des limites de longueur de message et de longueur de ligne peuvent être introduites.

Si vous configurez AutoSupport avec des adresses e-mail spécifiques pour votre service de support interne ou une organisation partenaire de support, ces messages sont toujours envoyés par SMTP.

Par exemple, si vous utilisez le protocole recommandé pour envoyer des messages à l'assistance technique et que vous souhaitez également envoyer des messages à votre organisation d'assistance interne, vos messages seront transportés en utilisant respectivement HTTPS et SMTP.

AutoSupport limite la taille maximale de fichier pour chaque protocole. Le paramètre par défaut pour les transferts HTTP et HTTPS est de 25 Mo. Le paramètre par défaut pour les transferts SMTP est 5 Mo. Si la taille du message AutoSupport dépasse la limite configurée, AutoSupport livre autant de messages que possible. Vous pouvez modifier la taille maximale en modifiant la configuration AutoSupport. Voir la `system node autosupport modify` page man pour plus d'informations

AutoSupport remplace automatiquement la limite de taille maximale des fichiers pour les protocoles HTTPS et HTTP lorsque vous générez et envoyez des messages AutoSupport qui chargent les fichiers « core dump » ou d'archivage des performances vers le site de support NetApp ou un URI spécifié. Le remplacement automatique s'applique uniquement lorsque vous téléchargez des fichiers à l'aide de l' `system node autosupport invoke-core-upload` ou le `system node autosupport invoke-performance-archive` commandes.

Configuration requise

Selon la configuration de votre réseau, le protocole HTTPS peut nécessiter une configuration supplémentaire d'une URL proxy. Si HTTPS envoie des messages AutoSupport au support technique et que vous disposez d'un proxy, vous devez identifier l'URL de ce proxy. Si le proxy utilise un port autre que le port par défaut, qui est 3128, vous pouvez spécifier le port pour ce proxy. Vous pouvez également spécifier un nom d'utilisateur et un mot de passe pour l'authentification par proxy.

Si vous utilisez SMTP pour envoyer des messages AutoSupport à votre organisation de support interne ou au support technique, vous devez configurer un serveur de messagerie externe. Le système de stockage ne fonctionne pas comme un serveur de messagerie ; il nécessite un serveur de messagerie externe sur votre site pour envoyer des messages. Le serveur de messagerie doit être un hôte qui écoute sur le port SMTP (25) ou sur un autre port, et il doit être configuré pour envoyer et recevoir le codage 8 bits Multipurpose Internet Mail Extensions (MIME). Les hôtes de messagerie par exemple incluent un hôte UNIX exécutant un serveur SMTP tel que le programme sendmail et un serveur Windows exécutant le serveur Microsoft Exchange. Vous pouvez avoir un ou plusieurs hôtes de messagerie.

Configurer AutoSupport

Vous pouvez contrôler si les informations de AutoSupport sont envoyées au support technique et à votre organisation de support interne, puis tester que la configuration est correcte.

Description de la tâche

Dans les versions ONTAP 9.5 et ultérieures, vous pouvez activer AutoSupport et modifier sa configuration simultanément sur tous les nœuds du cluster. Lorsqu'un nouveau nœud rejoint le cluster, le nœud hérite automatiquement de la configuration de cluster AutoSupport. Vous n'avez pas besoin de mettre à jour la configuration séparément sur chaque nœud.

Depuis ONTAP 9.5, le champ d'application du `system node autosupport modify` la commande s'effectue au niveau du cluster. La configuration AutoSupport est modifiée sur tous les nœuds du cluster, même lorsque `-node` est spécifié. L'option est ignorée, mais elle a été conservée pour la rétrocompatibilité CLI.

Dans ONTAP 9.4 et les versions antérieures, le champ d'application du `system node autosupport modify` la commande est spécifique au nœud. La configuration AutoSupport doit être modifiée sur chaque nœud de votre cluster.

Par défaut, AutoSupport est activé sur chaque nœud pour envoyer des messages au support technique via le protocole de transport HTTPS.

Vous devez utiliser HTTPS avec TLSv1.2 ou SMTP sécurisé pour la transmission des messages AutoSupport afin de garantir une sécurité optimale et de prendre en charge toutes les fonctionnalités AutoSupport les plus récentes.

Étapes

1. Assurez-vous que AutoSupport est activé :

```
system node autosupport modify -state enable
```

2. Si vous souhaitez que le support technique reçoive les messages AutoSupport, utilisez la commande suivante :

```
system node autosupport modify -support enable
```

   Vous devez activer cette option si vous souhaitez permettre à AutoSupport de travailler avec AutoSupport OnDemand ou si vous souhaitez télécharger des fichiers volumineux, tels que les fichiers core dump et d'archivage des performances, vers le support technique ou une URL spécifiée.

3. Si le support technique est activé pour recevoir des messages AutoSupport, spécifiez le protocole de transport à utiliser pour les messages.

   Vous pouvez choisir parmi les options suivantes :

Les fonctions que vous recherchez…	Définissez ensuite les paramètres suivants du `system node autosupport modify` commande…
Utilisez le protocole HTTPS par défaut	a. Réglez `-transport` à `https`. b. Si vous utilisez un proxy, définissez `-proxy-url` À l'URL de votre proxy. Cette configuration prend en charge la communication avec AutoSupport OnDemand et les téléchargements de fichiers volumineux.

Utiliser SMTP	Réglez `-transport` à `smtp`. Cette configuration ne prend pas en charge AutoSupport OnDemand ni les téléchargements de fichiers volumineux.

4. Si vous souhaitez que votre service de support interne ou un partenaire de support reçoive les messages AutoSupport, effectuez les opérations suivantes :
   a. Identifiez les destinataires de votre organisation en définissant les paramètres suivants de l' `system node autosupport modify` commande :

Définir ce paramètre…	À ceci…
`-to`	Jusqu'à cinq adresses e-mail ou listes de distribution individuelles séparées par des virgules dans votre service de support interne qui recevront des messages AutoSupport clés
`-noteto`	Jusqu'à cinq adresses e-mail ou listes de distribution individuelles séparées par des virgules dans votre service d'assistance interne qui recevront une version abrégée des messages clés AutoSupport conçus pour les téléphones portables et autres appareils mobiles
`-partner-address`	Jusqu'à cinq adresses e-mail ou listes de distribution séparées par des virgules dans votre organisation partenaire de support qui recevront tous les messages AutoSupport

   b. Vérifiez que les adresses sont correctement configurées en répertoriant les destinations à l'aide de l' `system node autosupport destinations show` commande.
5. Si vous envoyez des messages à votre organisation de support interne ou si vous avez choisi le transport SMTP pour les messages au support technique, configurez SMTP en définissant les paramètres suivants de l' `system node autosupport modify` commande :
   - Réglez `-mail-hosts` à un ou plusieurs hôtes de messagerie, séparés par des virgules.

     Vous pouvez définir un maximum de cinq.

     Vous pouvez configurer une valeur de port pour chaque hôte de messagerie en spécifiant un point-virgule et un numéro de port après le nom d'hôte de messagerie : par exemple, `mymailhost.example.com:5678`, où 5678 est le port de l'hôte de messagerie.
   - Réglez `-from` À l'adresse e-mail qui envoie le message AutoSupport.
6. Configurez DNS.
7. Vous pouvez également ajouter des options de commande si vous souhaitez modifier des paramètres spécifiques :

Pour cela…	Définissez ensuite les paramètres suivants du `system node autosupport modify` commande…
Masquez des données privées en supprimant, masquant ou encodant des données sensibles dans les messages	Réglez `-remove-private-data` à `true`. Si vous changez de `false` à `true`, Tous les fichiers historiques AutoSupport et tous les fichiers associés sont supprimés.
Arrêt de l'envoi des données de performance dans des messages AutoSupport périodiques	Réglez `-perf` à `false`.

8. Vérifiez la configuration globale à l'aide du `system node autosupport show` commande avec `-node` paramètre.
9. Vérifier le fonctionnement de AutoSupport à l'aide de l' `system node autosupport check show` commande.

   Si des problèmes sont signalés, utilisez le `system node autosupport check show-details` pour afficher plus d'informations.

10. Vérifiez que les messages AutoSupport sont en cours d'envoi et de réception :

    a. Utilisez le `system node autosupport invoke` commande avec `-type` paramètre défini sur `test`.

    ```
    cluster1::> system node autosupport invoke -type test -node node1
    ```

    b. Vérifiez que NetApp reçoit vos messages AutoSupport :

    l'historique de AutoSupport du nœud système affiche -node local

Le statut du dernier message AutoSupport sortant doit finalement être défini sur `sent-successful` pour toutes les destinations de protocole appropriées.

a. Vous pouvez également vérifier si le message AutoSupport est envoyé à votre service de support interne ou à votre partenaire de support en consultant l'e-mail de toute adresse configurée pour le `-to`, `-noteto`, ou `-partner-address` paramètres du `system node autosupport modify` commande.

Charger les fichiers core dump

Lorsqu'un fichier « core dump » est enregistré, un message d'événement est généré. Si le service AutoSupport est activé et configuré pour envoyer des messages au support NetApp, un message AutoSupport est transmis, ainsi qu'un e-mail de confirmation automatique vous est envoyé.

Ce dont vous avez besoin

- Vous devez avoir configuré AutoSupport avec les paramètres suivants :
  - AutoSupport est activé sur le nœud.

- AutoSupport est configuré pour envoyer des messages au support technique.
- AutoSupport est configuré pour utiliser le protocole de transport HTTP ou HTTPS.

  Le protocole de transport SMTP n'est pas pris en charge lors de l'envoi de messages contenant des fichiers volumineux, tels que des fichiers de vidage de mémoire.

Description de la tâche

Vous pouvez également charger le fichier « core dump » via le service AutoSupport via HTTPS en utilisant le `system node autosupport invoke-core-upload` Si le support NetApp en a besoin.

"Télécharger un fichier vers NetApp"

Étapes

1. Afficher les fichiers « core dump » d'un nœud en utilisant le `system node coredump show` commande.

   Dans l'exemple suivant, les fichiers « core dump » sont affichés pour le nœud local :

   ```
   cluster1::> system node coredump show -node local
   Node:Type Core Name Saved Panic Time
   --------- ------------------------------------------ -----
   -----------------
   node:kernel
   core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
   ```

2. Générez un message AutoSupport et téléchargez un fichier « core dump » à l'aide de `system node autosupport invoke-core-upload` commande.

   Dans l'exemple suivant, un message AutoSupport est généré et envoyé à l'emplacement par défaut, qui est le support technique, et le fichier core dump est téléchargé vers l'emplacement par défaut, qui est le site du support NetApp :

   ```
   cluster1::> system node autosupport invoke-core-upload -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

   Dans l'exemple suivant, un message AutoSupport est généré et envoyé à l'emplacement spécifié dans l'URI, et le fichier core dump est chargé dans l'URI :

   ```
   cluster1::> system node autosupport invoke-core-upload -uri
   https//files.company.com -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

Téléchargez les fichiers d'archivage des performances

Vous pouvez générer et envoyer un message AutoSupport contenant un archivage des performances. Par défaut, le support technique NetApp reçoit le message AutoSupport,

et l'archivage des performances est téléchargé sur le site du support NetApp. Vous pouvez spécifier une autre destination pour le message et le téléchargement.

Ce dont vous avez besoin

- Vous devez avoir configuré AutoSupport avec les paramètres suivants :
  - AutoSupport est activé sur le nœud.
  - AutoSupport est configuré pour envoyer des messages au support technique.
  - AutoSupport est configuré pour utiliser le protocole de transport HTTP ou HTTPS.

    Le protocole de transport SMTP n'est pas pris en charge lors de l'envoi de messages contenant des fichiers volumineux, tels que des fichiers d'archivage de performance.

Description de la tâche

Vous devez spécifier une date de début pour les données d'archive de performances que vous souhaitez télécharger. La plupart des systèmes de stockage conservent des archives de performances pendant deux semaines. Vous pouvez ainsi spécifier une date de démarrage il y a deux semaines. Par exemple, si aujourd'hui est janvier 15, vous pouvez spécifier une date de début de janvier 2.

Étape

1. Générez un message AutoSupport et téléchargez le fichier d'archivage des performances à l'aide de `system node autosupport invoke-performance-archive` commande.

   Dans l'exemple suivant, 4 heures de fichiers d'archivage des performances date du 12 janvier 2015 sont ajoutés à un message AutoSupport et téléchargés sur l'emplacement par défaut, qui est le site de support NetApp :

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   Dans l'exemple suivant, 4 heures de fichiers d'archive de performances à partir du 12 janvier 2015 sont ajoutés à un message AutoSupport et chargés à l'emplacement spécifié par l'URI :

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h -uri
   https://files.company.com
   ```

Lire les descriptions de messages AutoSupport

Les descriptions des messages AutoSupport que vous recevez sont disponibles via le convertisseur Syslog ONTAP.

Étapes

1. Accédez au "Traducteur syslog".
2. Dans le champ **version**, entrez la version de ONTAP que vous utilisez. Dans le champ **Search String**, entrez « callhome ». Sélectionnez **Translate**.

3. Syslog Translator répertorie par ordre alphabétique tous les événements correspondant à la chaîne de message que vous avez saisie.

Commandes de gestion de AutoSupport

Vous utilisez le `system node autosupport` Commandes permettant de modifier ou d'afficher la configuration AutoSupport, d'afficher des informations sur les messages AutoSupport précédents et d'envoyer, de renvoyer ou d'annuler un message AutoSupport.

Configurez AutoSupport

Les fonctions que vous recherchez…	Utilisez cette commande…
Contrôlez si des messages AutoSupport sont envoyés	`system node autosupport modify` avec le `-state` paramètre
Contrôlez si les messages AutoSupport sont envoyés au support technique	`system node autosupport modify` avec le `-support` paramètre
Configurer AutoSupport ou modifier la configuration de AutoSupport	`system node autosupport modify`
Activez et désactivez les messages AutoSupport à votre organisation de support interne pour les événements de déclenchement individuels. Vous pouvez également spécifier des rapports de sous-système supplémentaires à inclure dans les messages envoyés en réponse aux événements de déclenchement individuels	`system node autosupport trigger modify`

Affiche des informations sur la configuration AutoSupport

Les fonctions que vous recherchez…	Utilisez cette commande…
Afficher la configuration AutoSupport	`system node autosupport show` avec le `-node` paramètre
Afficher un récapitulatif de toutes les adresses et URL qui reçoivent des messages AutoSupport	`system node autosupport destinations show`
Affichez les messages AutoSupport envoyés à votre organisation de support interne pour des événements déclencheurs individuels	`system node autosupport trigger show`
Affichage de l'état de la configuration AutoSupport ainsi que de la livraison vers différentes destinations	`system node autosupport check show`

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche l'état détaillé de la configuration AutoSupport ainsi que la livraison à différentes destinations	`system node autosupport check show-details`

Affiche les informations relatives aux messages AutoSupport précédents

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations sur un ou plusieurs des 50 messages AutoSupport les plus récents	`system node autosupport history show`
Affiche des informations sur les messages AutoSupport récents générés pour télécharger les fichiers core dump ou archive des performances vers le site de support technique ou un URI spécifié	`system node autosupport history show-upload-details`
Affichez les informations des messages AutoSupport, y compris le nom et la taille de chaque fichier collecté pour le message, ainsi que toute erreur	`system node autosupport manifest show`

Envoyer, renvoyer ou annuler des messages AutoSupport

Les fonctions que vous recherchez…	Utilisez cette commande…
Retransmettez un message AutoSupport stocké localement, identifié par son numéro de séquence AutoSupport Si vous retransmettez un message AutoSupport et que le support a déjà reçu ce message, le système de support ne crée pas de dossier en double. Si, par contre, le support ne recevait pas ce message, le système AutoSupport analysera le message et créera un dossier, si nécessaire.	`system node autosupport history retransmit`
Générer et envoyer un message AutoSupport, par exemple, à des fins de test	`system node autosupport invoke` Utilisez le `-force` Paramètre permettant d'envoyer un message même si AutoSupport est désactivé. Utilisez le `-uri` paramètre pour envoyer le message à la destination que vous spécifiez au lieu de la destination configurée.

Les fonctions que vous recherchez…	Utilisez cette commande…
Annuler un message AutoSupport	`system node autosupport history cancel`

Informations associées

"Commandes de ONTAP 9"

Informations incluses dans le manifeste AutoSupport

Le manifeste AutoSupport vous offre une vue détaillée des fichiers collectés pour chaque message AutoSupport. Le manifeste AutoSupport contient également des informations sur les erreurs de collecte lorsque AutoSupport ne peut pas collecter les fichiers dont il a besoin.

Le manifeste du AutoSupport inclut les informations suivantes :

- Numéro de séquence du message AutoSupport
- Fichiers AutoSupport inclus dans le message AutoSupport
- Taille de chaque fichier, en octets
- Statut de la collection du manifeste AutoSupport
- Description de l'erreur, si AutoSupport n'a pas pu collecter un ou plusieurs fichiers

Vous pouvez afficher le manifeste AutoSupport en utilisant le `system node autosupport manifest show` commande.

Le manifeste AutoSupport est inclus avec chaque message AutoSupport et présenté au format XML, ce qui signifie que vous pouvez soit utiliser un visualiseur XML générique pour le lire, soit l'afficher à l'aide du portail Active IQ (précédemment appelé My AutoSupport).

Suppression du boîtier AutoSupport pendant les fenêtres de maintenance planifiées

La suppression de dossier AutoSupport vous permet d'arrêter la création de dossiers inutiles provenant de messages AutoSupport déclenchés lors des fenêtres de maintenance planifiées.

Pour supprimer des cas AutoSupport, vous devez appeler manuellement un message AutoSupport avec une chaîne de texte spécialement formatée : `MAINT=xh`. `x` est la durée de la fenêtre de maintenance en unités d'heures.

Informations associées

"Comment supprimer la création automatique de dossier pendant les fenêtres de maintenance planifiées"

Dépanner AutoSupport lorsque les messages ne sont pas reçus

Si le système n'envoie pas le message AutoSupport, vous pouvez déterminer si c'est parce que AutoSupport ne peut pas générer le message ou ne peut pas le transmettre.

Étapes

1. Vérifiez l'état de transmission des messages à l'aide de `system node autosupport history show` commande.
2. Lire l'état.

Ce statut	Signifie
initialisation	Le processus de collecte démarre. Si cet état est temporaire, tout est bien. Toutefois, si cet état persiste, il y a un problème.
echec de la collecte	AutoSupport ne peut pas créer le contenu AutoSupport dans le répertoire spoule. Vous pouvez afficher ce que AutoSupport tente de collecter en entrant dans le `system node autosupport history show -detail` commande.
collecte en cours	AutoSupport collecte du contenu AutoSupport. Vous pouvez afficher les données collectées par AutoSupport en entrant `system node autosupport manifest show` commande.
en file d'attente	Les messages AutoSupport sont placés en file d'attente pour livraison, mais pas encore livrés.
transmission	AutoSupport fournit actuellement des messages.
envoi réussi	AutoSupport a envoyé le message avec succès. Pour savoir où AutoSupport a envoyé le message, entrez la `system node autosupport history show -delivery` commande.
ignorer	AutoSupport n'a aucune destination pour le message. Vous pouvez afficher les détails de livraison en entrant le `system node autosupport history show -delivery` commande.
mise en file d'attente	AutoSupport a tenté de livrer des messages, mais la tentative a échoué. Par conséquent, AutoSupport a replacé les messages dans la file d'attente de livraison pour une autre tentative. Vous pouvez afficher l'erreur en entrant le `system node autosupport history show` commande.
transmission défectueuse	AutoSupport n'a pas réussi à transmettre le message le nombre spécifié de fois et a cessé d'essayer de le transmettre. Vous pouvez afficher l'erreur en entrant le `system node autosupport history show` commande.
ondemand-ignore	Le message AutoSupport a été traité avec succès, mais le service AutoSupport OnDemand a choisi de l'ignorer.

3. Effectuez l'une des opérations suivantes :

Pour ce statut	Faites ça
échec de l'initialisation ou de la collecte	Contactez le support NetApp, car AutoSupport ne peut pas générer le message. Mentionner l'article suivant de la base de connaissances : "Échec de la livraison d'AutoSupport : l'état est bloqué en cours d'initialisation"
échec de l'ignorer, de la mise en file d'attente ou de la transmission	Vérifiez que les destinations sont correctement configurées pour SMTP, HTTP ou HTTPS car AutoSupport ne peut pas transmettre le message.

Dépanner la distribution des messages AutoSupport via HTTP ou HTTPS

Si le système n'envoie pas le message AutoSupport attendu et que vous utilisez HTTP ou HTTPS ou si la fonction de mise à jour automatique ne fonctionne pas, vous pouvez vérifier un certain nombre de paramètres pour résoudre le problème.

Ce dont vous avez besoin

Vous devez avoir confirmé la connectivité réseau de base et la recherche DNS :

- Votre LIF de node-management doit être active et administrative.
- Vous devez pouvoir envoyer une requête ping à un hôte opérationnel sur le même sous-réseau à partir de la LIF de gestion du cluster (il ne s'agit pas d'une LIF sur un des nœuds).
- Vous devez pouvoir envoyer des requêtes ping à un hôte opérationnel en dehors du sous-réseau à partir de la LIF de gestion du cluster.
- Vous devez pouvoir ping un hôte opérationnel hors du sous-réseau depuis la LIF de gestion du cluster utilisant le nom de l'hôte (pas l'adresse IP).

Description de la tâche

Ces étapes sont pour les cas où vous avez déterminé que AutoSupport peut générer le message, mais que vous ne pouvez pas le transmettre via HTTP ou HTTPS.

Si vous rencontrez des erreurs ou si vous ne parvenez pas à effectuer une étape de cette procédure, déterminez et traitez le problème avant de passer à l'étape suivante.

Étapes

1. Afficher l'état détaillé du sous-système AutoSupport :

   ```
   system node autosupport check show-details
   ```

   Cela inclut la vérification de la connectivité aux destinations AutoSupport via l'envoi de messages de test et la liste des erreurs possibles dans les paramètres de configuration de AutoSupport.

2. Vérifier l'état du LIF node management :

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

Le `status-oper` et `status-admin` les champs doivent retourner « up ».

3. Enregistrer le nom du SVM, le nom de la LIF et l'adresse IP de la LIF pour une utilisation ultérieure.
4. Assurez-vous que le DNS est activé et configuré correctement :

   ```
   vserver services name-service dns show
   ```

5. Corriger toute erreur renvoyée par le message AutoSupport :

   ```
   system node autosupport history show -node * -fields node,seq-
   num,destination,last-update,status,error
   ```

   Pour obtenir de l'aide sur le dépannage des erreurs renvoyées, reportez-vous au "Guide de résolution ONTAP AutoSupport (transport HTTPS et HTTP)".

6. Vérifiez que le cluster peut accéder aux serveurs dont il a besoin et à Internet :

   a. `network traceroute -lif node-management_LIF -destination DNS server`

   b. `network traceroute -lif node_management_LIF -destination support.netapp.com`

   > L'adresse `support.netapp.com` elle-même ne répond pas à la commande ping/traceroute, mais l'information par saut est utile.

   c. `system node autosupport show -fields proxy-url`

   d. `network traceroute -node node_management_LIF -destination proxy_url`

   Si l'une de ces routes ne fonctionne pas, essayez la même route à partir d'un hôte en fonctionnement sur le même sous-réseau que le cluster, en utilisant l'utilitaire « traceroute » ou « tracert » situé sur la plupart des clients réseau tiers. Cela vous aide à déterminer si le problème se situe dans votre configuration réseau ou dans votre configuration de cluster.

7. Si vous utilisez HTTPS pour votre protocole de transport AutoSupport, assurez-vous que le trafic HTTPS peut quitter le réseau :

   a. Configurez un client web sur le même sous-réseau que la LIF de gestion du cluster.

      Assurez-vous que tous les paramètres de configuration sont les mêmes que pour la configuration AutoSupport, y compris en utilisant le même serveur proxy, le même nom d'utilisateur, le même mot de passe et le même port.

   b. L'accès `https://support.netapp.com` avec le client web.

      L'accès doit être réussi. Si ce n'est pas le cas, assurez-vous que tous les pare-feu sont correctement configurés pour autoriser le trafic HTTPS et DNS et que le serveur proxy est configuré correctement. Pour plus d'informations sur la configuration de la résolution statique des noms pour support.netapp.com, consultez l'article de la base de connaissances "Comment ajouter une entrée D'HÔTE dans ONTAP pour support.netapp.com?"

8. Depuis ONTAP 9.10.1, si vous avez activé la fonction mise à jour automatique, assurez-vous que vous disposez de la connectivité HTTPS aux URL supplémentaires suivantes :
   - https://support-sg-emea.netapp.com
   - https://support-sg-naeast.netapp.com

- https://support-sg-nawest.netapp.com

Dépanner la transmission des messages AutoSupport via SMTP

Si le système ne parvient pas à transmettre les messages AutoSupport via SMTP, vous pouvez vérifier un certain nombre de paramètres pour résoudre le problème.

Ce dont vous avez besoin

Vous devez avoir confirmé la connectivité réseau de base et la recherche DNS :

- Votre LIF de node-management doit être active et administrative.
- Vous devez pouvoir envoyer une requête ping à un hôte opérationnel sur le même sous-réseau à partir de la LIF de gestion du cluster (il ne s'agit pas d'une LIF sur un des nœuds).
- Vous devez pouvoir envoyer des requêtes ping à un hôte opérationnel en dehors du sous-réseau à partir de la LIF de gestion du cluster.
- Vous devez pouvoir ping un hôte opérationnel hors du sous-réseau depuis la LIF de gestion du cluster utilisant le nom de l'hôte (pas l'adresse IP).

Description de la tâche

Ces étapes sont destinées aux cas où vous avez déterminé que AutoSupport peut générer le message, mais ne peut pas le transmettre via SMTP.

Si vous rencontrez des erreurs ou si vous ne parvenez pas à effectuer une étape de cette procédure, déterminez et traitez le problème avant de passer à l'étape suivante.

Toutes les commandes sont saisies au niveau de l'interface de ligne de commandes ONTAP, sauf indication contraire.

Étapes

1. Vérifier l'état du LIF node management :

   network interface show -home-node local -role node-mgmt -fields vserver,lif,status-oper,status-admin,address,role

   Le `status-oper` et `status-admin` vous devriez y retourner `up`.

2. Enregistrer le nom du SVM, le nom de la LIF et l'adresse IP de la LIF pour une utilisation ultérieure.
3. Assurez-vous que le DNS est activé et configuré correctement :

   vserver services name-service dns show

4. Afficher tous les serveurs configurés pour être utilisés par AutoSupport :

   system node autosupport show -fields mail-hosts

   Enregistrer tous les noms de serveur affichés.

5. Pour chaque serveur affiché par l'étape précédente, et `support.netapp.com`, Assurez-vous que le serveur ou l'URL peut être atteint par le noeud :

   network traceroute -node local -destination *server_name*

Si l'une de ces routes ne fonctionne pas, essayez la même route à partir d'un hôte en fonctionnement sur le même sous-réseau que le cluster, en utilisant l'utilitaire « traceroute » ou « tracert » situé sur la plupart des clients réseau tiers. Cela vous aide à déterminer si le problème se situe dans votre configuration réseau ou dans votre configuration de cluster.

6. Connectez-vous à l'hôte désigné comme hôte de messagerie et assurez-vous qu'il peut traiter les demandes SMTP :

   netstat -aAn|grep 25

   `25` Est le numéro de port SMTP du port d'écoute.

   Un message similaire au texte suivant s'affiche :

   ```
   ff64878c tcp        0      0  *.25    *.*    LISTEN.
   ```

7. À partir d'un autre hôte, ouvrez une session Telnet avec le port SMTP de l'hôte de messagerie :

   telnet *mailhost* 25

   Un message similaire au texte suivant s'affiche :

   ```
   220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
   10:49:04 PST
   ```

8. À l'invite telnet, assurez-vous qu'un message peut être relayé depuis votre hôte de messagerie :

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   `domain_name` est le nom de domaine de votre réseau.

   Si une erreur est renvoyée indiquant que la retransmission est refusée, la retransmission n'est pas activée sur l'hôte de messagerie. Contactez votre administrateur système.

9. À l'invite telnet, envoyez un message de test :

   DATA

   SUBJECT: TESTING
   THIS IS A TEST

   .

   Assurez-vous d'entrer la dernière période (.) sur une ligne par elle-même. La période indique à l'hôte de messagerie que le message est terminé.

Si une erreur est renvoyée, votre hôte de messagerie n'est pas configuré correctement. Contactez votre administrateur système.

10. À partir de l'interface de ligne de commande ONTAP, envoyez un message de test AutoSupport à une adresse e-mail de confiance à laquelle vous avez accès :

    `system node autosupport invoke -node local -type test`

11. Recherchez le numéro de séquence de la tentative :

    `system node autosupport history show -node local -destination smtp`

    Recherchez le numéro de séquence de votre tentative en fonction de l'horodatage. C'est probablement la tentative la plus récente.

12. Afficher l'erreur de votre tentative de message de test :

    `system node autosupport history show -node local -seq-num seq_num -fields error`

    Si l'erreur affichée est de `Login denied`, Votre serveur SMTP n'accepte pas les requêtes d'envoi de la LIF de gestion du cluster. Si vous ne souhaitez pas passer à utiliser HTTPS comme protocole de transport, contactez votre administrateur réseau de site pour configurer les passerelles SMTP afin de résoudre ce problème.

    Si ce test réussit mais que le même message envoyé à mailto:autosupport@netapp.com ne le fait pas, assurez-vous que le relais SMTP est activé sur tous vos hôtes de messagerie SMTP ou utilisez HTTPS comme protocole de transport.

    Si même le message du compte de messagerie géré localement ne fonctionne pas, vérifiez que vos serveurs SMTP sont configurés pour transférer les pièces jointes avec les deux caractéristiques suivantes :

    - Le suffixe « 7z »
    - Le type MIME « application/x-7X-compressé ».

Dépanner le sous-système AutoSupport

Le `system node check show` Les commandes permettent de vérifier et de résoudre tous les problèmes liés à la configuration et à la livraison de AutoSupport.

Étape

1. Utiliser les commandes suivantes pour afficher l'état du sous-système AutoSupport.

Utilisez cette commande…	Pour cela…
`system node autosupport check show`	Affiche l'état général du sous-système AutoSupport, tel que l'état de la destination AutoSupport HTTP ou HTTPS, les destinations SMTP AutoSupport, le serveur AutoSupport OnDemand et la configuration AutoSupport

Utilisez cette commande…	Pour cela…
`system node autosupport check show-details`	Affiche l'état détaillé du sous-système AutoSupport, notamment des descriptions détaillées des erreurs et des actions correctives

Contrôle de l'état du système

Surveillez l'état de santé de votre système

Cette fonction surveille de manière proactive certaines conditions critiques du cluster et déclenche des alertes en cas de défaillance ou de risque. Si des alertes sont actives, l'état de l'état du système signale un état dégradé pour le cluster. Les alertes incluent les informations dont vous avez besoin pour répondre à la dégradation de l'état du système.

Si l'état est dégradé, vous pouvez afficher des détails sur le problème, y compris la cause probable et les actions de récupération recommandées. Une fois le problème résolu, l'état de l'état du système revient automatiquement à OK.

L'état de l'état du système reflète plusieurs moniteurs d'état distincts. Un état dégradé au sein d'un moniteur d'état entraîne un état dégradé pour l'état global du système.

Pour plus de détails sur la prise en charge des commutateurs de cluster par ONTAP pour le contrôle de l'état du système dans votre cluster, reportez-vous au *Hardware Universe*.

"Commutateurs pris en charge dans le Hardware Universe"

Pour plus d'informations sur les causes des messages AutoSupport du moniteur d'intégrité des commutateurs de cluster (CSHM) et sur les actions nécessaires pour résoudre ces alertes, consultez l'article de la base de connaissances.

"Message AutoSupport : processus de surveillance de l'état CSHM"

Fonctionnement de la surveillance de l'état

Les moniteurs de santé individuels disposent d'un ensemble de règles qui déclenchent des alertes lorsque certaines conditions se produisent. Comprendre le fonctionnement de la surveillance de l'état de santé peut vous aider à résoudre les problèmes et à contrôler les alertes futures.

La surveillance de l'état des systèmes comprend les composants suivants :

- Chaque état de santé surveille pour des sous-systèmes spécifiques, chacun ayant son propre état d'intégrité

  Par exemple, le sous-système de stockage dispose d'un contrôle de l'état de la connectivité des nœuds.

- Un contrôle de l'état global du système qui consolide l'état d'intégrité des différents moniteurs de santé

  Un état dégradé dans un seul sous-système entraîne un état dégradé pour tout le système. Si aucun sous-système n'a d'alertes, l'état global du système est OK.

Chaque contrôle de l'état est constitué des éléments clés suivants :

- Alertes que le contrôle de l'état peut potentiellement générer

  Chaque alerte a une définition, qui inclut des détails tels que la gravité de l'alerte et sa cause probable.

- Règles de santé qui identifient quand chaque alerte est déclenchée

  Chaque règle de santé dispose d'une expression de règle, qui est la condition ou la modification exacte qui déclenche l'alerte.

Un contrôle de l'état surveille et valide en permanence les ressources de son sous-système à des fins de modification de l'état ou des conditions. Lorsqu'une condition ou une modification d'état correspond à une expression de règle dans une politique de santé, le contrôle de l'état génère une alerte. Une alerte provoque l'état de l'état de santé du sous-système et l'état global de l'intégrité du système.

Moyens de répondre aux alertes d'intégrité du système

Lorsqu'une alerte d'intégrité du système se produit, vous pouvez la valider, en savoir plus sur celui-ci, réparer l'état sous-jacent et éviter qu'elle ne se reproduise.

Lorsqu'un contrôle de l'état soulève une alerte, vous pouvez répondre de l'une des manières suivantes :

- Obtenez des informations sur l'alerte, qui inclut la ressource affectée, la gravité de l'alerte, la cause probable, l'effet possible et les actions correctives.
- Obtenez des informations détaillées sur l'alerte, telles que l'heure à laquelle l'alerte a été générée et si quelqu'un d'autre a déjà reconnu l'alerte.
- Consultez les informations relatives à l'état de la ressource ou du sous-système affecté, par exemple un tiroir ou un disque spécifique.
- Reconnaissez l'alerte pour indiquer qu'une personne travaille sur le problème et identifiez-vous comme « vérificateur ».
- Résolvez le problème en prenant les mesures correctives fournies dans l'alerte, telles que la résolution du câblage pour résoudre un problème de connectivité.
- Supprimez l'alerte si le système ne l'a pas supprimée automatiquement.
- Supprimez une alerte pour l'empêcher d'affecter l'état de santé d'un sous-système.

  La suppression est utile lorsque vous comprenez un problème. Après avoir supprimé une alerte, elle peut toujours se produire, mais l'état de santé du sous-système s'affiche sous la forme « ok-avec-supprimé » lorsque l'alerte supprimée se produit.

Personnalisation des alertes d'intégrité du système

Vous pouvez contrôler les alertes qu'un contrôle de l'état génère en activant et en désactivant les politiques d'intégrité du système qui définissent lorsque les alertes sont déclenchées. Cela vous permet de personnaliser le système de surveillance de l'état de santé pour votre environnement particulier.

Pour connaître le nom d'une règle, vous pouvez afficher des informations détaillées sur une alerte générée ou afficher les définitions de règles pour un contrôle de l'état, un nœud ou un ID d'alerte spécifique.

La désactivation des politiques de santé est différente de la suppression des alertes. Lorsque vous supprimez une alerte, elle n'a pas d'impact sur l'état de santé du sous-système, mais l'alerte peut toujours se produire.

Si vous désactivez une règle, la condition ou l'état défini dans son expression de règle de gestion ne déclenche plus d'alerte.

Exemple d'alerte que vous souhaitez désactiver

Par exemple, supposons qu'une alerte ne vous soit pas utile. Vous utilisez le `system health alert show -instance` Commande pour obtenir l'ID de la règle pour l'alerte. Vous utilisez l'ID de la police dans le `system health policy definition show` commande pour afficher les informations relatives à la règle. Après avoir vérifié l'expression de règle et d'autres informations sur la stratégie, vous décidez de la désactiver. Vous utilisez le `system health policy definition modify` commande pour désactiver la règle.

Le mode d'alerte de santé déclenche des messages et des événements AutoSupport

Les alertes d'intégrité du système déclenchent des messages AutoSupport et des événements dans le système de gestion des événements (EMS), ce qui vous permet de surveiller l'état du système à l'aide des messages AutoSupport et du système EMS en plus d'utiliser directement le système de contrôle de l'état.

Votre système envoie un message AutoSupport dans les cinq minutes qui suivent une alerte. Le message AutoSupport inclut toutes les alertes générées depuis le message AutoSupport précédent, à l'exception des alertes qui dupliquent une alerte pour la même ressource et la même cause probable au cours de la semaine précédente.

Certaines alertes ne déclenchent pas de messages AutoSupport. Une alerte ne déclenche pas de message AutoSupport si sa politique d'intégrité désactive l'envoi de messages AutoSupport. Par exemple, une politique de santé peut désactiver les messages AutoSupport par défaut, car AutoSupport génère déjà un message lorsque le problème se produit. Vous pouvez configurer des règles pour ne pas déclencher de messages AutoSupport à l'aide de `system health policy definition modify` commande.

Vous pouvez afficher la liste de tous les messages AutoSupport déclenchés par les alertes envoyés au cours de la semaine précédente à l'aide du `system health autosupport trigger history show` commande.

Les alertes déclenchent également la génération d'événements au SGE. Un événement est généré chaque fois qu'une alerte est créée et chaque fois qu'une alerte est effacée.

Contrôles disponibles de l'état du cluster

Plusieurs moniteurs d'état permettent de surveiller différentes parties d'un cluster. Les contrôles d'état vous aident à corriger des erreurs au sein des systèmes ONTAP en détectant des événements, en vous envoyant des alertes et en supprimant les événements tels qu'ils sont clairs.

Nom du contrôle de l'état (identifiant)	Nom du sous-système (identifiant)	Objectif
Commutateur du cluster(commutateur du cluster)	Commutateur (commutateur - état)	Surveille les commutateurs du réseau de cluster et les commutateurs du réseau de gestion en termes de température, d'utilisation, de configuration des interfaces, de redondance (commutateurs du réseau de cluster uniquement), et de fonctionnement des ventilateurs et de l'alimentation. Le contrôle de l'état du commutateur de cluster communique avec les commutateurs via SNMP. SNMPv2c est le paramètre par défaut. Depuis ONTAP 9.2, ce moniteur peut détecter et signaler le redémarrage d'un commutateur de cluster depuis la dernière période d'interrogation.
Structure MetroCluster	Commutateur	Surveille la topologie de la configuration MetroCluster back-end de la structure et détecte les erreurs de configuration, comme le câblage et la segmentation incorrects ou les défaillances ISL.
État de santé du MetroCluster	Interconnexion, RAID et stockage	Surveille les adaptateurs FC-VI, les adaptateurs d'initiateurs FC, les agrégats et disques situés derrière le côté gauche et les ports d'intercluster
Connectivité nœud(nœud-Connect)	Continuité de l'activité CIFS	Surveille les connexions SMB afin de garantir la continuité de l'activité aux applications Hyper-V.
Stockage (SAS-Connect)	Surveille les tiroirs, les disques et les adaptateurs au niveau du nœud pour s'assurer que les chemins et les connexions sont appropriés.	Système

Nom du contrôle de l'état (identifiant)	Nom du sous-système (identifiant)	Objectif
sans objet	Rassemble les informations d'autres moniteurs de santé.	Connectivité système (system-Connect)

Recevez automatiquement les alertes d'état du système

Vous pouvez afficher manuellement les alertes d'état du système en utilisant le `system health alert show` commande. Vous devez toutefois vous abonner à des messages EMS pour recevoir automatiquement des notifications lorsqu'un contrôle de l'état génère une alerte.

Description de la tâche

La procédure suivante vous indique comment configurer les notifications pour tous les messages hm.Alert.déclenché et pour tous les messages hm.Alert.effacé.

Tous les messages hm.Alert.déclenché et tous les messages hm.Alert.décoché comprennent une interruption SNMP. Les noms des traps SNMP sont `HealthMonitorAlertRaised` et `HealthMonitorAlertCleared`. Pour plus d'informations sur les interruptions SNMP, consultez le *Network Management Guide*.

Étapes

1. Utilisez le `event destination create` Commande pour définir la destination à laquelle vous souhaitez envoyer les messages EMS.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. Utilisez le `event route add-destinations` commande permettant d'acheminer le `hm.alert.raised` message et le `hm.alert.cleared` message vers une destination.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

Informations associées

"Gestion du réseau"

Répondez à la dégradation de l'état du système

Lorsque l'état de santé de votre système est dégradé, vous pouvez afficher des alertes, lire les informations sur la cause probable et les actions correctives, afficher des informations sur le sous-système dégradé et résoudre le problème. Les alertes supprimées s'affichent également pour vous permettre de les modifier et de vérifier si elles ont été acquittées.

Description de la tâche

Vous pouvez découvrir qu'une alerte a été générée en visualisant un message AutoSupport ou un événement EMS, ou en utilisant le `system health` commandes.

Étapes

1. Utilisez le `system health alert show` commande pour afficher les alertes qui compromettre l'intégrité du système
2. Lisez la cause probable, l'effet possible et les actions correctives de l'alerte pour déterminer si vous pouvez résoudre le problème ou si vous avez besoin d'informations supplémentaires.
3. Si vous avez besoin de plus d'informations, utilisez le `system health alert show -instance` pour afficher les informations supplémentaires disponibles pour l'alerte.
4. Utilisez le `system health alert modify` commande avec `-acknowledge` paramètre pour indiquer que vous travaillez sur une alerte spécifique.
5. Prendre des mesures correctives pour résoudre le problème comme décrit dans le `Corrective Actions` champ dans l'alerte.

   Les actions correctives peuvent inclure le redémarrage du système.

   Une fois le problème résolu, l'alerte est automatiquement effacée. Si le sous-système n'a pas d'autres alertes, l'intégrité du sous-système devient `OK`. Si l'intégrité de tous les sous-systèmes est correcte, l'état d'intégrité globale du système passe à `OK`.

6. Utilisez le `system health status show` commande pour vérifier que l'état de l'intégrité du système est `OK`.

   Si l'état de l'état de santé du système n'est pas `OK`, répéter cette procédure.

Exemple de réponse à une dégradation de l'état du système

En examinant un exemple spécifique de l'état du système dégradé après un tiroir qui manque deux chemins d'accès à un nœud, vous pouvez voir ce que l'interface de ligne de commandes affiche lorsque vous répondez à une alerte.

Après avoir démarré ONTAP, vous vérifiez l'état du système et vous découvrez que son état est dégradé :

```
cluster1::>system health status show
  Status
  ---------------
  degraded
```

Vous affichez les alertes pour déterminer l'emplacement du problème et vous voyez que le tiroir 2 n'a pas deux chemins d'accès au nœud 1 :

```
      cluster1::>system health alert show
                 Node: node1
             Resource: Shelf ID 2
             Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

Vous affichez des informations détaillées sur l'alerte pour obtenir plus d'informations, notamment l'ID d'alerte :

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
          Acknowledge: false
             Suppress: false
               Policy: DualPathToDiskShelf_Policy
         Acknowledger: -
           Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

Vous reconnaissez l'alerte pour indiquer que vous y travaillez.

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

Vous avez résolu le câblage entre le tiroir 2 et le nœud 1, puis redémarré le système. Ensuite, vous vérifiez de nouveau l'état du système et voyez que son état est `OK`:

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

Configurer la détection des commutateurs du réseau de gestion et du cluster

Le contrôle de l'état du switch de cluster tente automatiquement de détecter les commutateurs du réseau de gestion et de cluster à l'aide du protocole CDP (Cisco Discovery Protocol). Vous devez configurer le contrôle de l'état s'il ne peut pas détecter automatiquement un switch ou si vous ne souhaitez pas utiliser CDP pour la découverte automatique.

Description de la tâche

Le `system cluster-switch show` la commande répertorie les switchs détectés par le contrôle de l'état. Si vous ne voyez pas de commutateur que vous aviez prévu dans cette liste, le contrôle de l'état ne peut pas le détecter automatiquement.

Étapes

1. Si vous souhaitez utiliser CDP pour la découverte automatique, procédez comme suit :

   a. Assurez-vous que le Cisco Discovery Protocol (CDP) est activé sur vos commutateurs.

      Reportez-vous à la documentation de votre commutateur pour obtenir des instructions.

   b. Exécutez la commande suivante sur chaque nœud du cluster pour vérifier si CDP est activée ou désactivée :

      `run -node node_name -command options cdpd.enable`

      Si CDP est activé, passez à l'étape d. Si le CDP est désactivé, passez à l'étape c.

   c. Exécutez la commande suivante pour activer CDP :

      `run -node node_name -command options cdpd.enable on`

   Attendez cinq minutes avant de passer à l'étape suivante.

   a. Utilisez le `system cluster-switch show` Commande pour vérifier si ONTAP peut désormais détecter automatiquement les commutateurs.

2. Si le contrôle de l'état ne peut pas détecter automatiquement un commutateur, utilisez le `system cluster-switch create` commande pour configurer la découverte du commutateur :

   ```
   cluster1::> system cluster-switch create -device switch1 -address
   192.0.2.250 -snmp-version SNMPv2c -community cshm1! -model NX5020 -type
   cluster-network
   ```

   Attendez cinq minutes avant de passer à l'étape suivante.

3. Utilisez le `system cluster-switch show` Commande pour vérifier que ONTAP peut détecter le switch pour lequel vous avez ajouté des informations.

Une fois que vous avez terminé

Vérifiez que le contrôle de l'état peut surveiller vos commutateurs.

Vérifier la surveillance du cluster et des commutateurs du réseau de gestion

Le contrôle de l'état du commutateur de cluster tente automatiquement de surveiller les commutateurs qu'il détecte ; toutefois, la surveillance peut ne pas se produire automatiquement si les commutateurs ne sont pas configurés correctement. Vérifiez que le contrôle de l'état est correctement configuré pour surveiller les commutateurs.

Étapes

1. Pour identifier les switchs détectés par le contrôle de l'état du commutateur de cluster, entrez la commande suivante :

   ONTAP 9.8 et versions ultérieures

   `system switch ethernet show`

   ONTAP 9.7 et versions antérieures

   `system cluster-switch show`

   Si le `Model` affiche la valeur `OTHER`, ONTAP ne peut pas surveiller le commutateur. ONTAP définit la valeur sur `OTHER` si un commutateur qu'il détecte automatiquement n'est pas pris en charge pour le contrôle de l'état de santé.

   Si un commutateur ne s'affiche pas dans la sortie de la commande, vous devez configurer la détection du commutateur.

2. Effectuez une mise à niveau vers la dernière version du logiciel de commutateur pris en charge et consultez le fichier de configuration (RCF) disponible sur le site de support NetApp.

   "Page des téléchargements du support NetApp"

   La chaîne de communauté dans le RCF du commutateur doit correspondre à la chaîne de communauté que le moniteur d'état est configuré pour utiliser. Par défaut, le contrôle de l'état utilise la chaîne de communauté `cshm1!`.

   Actuellement, le moniteur de santé ne prend en charge que SNMPv2.

   Si vous avez besoin de modifier les informations concernant un commutateur que le cluster surveille, vous pouvez modifier la chaîne de communauté utilisée par le contrôle de l'état à l'aide de la commande suivante :

ONTAP 9.8 et versions ultérieures

`system switch ethernet modify`

ONTAP 9.7 et versions antérieures

`system cluster-switch modify`

3. Vérifiez que le port de gestion du commutateur est connecté au réseau de gestion.

   Cette connexion est requise pour exécuter des requêtes SNMP.

Commandes permettant de contrôler l'état de santé de votre système

Vous pouvez utiliser le `system health` commandes permettant d'afficher des informations relatives à l'état de santé des ressources système, de répondre aux alertes et de configurer les alertes futures. L'utilisation des commandes de l'interface de ligne de commandes vous permet d'afficher des informations détaillées sur la configuration de la surveillance de l'état. Les pages de manuels des commandes contiennent plus d'informations.

Affiche l'état de l'état de santé du système

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche l'état de santé du système, qui reflète l'état global des moniteurs d'intégrité individuels	`system health status show`
Affiche l'état d'intégrité des sous-systèmes pour lesquels la surveillance de l'état est disponible	`system health subsystem show`

Affiche l'état de la connectivité du nœud

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations détaillées sur la connectivité du nœud au tiroir de stockage, notamment les informations relatives aux ports, la vitesse du port HBA, le débit d'E/S et le taux d'opérations d'E/S par seconde	`storage shelf show -connectivity` Utilisez le `-instance` paramètre pour afficher des informations détaillées sur chaque tiroir.
Affiche des informations sur les disques et les LUN de baie, y compris l'espace utilisable, les numéros de tiroir et de compartiment, ainsi que le nom de nœud propriétaire	`storage disk show` Utilisez le `-instance` paramètre pour afficher des informations détaillées sur chaque lecteur.

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations détaillées sur les ports des tiroirs de stockage, notamment le type de port, la vitesse et l'état	`storage port show` Utilisez le `-instance` paramètre pour afficher des informations détaillées sur chaque adaptateur.

Gérer la détection des commutateurs de cluster, de stockage et de réseau de gestion

Les fonctions que vous recherchez…	Utilisez cette commande. (ONTAP 9.8 et versions ultérieures)	Utilisez cette commande. (ONTAP 9.7 et versions antérieures)
Afficher les commutateurs surveillés par le bloc d'instruments	`system switch ethernet show`	`system cluster-switch show`
Afficher les commutateurs actuellement surveillés par le cluster, notamment les commutateurs que vous avez supprimés (indiqués dans la colonne raison de la sortie de la commande) et les informations de configuration dont vous avez besoin pour accéder au réseau au cluster et aux commutateurs du réseau de gestion. Cette commande est disponible au niveau de privilège avancé.	`system switch ethernet show-all`	`system cluster-switch show-all`
Configurer la détection d'un commutateur non découvert	`system switch ethernet create`	`system cluster-switch create`
Modifier les informations relatives à un commutateur que le cluster surveille (par exemple, nom de périphérique, adresse IP, version SNMP et chaîne de communauté)	`system switch ethernet modify`	`system cluster-switch modify`
Désactiver la surveillance d'un commutateur	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
Désactiver la détection et la surveillance d'un commutateur et supprimer les informations de configuration du commutateur	`system switch ethernet delete`	`system cluster-switch delete`

Les fonctions que vous recherchez…	Utilisez cette commande. (ONTAP 9.8 et versions ultérieures)	Utilisez cette commande. (ONTAP 9.7 et versions antérieures)
Supprimez définitivement les informations de configuration du commutateur stockées dans la base de données (ce qui permet de réactiver la détection automatique du commutateur)	`system switch ethernet delete -force`	`system cluster-switch delete -force`
Activez la journalisation automatique pour envoyer des messages AutoSupport.	`system switch ethernet log`	`system cluster-switch log`

Répondez aux alertes générées

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations sur les alertes générées, telles que la ressource et le nœud où l'alerte a été déclenchée, ainsi que la gravité et la cause probable de l'alerte	`system health alert show`
Affiche des informations sur chaque alerte générée	`system health alert show -instance`
Indique que quelqu'un travaille sur une alerte	`system health alert modify`
Accuser réception d'une alerte	`system health alert modify -acknowledge`
Supprimez une alerte ultérieure afin qu'elle n'affecte pas l'état de santé d'un sous-système	`system health alert modify -suppress`
Supprimez une alerte qui n'a pas été automatiquement effacée	`system health alert delete`
Affiche des informations sur les messages AutoSupport qui déclenchent les alertes la semaine dernière, par exemple pour déterminer si une alerte a déclenché un message AutoSupport	`system health autosupport trigger history show`

Configurez les alertes futures

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez ou désactivez la règle qui contrôle si un état de ressource spécifique génère une alerte spécifique	`system health policy definition modify`

Affiche des informations sur la configuration de la surveillance de l'état

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations relatives aux contrôles d'état, telles que leurs nœuds, leurs noms, leurs sous-systèmes et leur état	`system health config show` Utilisez le `-instance` paramètre pour afficher des informations détaillées sur chaque contrôle de l'état.
Affiche des informations sur les alertes qu'un contrôle de l'état peut générer	`system health alert definition show` Utilisez le `-instance` paramètre pour afficher des informations détaillées sur chaque définition d'alerte.
Affiche des informations sur les règles de contrôle de l'état, qui déterminent l'heure à laquelle les alertes sont émises	`system health policy definition show` Utilisez le `-instance` paramètre pour afficher des informations détaillées sur chaque règle. Utilisez d'autres paramètres pour filtrer la liste des alertes, par exemple en fonction de l'état (activé ou non), du contrôle de l'état, de l'alerte, etc.

Affiche des informations environnementales

Les capteurs vous aident à surveiller les composants environnementaux de votre système. Les informations que vous pouvez afficher concernant les capteurs environnementaux incluent leur type, leur nom, leur état, leur valeur et les avertissements de seuil.

Étape

1. Pour afficher des informations sur les capteurs environnementaux, utilisez le `system node environment sensors show` commande.

Analytique du système de fichiers

Présentation de l'analytique du système de fichiers

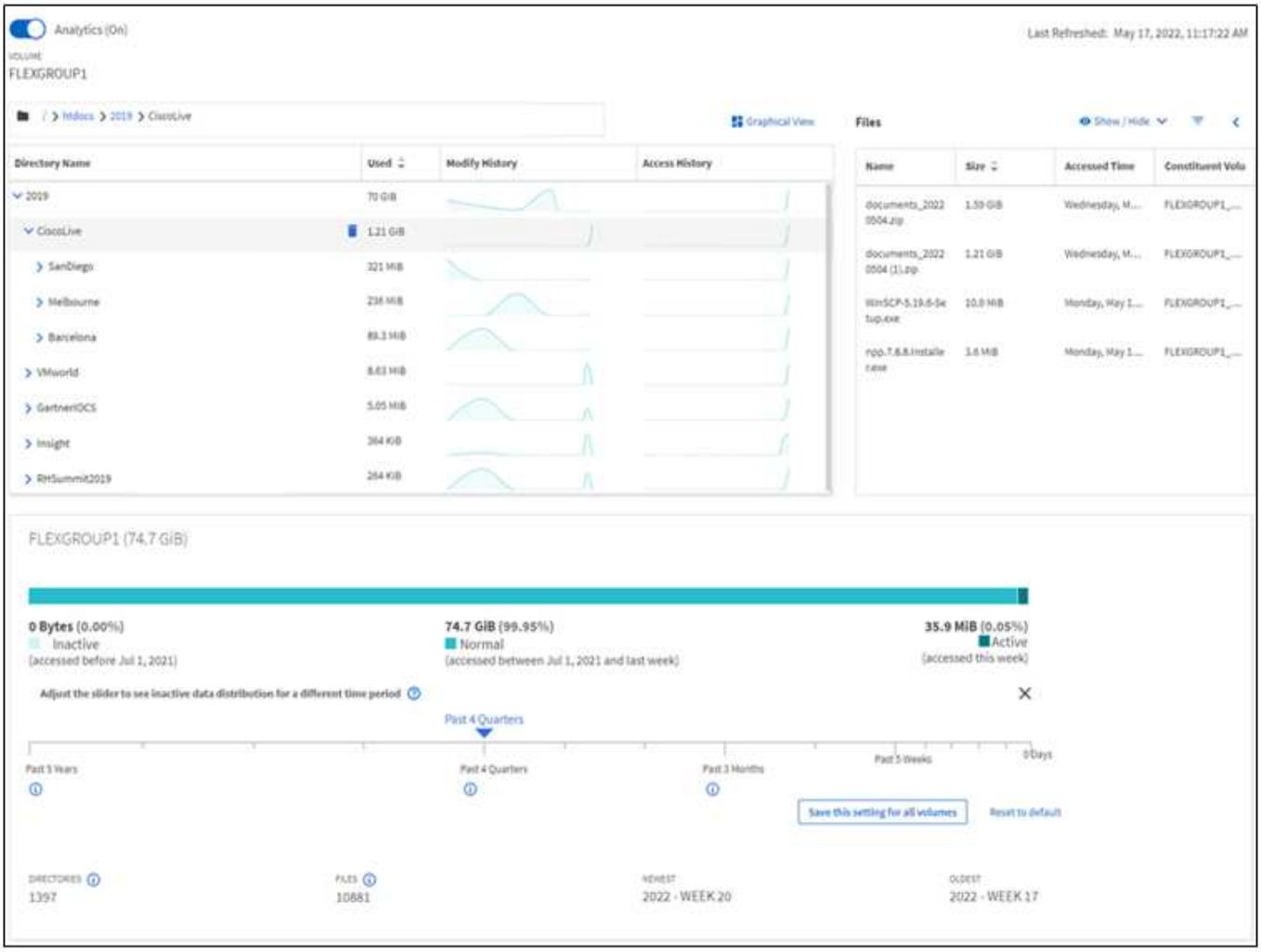
Le service File System Analytics (FSA) a été intégré à ONTAP 9.8 pour fournir une visibilité en temps réel sur l'utilisation des fichiers et les tendances en matière de capacité de stockage au sein des volumes ONTAP FlexGroup ou FlexVol. Cette fonctionnalité native élimine la nécessité de disposer d'outils externes et fournit des informations essentielles sur l'utilisation du stockage et sur les possibilités d'optimisation du stockage en fonction des besoins de l'entreprise.

Avec FSA, vous disposez d'une visibilité à tous les niveaux de la hiérarchie du système de fichiers d'un volume dans NAS. Par exemple, vous pouvez obtenir des informations sur l'utilisation et la capacité au niveau des VM de stockage (SVM), des volumes, des répertoires et des fichiers. Ce compte vous permet de répondre à des questions telles que :

- Qu'est-ce qui remplit mon système de stockage et y a-t-il des fichiers volumineux que je peux déplacer vers un autre emplacement de stockage ?
- Quels sont mes volumes, répertoires et fichiers les plus actifs ? Mes performances de stockage sont-elles optimisées pour répondre aux besoins de mes utilisateurs ?
- Quelle quantité de données ont été ajoutées au mois dernier ?
- Qui sont mes utilisateurs de stockage les plus actifs ou les moins actifs ?
- Quel est le volume de données inactives ou inactives sur mon stockage primaire ? Puis-je déplacer ces données vers un niveau à froid moins coûteux ?
- Les modifications planifiées de la qualité de service auront-elles une incidence négative sur l'accès aux fichiers stratégiques fréquemment utilisés ?

L'analytique du système de fichiers est intégrée à ONTAP System Manager. Les vues dans System Manager fournissent les éléments suivants :

- Visibilité en temps réel pour une gestion et un fonctionnement efficaces des données
- Collecte et agrégation des données en temps réel
- Tailles et nombres de fichiers et de sous-répertoires, ainsi que les profils de performances associés
- Classez les histogrammes d'âge pour modifier et accéder aux historiques



Types de volume pris en charge

L'analytique du système de fichiers est conçue pour fournir une visibilité sur les volumes contenant des données NAS actives, à l'exception des caches FlexCache et des volumes de destination SnapMirror.

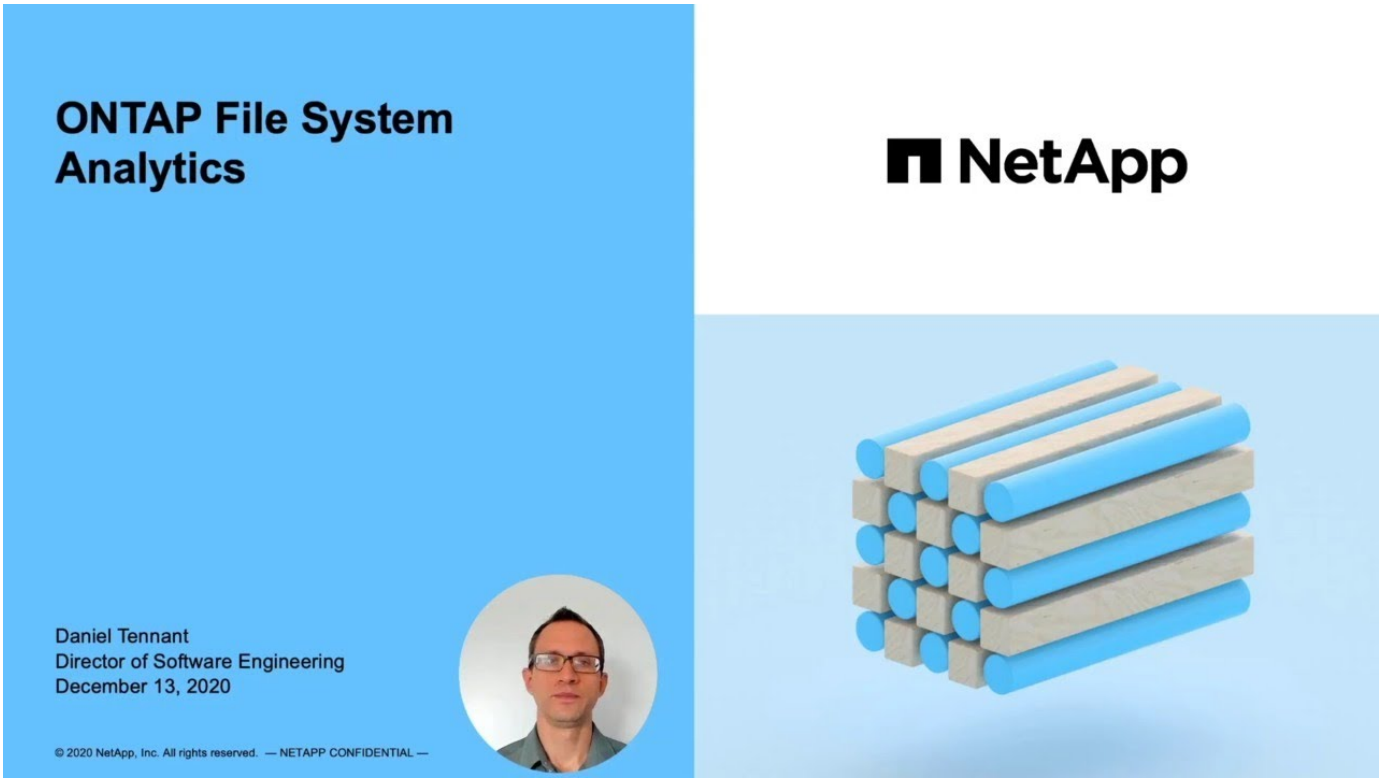
Disponibilité des fonctions d'analytique du système de fichiers

Chaque version d'ONTAP étend l'étendue de l'analytique des systèmes de fichiers.

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
Visualisation dans System Manager	✓	✓	✓	✓	✓	✓	✓
Analyse de la capacité	✓	✓	✓	✓	✓	✓	✓
Informations sur les données inactives	✓	✓	✓	✓	✓	✓	✓
La prise en charge des volumes a migré depuis Data ONTAP 7-mode	✓	✓	✓	✓	✓	✓	

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
Personnalisation de la période inactive dans System Manager	✓	✓	✓	✓	✓	✓	
Suivi des activités au niveau du volume	✓	✓	✓	✓	✓		
Téléchargez les données de suivi d'activité au format CSV	✓	✓	✓	✓	✓		
Suivi d'activité au niveau de SVM	✓	✓	✓	✓			
De la chronologie	✓	✓	✓	✓			
Analyse de l'utilisation	✓	✓	✓				
Option permettant d'activer l'analyse du système de fichiers par défaut	✓	✓					
Moniteur de progression de l'acquisition d'initialisation	✓						

En savoir plus sur l'analytique des systèmes de fichiers



Plus de lecture

- "Tr 4687 : recommandations sur les meilleures pratiques pour l'analytique des systèmes de fichiers ONTAP"
- "Base de connaissances : latence élevée ou variable après l'activation de l'analytique du système de fichiers ONTAP de NetApp"

Activez l'analyse du système de fichiers

Pour collecter et afficher des données d'utilisation telles que l'analyse de la capacité, vous devez activer l'analytique du système de fichiers sur un volume.

Description de la tâche

- Depuis ONTAP 9.8, vous pouvez activer l'analytique du système de fichiers sur un volume nouveau ou existant. Si vous mettez à niveau un système vers ONTAP 9.8 ou une version ultérieure, assurez-vous que tous les processus de mise à niveau sont terminés avant d'activer l'analyse du système de fichiers.
- Selon la taille et le contenu du volume, l'activation d'une fonctionnalité d'analytique peut prendre du temps pendant le traitement des données existantes dans le volume par ONTAP. System Manager affiche la progression et présente les données analytiques une fois terminées. Si vous avez besoin d'informations plus précises sur la progression de l'initialisation, vous pouvez utiliser la commande d'interface de ligne de commandes de ONTAP `volume analytics show`.

  À partir de ONTAP 9.14.1, ONTAP fournit un suivi de la progression de l'analyse d'initialisation en plus des notifications sur les événements de limitation qui affectent la progression de l'analyse.

  Pour plus d'informations sur l'acquisition d'initialisation, reportez-vous à la section Considérations relatives à l'analyse.

Étapes

Vous pouvez activer l'analytique du système de fichiers avec ONTAP System Manager ou l'interface de ligne de commande.

System Manager

À ONTAP 9.8 et 9.9.1	À partir de ONTAP 9.10.1
1. Sélectionnez **stockage > volumes**. 2. Sélectionnez le volume souhaité, puis **Explorer**. 3. Sélectionnez **Activer les analyses** ou **Désactiver les analyses**.	1. Sélectionnez **stockage > volumes**. 2. Sélectionnez le volume souhaité. Dans le menu volume individuel, sélectionnez **système de fichiers > Explorateur**. 3. Sélectionnez **Activer les analyses** ou **Désactiver les analyses**.

CLI

Activez l'analyse du système de fichiers à l'aide de la CLI

1. Exécutez la commande suivante :
   `volume analytics on -vserver` *`svm_name`* `-volume` *`volume_name`* `[-foreground {true|false}]`
   Par défaut, la commande s'exécute au premier plan ; ONTAP affiche la progression et présente les données analytiques une fois l'opération terminée. Si vous avez besoin d'informations plus précises, vous pouvez exécuter la commande en arrière-plan à l'aide de la `-foreground false` puis utilisez l' `volume analytics show` Commande permettant d'afficher la progression de l'initialisation dans l'interface de ligne de commandes.
2. Une fois l'analyse du système de fichiers terminée, utilisez System Manager ou l'API REST ONTAP pour afficher les données analytiques.

Modifier les paramètres par défaut de l'analyse du système de fichiers

À partir de la version ONTAP 9.13.1, vous pouvez modifier les paramètres des SVM ou des clusters pour activer l'analytique du système de fichiers par défaut sur les nouveaux volumes.

System Manager

Si vous utilisez System Manager, vous pouvez modifier les paramètres de la machine virtuelle de stockage ou du cluster pour activer l'analyse de la capacité et le suivi des activités lors de la création du volume par défaut. L'activation par défaut s'applique uniquement aux volumes créés après la modification des paramètres, et non aux volumes existants.

Modifier les paramètres d'analyse du système de fichiers sur un cluster

1. Dans System Manager, accédez à **Paramètres de cluster**.
2. Dans **Paramètres du cluster**, consultez l'onglet Paramètres du système de fichiers. Pour modifier les paramètres, sélectionnez icône.
3. Dans le champ **Activity Tracking**, entrez les noms des SVM pour lequel le suivi des activités est activé par défaut. Si vous ne renseignez pas ce champ, le suivi d'activité sera désactivé sur tous les SVM.

   Décochez la case **Activer sur les nouveaux ordinateurs virtuels de stockage** pour désactiver le suivi des activités par défaut sur les nouveaux ordinateurs virtuels de stockage.

4. Dans le champ **Analytics**, entrez les noms des machines virtuelles de stockage pour lesquels l'analyse des capacités doit être activée par défaut. Si vous ne renseignez pas ce champ, l'analyse de la capacité est désactivée sur tous les SVM.

   Décochez la case **Activer sur les nouvelles machines virtuelles de stockage** pour désactiver l'analyse des capacités par défaut sur les nouvelles machines virtuelles de stockage.

5. Sélectionnez **Enregistrer**.

Modification des paramètres d'analytique du système de fichiers sur une SVM

1. Sélectionner le SVM à modifier puis **Storage VM settings**.
2. Dans la carte **File System Analytics**, utilisez les commutateurs pour activer ou désactiver le suivi des activités et l'analyse des capacités pour tous les nouveaux volumes de la machine virtuelle de stockage.

CLI

Vous pouvez configurer la machine virtuelle de stockage pour activer l'analytique du système de fichiers par défaut sur les nouveaux volumes à l'aide de l'interface de ligne de commande ONTAP.

Activer l'analytique des systèmes de fichiers par défaut sur une SVM

1. Modifier le SVM pour activer l'analytique de capacité et le suivi des activités par défaut sur tous les volumes nouvellement créés :
   `vserver modify -vserver svm_name -auto-enable-activity-tracking true -auto -enable-analytics true`

Afficher l'activité du système de fichiers

Une fois que File System Analytics (FSA) est activé, vous pouvez afficher le contenu du

répertoire racine d'un volume sélectionné trié par espace utilisé dans chaque sous-arborescence.

Sélectionnez un objet système de fichiers pour parcourir le système de fichiers et afficher des informations détaillées sur chaque objet d'un répertoire. Les informations sur les répertoires peuvent également être affichées graphiquement. Au fil du temps, les données historiques sont affichées pour chaque sous-arbre. L'espace utilisé n'est pas trié s'il y a plus de 3000 répertoires.

Explorateur

L'écran File System Analytics **Explorer** comprend trois zones :

- Arborescence des répertoires et sous-répertoires ; liste extensible indiquant le nom, la taille, l'historique des modifications et l'historique des accès.
- Fichiers ; affichage du nom, de la taille et du temps d'accès de l'objet sélectionné dans la liste de répertoires.
- Comparaison des données actives et inactives pour l'objet sélectionné dans la liste des répertoires.

  Depuis ONTAP 9.9.1, vous pouvez personnaliser la plage à laquelle vous souhaitez faire état. La valeur par défaut est un an. En fonction de ces personnalisations, il est possible d'effectuer des actions correctives, telles que le déplacement de volumes et la modification de la règle de hiérarchisation.

L'heure d'accès est affichée par défaut. Cependant, si la valeur par défaut du volume a été modifiée à partir de l'interface de ligne de commande (en définissant le paramètre `-atime-update` option à `false` avec le `volume modify` commande), seule la dernière heure modifiée est affichée. Par exemple :

- L'arborescence n'affiche pas l'historique **Access**.
- La vue fichiers sera modifiée.
- La vue des données actives/inactives est basée sur l'heure modifiée (`mtime`).

Ces affichages permettent d'examiner les éléments suivants :

- Les emplacements des systèmes de fichiers consomment le plus d'espace
- Informations détaillées sur une arborescence de répertoires, y compris le nombre de fichiers et de sous-répertoires dans les répertoires et sous-répertoires
- Emplacements des systèmes de fichiers contenant d'anciennes données (par exemple, égratignures, temporaires ou arborescences des journaux)

Gardez à l'esprit les points suivants lors de l'interprétation des résultats de FSA :

- FSA affiche où et quand vos données sont en cours d'utilisation, pas la quantité de données traitées. Par exemple, la consommation d'espace importante pour les fichiers récemment utilisés ou modifiés n'indique pas nécessairement des charges de traitement système élevées.
- La façon dont l'onglet **Volume Explorer** calcule la consommation d'espace pour FSA peut différer des autres outils. En particulier, il peut y avoir des différences significatives par rapport à la consommation indiquée dans **Volume Overview** si les fonctions d'efficacité du stockage du volume sont activées. Cela est dû au fait que l'onglet **Volume Explorer** n'inclut pas les économies d'efficacité.
- En raison des limitations d'espace dans l'affichage du répertoire, il n'est pas possible d'afficher une profondeur de répertoire supérieure à 8 niveaux dans *List View*. Pour afficher des répertoires de plus de 8 niveaux au fond, vous devez passer à *Graphical View*, localiser le répertoire souhaité, puis revenir à *List*

View. Cela permet d'ajouter de l'espace à l'écran.

Étapes

1. Afficher le contenu du répertoire racine d'un volume sélectionné :

À ONTAP 9.8 et 9.9.1	À partir de ONTAP 9.10.1
Cliquez sur **stockage > volumes**, sélectionnez le volume souhaité, puis cliquez sur **Explorer**.	Sélectionnez **stockage > volumes**, puis sélectionnez le volume souhaité. Dans le menu volume individuel, sélectionnez **système de fichiers > Explorateur**.

Activer le suivi des activités

À partir de ONTAP 9.10.1, l'analyse du système de fichiers inclut une fonction de suivi des activités qui vous permet d'identifier les objets sensibles et de télécharger les données sous forme de fichier CSV. Depuis ONTAP 9.11.1, le suivi de l'activité est étendu au périmètre de la SVM. À partir de ONTAP 9.11.1, System Manager propose également une chronologie pour le suivi des activités, vous permettant d'examiner jusqu'à cinq minutes de données de suivi des activités.

Le suivi des activités permet la surveillance en quatre catégories :

- Répertoires
- Fichiers
- Clients
- Utilisateurs

Pour chaque catégorie surveillée, Activity Tracking affiche les IOPS en lecture, les IOPS en écriture, les débits de lecture et les débits d'écriture. Les requêtes sur le suivi d'activité se réactualisent toutes les 10 à 15 secondes en rapport avec les points sensibles observés dans le système au cours de l'intervalle de cinq secondes précédent.

Les informations de suivi d'activité sont approximatives et la précision des données dépend de la distribution du trafic d'E/S entrant.

Lors de l'affichage du suivi d'activité dans System Manager au niveau du volume, seul le menu du volume étendu est actualisé activement. Si l'affichage d'un volume est réduit, il ne sera pas actualisé tant que l'affichage du volume n'aura pas été développé. Vous pouvez arrêter les actualisations à l'aide du bouton **Pause Rafraîchir**. Les données d'activité peuvent être téléchargées au format CSV pour afficher toutes les données ponctuelles capturées pour le volume sélectionné.

La fonction de chronologie proposée sous ONTAP 9.11.1 vous permet de conserver un enregistrement d'activité de zone sensible sur un volume ou une SVM, en mettant à jour en continu environ toutes les cinq secondes et en conservant les données des cinq minutes précédentes. Les données de chronologie ne sont conservées que pour les champs qui sont une zone visible de la page. Si vous réduisez une catégorie de suivi ou faites défiler de façon à ce que la chronologie ne soit plus en vue, la chronologie arrête de collecter les données. Par défaut, les délais sont désactivés et sont automatiquement désactivés lorsque vous vous éloignez de l'onglet activité.

Activez le suivi des activités pour un seul volume

Vous pouvez activer le suivi des activités avec ONTAP System Manager ou l'interface de ligne de commande.

Description de la tâche

Si vous utilisez le RBAC avec l'API REST de ONTAP ou System Manager, vous devez créer des rôles personnalisés pour gérer l'accès au suivi des activités. Voir Contrôle d'accès basé sur des rôles pour ce processus.

System Manager

Étapes

1. Sélectionnez **stockage > volumes**. Sélectionnez le volume souhaité. Dans le menu volume individuel, sélectionnez système de fichiers, puis sélectionnez l'onglet activité.
2. Assurez-vous que **suivi d'activité** est activé pour afficher des rapports individuels sur les répertoires, les fichiers, les clients et les utilisateurs supérieurs.
3. Pour analyser des données plus en profondeur sans actualiser, sélectionnez **Pause Rafraîchir**. Vous pouvez également télécharger les données pour obtenir un enregistrement CSV du rapport.

CLI

Étapes

1. Activer le suivi d'activité :

   ```
   volume activity-tracking on -vserver svm_name -volume volume_name
   ```

2. Vérifiez si l'état suivi d'activité d'un volume est activé ou désactivé à l'aide de la commande :

   ```
   volume activity-tracking show -vserver svm_name -volume volume_name -state
   ```

3. Une fois activée, utilisez ONTAP System Manager ou l'API REST ONTAP pour afficher les données de suivi d'activité.

Activez le suivi des activités pour plusieurs volumes

Vous pouvez activer le suivi des activités pour plusieurs volumes avec System Manager ou l'interface de ligne de commande.

Description de la tâche

Si vous utilisez le RBAC avec l'API REST de ONTAP ou System Manager, vous devez créer des rôles personnalisés pour gérer l'accès au suivi des activités. Voir Contrôle d'accès basé sur des rôles pour ce processus.

System Manager

Activez pour des volumes spécifiques

1. Sélectionnez **stockage > volumes**. Sélectionnez le volume souhaité. Dans le menu volume individuel, sélectionnez système de fichiers, puis sélectionnez l'onglet activité.
2. Sélectionnez les volumes sur lesquels vous souhaitez activer le suivi d'activité. En haut de la liste des volumes, sélectionnez le bouton **plus d'options**. Sélectionnez **Activer le suivi d'activité**.
3. Pour afficher le suivi des activités au niveau du SVM, sélectionnez le SVM spécifique que vous souhaitez afficher dans **Storage > volumes**. Naviguez jusqu'à l'onglet système de fichiers, puis activité et vous verrez les données des volumes sur lesquels le suivi d'activité est activé.

Activer pour tous les volumes

1. Sélectionnez **stockage > volumes**. Sélectionner un SVM dans le menu.
2. Accédez à l'onglet **système de fichiers**, choisissez l'onglet **plus** pour activer le suivi d'activité sur tous les volumes de la SVM.

CLI

À partir de ONTAP 9.13.1, vous pouvez activer le suivi d'activité pour plusieurs volumes à l'aide de l'interface de ligne de commande ONTAP.

Étapes

1. Activer le suivi d'activité :

   `volume activity-tracking on -vserver` *`svm_name`* `-volume [*|!`*`volume_names`*`]`

   Utiliser `*` Pour activer le suivi des activités pour tous les volumes de la machine virtuelle de stockage spécifiée.

   Utiliser `!` Suivi des noms de volumes pour activer le suivi d'activité pour tous les volumes du SVM à l'exception des volumes nommés.

2. Confirmez que l'opération a réussi :

   `volume show -fields activity-tracking-state`

3. Une fois activée, utilisez ONTAP System Manager ou l'API REST ONTAP pour afficher les données de suivi d'activité.

Analytique de l'utilisation

À partir de ONTAP 9.12.1, vous pouvez activer l'analyse de l'utilisation pour voir quels répertoires d'un volume utilisent le plus d'espace. Vous pouvez afficher le nombre total de répertoires d'un volume ou le nombre total de fichiers d'un volume. La création de rapports est limitée aux répertoires 25 qui utilisent le plus d'espace.

Les analyses des répertoires volumineux sont actualisées toutes les 15 minutes. Vous pouvez contrôler l'actualisation la plus récente en vérifiant l'horodatage de la dernière actualisation en haut de la page. Vous pouvez également cliquer sur le bouton Télécharger pour télécharger des données dans un classeur Excel. L'opération de téléchargement s'exécute en arrière-plan et présente les informations les plus récentes pour le volume sélectionné. Si l'analyse revient sans résultat, vérifiez que le volume est en ligne. Des événements tels

que SnapRestore entraînent la reconstruction de la liste de grands répertoires par l'analytique système de fichiers.

Étapes

1. Sélectionnez **stockage > volumes**. Sélectionnez le volume souhaité.
2. Dans le menu volume individuel, sélectionnez **système de fichiers**. Sélectionnez ensuite l'onglet **usage**.
3. Activez l'option **Analytics** pour activer l'analyse de l'utilisation.
4. System Manager affiche un graphique à barres identifiant les répertoires dont la taille est la plus grande dans l'ordre décroissant.

> ONTAP peut afficher des données partielles ou aucune donnée du tout pendant la collecte de la liste des principaux répertoires. La progression de l'acquisition peut se trouver dans l'onglet **usage** qui s'affiche pendant l'acquisition.

Pour obtenir plus d'informations sur un répertoire spécifique, vous pouvez le faire afficher l'activité sur un système de fichiers.

Prendre les mesures correctives basées sur l'analytique

Depuis ONTAP 9.9.1, vous pouvez effectuer des actions correctives en fonction des données actuelles et des résultats souhaités, directement à partir des affichages d'analytique du système de fichiers.

Supprimez des répertoires et des fichiers

Dans l'écran de l'Explorateur, vous pouvez sélectionner des répertoires ou des fichiers individuels à supprimer. Les répertoires sont supprimés avec une fonctionnalité de suppression rapide des répertoires à faible latence. (La suppression rapide des répertoires est également disponible depuis ONTAP 9.9.1, sans activation des analyses.)

Étapes

1. Cliquez sur **Storage > volumes**, puis sur **Explorer**.

   Lorsque vous placez le pointeur de la souris sur un fichier ou un dossier, l'option de suppression apparaît. Vous ne pouvez supprimer qu'un seul objet à la fois.

> Lorsque des répertoires et des fichiers sont supprimés, les nouvelles valeurs de capacité de stockage ne sont pas affichées immédiatement.

Attribuez le coût du support dans les tiers de stockage pour comparer les coûts des emplacements de stockage de données inactifs

Le coût du support est une valeur que vous attribuez en fonction de votre évaluation des coûts de stockage, représentée comme la devise par Go de votre choix. Lorsqu'il est défini, System Manager utilise le coût de support attribué pour projeter les économies estimées lors du déplacement des volumes.

Le coût de support que vous avez défini n'est pas persistant ; il ne peut être défini que pour une seule session de navigateur.

Étapes

1. Cliquez sur **stockage > niveaux**, puis cliquez sur **définir le coût du support** dans les mosaïques de niveau local (agrégat) souhaitées.

   Veillez à sélectionner les tiers actifs et inactifs pour permettre la comparaison.

2. Entrez un type de devise et un montant.

   Lorsque vous saisissez ou modifiez le coût du support, la modification est effectuée dans tous les types de support.

Déplacez des volumes pour réduire les coûts de stockage

En se basant sur des analyses et des comparaisons des coûts des supports, vous pouvez déplacer des volumes vers un stockage moins coûteux au niveau local.

Vous ne pouvez comparer et déplacer qu'un seul volume à la fois.

Étapes

1. Une fois l'affichage du coût du support pris en charge, cliquez sur **stockage > niveaux**, puis sur **volumes**.
2. Pour comparer les options de destination d'un volume, cliquez sur ⋮ Pour le volume, puis cliquez sur **déplacer**.
3. Dans l'écran **Sélectionner le niveau local** de destination, sélectionnez les niveaux de destination pour afficher la différence de coût estimée.
4. Après avoir comparé les options, sélectionnez le niveau souhaité et cliquez sur **déplacer**.

Contrôle d'accès basé sur des rôles avec File System Analytics

À partir de ONTAP 9.12.1, ONTAP inclut un rôle de contrôle d'accès basé sur des rôles (RBAC) prédéfini appelé `admin-no-fsa`. Le `admin-no-fsa` le rôle accorde des privilèges de niveau administrateur mais empêche l'utilisateur d'effectuer des opérations liées à l' `files` Terminal (analytique du système de fichiers) dans l'interface de ligne de commande ONTAP, l'API REST et dans System Manager.

Pour plus d'informations sur le `admin-no-fsa` rôle, voir Rôles prédéfinis pour les administrateurs du cluster.

Si vous utilisez une version de ONTAP antérieure à ONTAP 9.12.1, vous devrez créer un rôle dédié pour contrôler l'accès à l'analyse du système de fichiers. Dans les versions de ONTAP antérieures à ONTAP 9.12.1, vous devez configurer les autorisations RBAC via l'interface de ligne de commande d'ONTAP ou l'API REST d'ONTAP.

System Manager

À partir de ONTAP 9.12.1, vous pouvez configurer les autorisations RBAC pour l'analyse du système de fichiers à l'aide de System Manager.

Étapes

1. Sélectionnez **Cluster > Paramètres**. Sous **sécurité**, accédez à **utilisateurs et rôles** et sélectionnez →.
2. Sous **rôles**, sélectionnez + Add .
3. Indiquez un nom pour le rôle. Sous attributs de rôle, configurez l'accès ou les restrictions pour le rôle d'utilisateur en fournissant le approprié "Terminaux d'API". Consultez le tableau ci-dessous pour connaître les chemins principaux et secondaires permettant de configurer l'accès ou les restrictions de l'analyse du système de fichiers.

Restriction	Chemin primaire	Chemin secondaire
Suivi d'activité sur les volumes	`/api/storage/volumes`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
Suivi de l'activité sur les SVM	`/api/svm/svms`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
Toutes les opérations d'analyse du système de fichiers	`/api/storage/volumes`	`/:uuid/files`

   Vous pouvez utiliser `/*/` Au lieu d'un UUID afin de définir la règle pour tous les volumes ou SVM sur le terminal.

   Choisissez les privilèges d'accès pour chaque noeud final.

4. Sélectionnez **Enregistrer**.
5. Pour attribuer le rôle à un ou plusieurs utilisateurs, voir Contrôlez l'accès administrateur.

CLI

Si vous utilisez une version de ONTAP antérieure à ONTAP 9.12.1, créez un rôle personnalisé à l'aide de

l'interface de ligne de commandes de ONTAP.

Étapes

1. Créez un rôle par défaut pour accéder à toutes les fonctions.

   Cette opération doit être effectuée avant de créer le rôle restrictif afin de garantir que le rôle n'est que restrictif sur le suivi d'activité :

   ```
   security login role create -cmddirname DEFAULT -access all -role
   storageAdmin
   ```

2. Créer le rôle restrictif :

   ```
   security login role create -cmddirname "volume file show-disk-usage"
   -access none -role storageAdmin
   ```

3. Autoriser les rôles à accéder aux services web du SVM :

   - `rest` Pour les appels API REST
   - `security` pour la protection par mot de passe
   - `sysmgr` Pour accéder à System Manager

     ```
     vserver services web access create -vserver svm-name -name_ -name rest
     -role storageAdmin

     vserver services web access create -vserver svm-name -name security
     -role storageAdmin
     ```

   ```
   vserver services web access create -vserver svm-name -name sysmgr -role
   storageAdmin
   ```

4. Créer un utilisateur.

   Vous devez exécuter une commande de création distincte pour chaque application que vous souhaitez appliquer à l'utilisateur. Les appels créent plusieurs fois sur le même utilisateur appliquent simplement toutes les applications à cet utilisateur et ne créent pas de nouvel utilisateur à chaque fois. Le `http` Le paramètre pour le type d'application s'applique à l'API REST ONTAP et à System Manager.

   ```
   security login create -user-or-group-name storageUser -authentication
   -method password -application http -role storageAdmin
   ```

5. Avec les nouvelles informations d'identification utilisateur, vous pouvez désormais vous connecter à System Manager ou utiliser l'API REST de ONTAP pour accéder aux données d'analytique des systèmes de fichiers.

Plus d'informations

- Rôles prédéfinis pour les administrateurs du cluster
- Contrôle de l'accès administrateur avec System Manager
- "En savoir plus sur les rôles RBAC et l'API REST de ONTAP"

Considérations relatives à l'analytique des systèmes de fichiers

Vous devez connaître les limites d'utilisation et les impacts potentiels sur les performances associés à l'implémentation de File System Analytics.

Relations protégées par un SVM

Si vous avez activé File System Analytics sur les volumes dont le SVM contient fait partie d'une relation de protection, les données d'analytique ne sont pas répliquées vers le SVM de destination. Si le SVM source doit être resynchronisé dans une opération de restauration, vous devez de nouveau activer manuellement l'analytique sur les volumes souhaités après sa restauration.

Performances

Dans certains cas, l'activation d'une analytique système de fichiers peut avoir un impact négatif sur les performances lors de la collecte de métadonnées initiale. Cela est généralement le plus fréquemment observé sur les systèmes qui atteignent une utilisation maximale. Pour éviter l'activation de l'analytique sur ces systèmes, vous pouvez utiliser les outils de contrôle des performances de ONTAP System Manager.

Si vous constatez une augmentation notable de la latence, consultez l'article de la base de connaissances "Latence élevée ou variable après l'activation de l'analytique système de fichiers ONTAP de NetApp".

Considérations relatives à l'analyse

Lorsque vous activez l'analyse de la capacité, ONTAP effectue une analyse d'initialisation pour l'analyse de la capacité. L'analyse accède aux métadonnées de tous les fichiers des volumes pour lesquels l'analyse de capacité est activée. Aucune donnée de fichier n'est lue pendant l'acquisition. À partir de ONTAP 9.14.1, vous pouvez suivre la progression de l'analyse avec l'API REST, dans l'onglet **Explorer** du Gestionnaire système ou avec le `volume analytics show` Commande CLI. En cas d'événement d'accélération, ONTAP envoie une notification.

Une fois l'analyse terminée, l'analyse du système de fichiers est mise à jour en temps réel en continu au fur et à mesure que le système de fichiers change, sans qu'il soit nécessaire d'exécuter à nouveau l'analyse.

Le temps requis pour l'analyse est proportionnel au nombre de répertoires et de fichiers sur le volume. Étant donné que l'analyse collecte des métadonnées, la taille du fichier n'a pas d'incidence sur le temps d'analyse.

Pour plus d'informations sur l'acquisition d'initialisation, reportez-vous à la section "Tr-4867 : recommandations sur les bonnes pratiques pour l'analytique de système de fichiers".

Et des meilleures pratiques

Vous devez démarrer l'analyse sur des volumes qui ne partagent pas d'agrégats. Vous pouvez voir quels agrégats hébergent actuellement les volumes à l'aide de la commande :

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

Pendant l'analyse, les volumes continuent de transmettre le trafic client. Il est recommandé de démarrer l'analyse pendant les périodes où vous prévoyez un trafic client plus faible.

Si le trafic client augmente, il consomme les ressources système et allonge l'analyse.

À partir de ONTAP 9.12.1, vous pouvez interrompre la collecte de données dans System Manager et via l'interface de ligne de commandes ONTAP.

- Si vous utilisez l'interface de ligne de commandes ONTAP :
  - Vous pouvez interrompre la collecte de données à l'aide de la commande : `volume analytics initialization pause -vserver svm_name -volume volume_name`
  - Une fois le trafic client ralenti, vous pouvez reprendre la collecte de données à l'aide de la commande : `volume analytics initialization resume -vserver svm_name -volume volume_name`
- Si vous utilisez System Manager, dans la vue **Explorer** du menu volume, vous utilisez les boutons **Pause collecte de données** et **reprendre collecte de données** pour gérer l'acquisition.

Configuration EMS

Présentation de la configuration EMS

Vous pouvez configurer ONTAP 9 pour envoyer des notifications d'événements EMS (Event Management System) importantes directement à une adresse e-mail, un serveur syslog, un traphost SNMP (simple Management Network Protocol) ou une application webhook afin que vous soyez immédiatement averti des problèmes système nécessitant une intervention rapide.

Comme les notifications d'événements importantes ne sont pas activées par défaut, vous devez configurer l'EMS pour qu'il envoie des notifications à une adresse e-mail, à un serveur syslog, à un traphost SNMP ou à une application webhook.

Examiner les versions spécifiques à la version du "Référence EMS ONTAP 9".

Si votre mappage d'événements EMS utilise des jeux de commandes ONTAP obsolètes (comme la destination de l'événement, la route des événements), il est recommandé de mettre à jour votre mappage. "Découvrez comment mettre à jour votre mappage EMS à partir de commandes ONTAP obsolètes".

Configurez les notifications d'événement EMS et les filtres avec System Manager

Vous pouvez utiliser System Manager pour configurer la manière dont le système EMS (Event Management System) envoie des notifications d'événements afin de vous informer des problèmes système qui nécessitent une intervention rapide.

Version ONTAP	Grâce à System Manager, vous pouvez…
ONTAP 9.12.1 et versions ultérieures	Spécifiez le protocole TLS (transport Layer Security) lors de l'envoi d'événements vers des serveurs syslog distants.
ONTAP 9.10.1 et versions ultérieures	Configurez les adresses électroniques, les serveurs syslog et les applications webhook, ainsi que les Traphosts SNMP.
ONTAP 9.7 à 9.10.0	Configurez uniquement les Traphosts SNMP. Vous pouvez configurer d'autres destinations EMS à l'aide de l'interface de ligne de commande ONTAP. Voir "Présentation de la configuration EMS".

Vous pouvez effectuer les opérations suivantes :

- [add-ems-destination]
- [create-ems-filter]
- [edit-ems-destination]
- [edit-ems-filter]
- [delete-ems-destination]
- [delete-ems-filter]

Informations associées

- "Référence ONTAP EMS"
- "Utilisation de l'interface de ligne de commande pour configurer les Traphosts SNMP pour recevoir des notifications d'événements"

Ajouter une destination de notification d'événement EMS

Vous pouvez utiliser System Manager pour spécifier l'emplacement d'envoi des messages EMS.

Depuis ONTAP 9.12.1, les événements EMS peuvent être envoyés vers un port désigné sur un serveur syslog distant via le protocole TLS (transport Layer Security). Pour plus d'informations, reportez-vous à la `event notification destination create` page de manuel.

Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **Notifications Management**, cliquez sur ⋮, Puis cliquez sur **Afficher les destinations de l'événement**.
3. Sur la page **gestion des notifications**, sélectionnez l'onglet **destinations d'événements**.
4. Cliquez sur + Add .
5. Spécifiez un nom, un type de destination EMS et des filtres.

   ⓘ Si nécessaire, vous pouvez ajouter un nouveau filtre. Cliquez sur **Ajouter un nouveau filtre d'événements**.

6. En fonction du type de destination EMS que vous avez sélectionné, spécifiez ce qui suit :

Pour configurer…	Spécifiez ou sélectionnez…
Traphost SNMP	• Nom TrapHost
E-mail (À partir de la version 9.10.1)	• Adresse e-mail de destination • Serveur de messagerie • De l'adresse e-mail

Serveur Syslog (À partir de la version 9.10.1)	• Nom d'hôte ou adresse IP du serveur • Port Syslog (commençant par 9.12.1) • Transport Syslog (à partir de 9.12.1) La sélection de **TCP chiffré** active le protocole TLS (transport Layer Security). Si aucune valeur n'est saisie pour **Syslog port**, une valeur par défaut est utilisée en fonction de la sélection **Syslog transport**.
Webhook (À partir de la version 9.10.1)	• URL de Webhook • Authentification client (sélectionnez cette option pour spécifier un certificat client)

Créer un nouveau filtre de notification d'événement EMS

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour définir de nouveaux filtres personnalisés spécifiant les règles de gestion des notifications EMS.

Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **Notifications Management**, cliquez sur ⋮, Puis cliquez sur **Afficher les destinations des événements**.
3. Sur la page **gestion des notifications**, sélectionnez l'onglet **filtres d'événements**.
4. Cliquez sur + Add .
5. Spécifiez un nom et indiquez si vous souhaitez copier des règles à partir d'un filtre d'événements existant ou ajouter de nouvelles règles.
6. Selon votre choix, effectuez les opérations suivantes :

Si vous choisissez….	Puis, effectuez ces étapes…
Copier les règles à partir du filtre d'événements existant	1. Sélectionnez un filtre d'événement existant. 2. Modifier les règles existantes. 3. Ajoutez d'autres règles, si nécessaire, en cliquant sur + Add .
Ajouter de nouvelles règles	Spécifiez le type, le modèle de nom, les niveaux de gravité et le type d'interruption SNMP pour chaque nouvelle règle.

Modifier une destination de notification d'événement EMS

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour modifier les données de destination de la notification d'événement.

Étapes

1. Cliquez sur **Cluster > Paramètres**.

2. Dans la section **Notifications Management**, cliquez sur ⋮, Puis cliquez sur **Afficher les destinations de l'événement**.
3. Sur la page **Notifications Management**, sélectionnez l'onglet **Evénements destinations**.
4. En regard du nom de la destination de l'événement, cliquez sur ⋮, Puis cliquez sur **Modifier**.
5. Modifiez les informations de destination de l'événement, puis cliquez sur **Enregistrer**.

Modifier un filtre de notification d'événement EMS

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour modifier les filtres personnalisés afin de modifier le mode de traitement des notifications d'événements.

ⓘ Vous ne pouvez pas modifier les filtres définis par le système.

Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **Notifications Management**, cliquez sur ⋮, Puis cliquez sur **Afficher les destinations des événements**.
3. Sur la page **gestion des notifications**, sélectionnez l'onglet **filtres d'événements**.
4. En regard du nom du filtre d'événements, cliquez sur ⋮, Puis cliquez sur **Modifier**.
5. Modifiez les informations de filtre d'événement, puis cliquez sur **Enregistrer**.

Supprimer une destination de notification d'événement EMS

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour supprimer une destination de notification d'événement EMS.

ⓘ Vous ne pouvez pas supprimer des destinations SNMP.

Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **Notifications Management**, cliquez sur ⋮, Puis cliquez sur **Afficher les destinations des événements**.
3. Sur la page **gestion des notifications**, sélectionnez l'onglet **destinations d'événements**.
4. En regard du nom de la destination de l'événement, cliquez sur ⋮, Puis cliquez sur **Supprimer**.

Supprimer un filtre de notification d'événement EMS

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour supprimer des filtres personnalisés.

ⓘ Vous ne pouvez pas supprimer des filtres définis par le système.

Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **Notifications Management**, cliquez sur ⋮, Puis cliquez sur **Afficher les destinations des événements**.
3. Sur la page **gestion des notifications**, sélectionnez l'onglet **filtres d'événements**.

4. En regard du nom du filtre d'événements, cliquez sur ⋮, Puis cliquez sur **Supprimer**.

Configurez les notifications d'événements EMS avec l'interface de ligne de commande

Flux de travail de configuration EMS

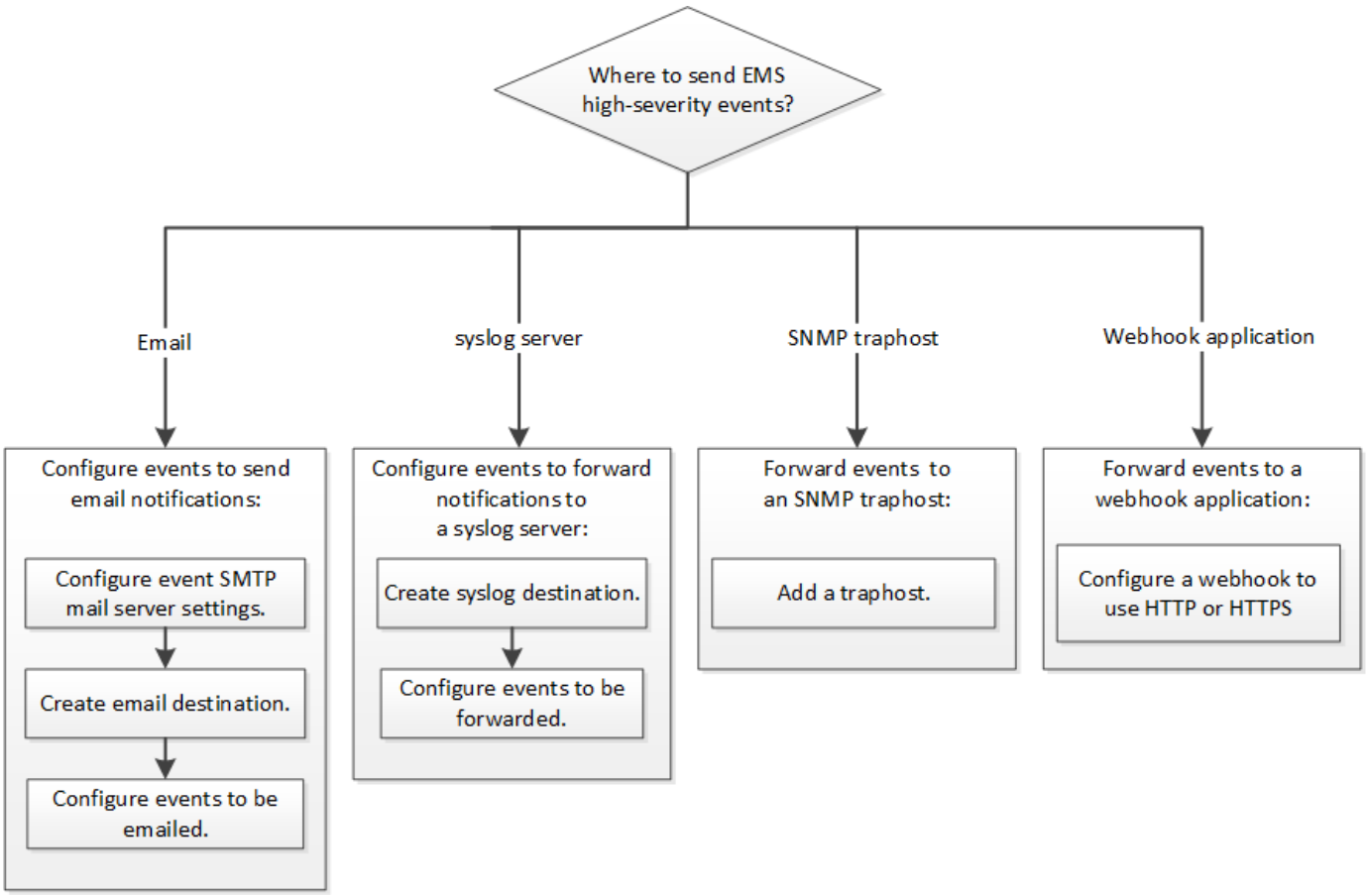
Vous devez configurer les notifications d'événements EMS importantes pour qu'elles soient envoyées par e-mail, envoyées à un serveur syslog, transférées à un hôte de transfert SNMP ou transmises à une application de connexion Web. Cela vous permet d'éviter toute interruption du système en prenant des actions correctives en temps opportun.

Description de la tâche

Si votre environnement contient déjà un serveur syslog permettant d'agréger les événements journaux d'autres systèmes, tels que des serveurs et des applications, il est plus facile d'utiliser ce serveur syslog également pour recevoir des notifications d'événements importantes provenant des systèmes de stockage.

Si votre environnement ne contient pas encore de serveur syslog, il est plus facile d'utiliser le courrier électronique pour les notifications d'événements importantes.

Si vous transférez déjà des notifications d'événement à un Traphost SNMP, il se peut que vous souhaitiez surveiller ce Traphost pour les événements importants.



Choix

- Configurez EMS pour envoyer des notifications d'événement.

Les fonctions que vous recherchez…	Reportez-vous à ceci…
L'EMS doit envoyer des notifications d'événements importantes à une adresse e-mail	Configurez les événements EMS importants pour envoyer des notifications par e-mail
L'EMS doit transmettre des notifications d'événements importantes à un serveur syslog	Configurez les événements EMS importants pour transférer des notifications à un serveur syslog
Si vous souhaitez que l'EMS envoie des notifications d'événement à un Traphost SNMP	Configurez les Traphosts SNMP pour recevoir des notifications d'événement
Si vous souhaitez que l'EMS envoie des notifications d'événement à une application de connexion Web	Configurez les événements EMS importants pour transférer les notifications vers une application webhook

Configurez les événements EMS importants pour envoyer des notifications par e-mail

Pour recevoir des notifications par e-mail des événements les plus importants, vous devez configurer l'EMS pour qu'il envoie des e-mails pour les événements qui signalent une activité importante.

Ce dont vous avez besoin

Le DNS doit être configuré sur le cluster pour résoudre les adresses e-mail.

Description de la tâche

Vous pouvez effectuer cette tâche à tout moment du cluster en entrant les commandes sur la ligne de commande ONTAP.

Étapes

1. Configurez les paramètres du serveur de messagerie SMTP d'événement :

   ```
   event config modify -mail-server mailhost.your_domain -mail-from
   cluster_admin@your_domain
   ```

2. Créer une destination e-mail pour les notifications d'événements :

   ```
   event notification destination create -name storage-admins -email
   your_email@your_domain
   ```

3. Configurez les événements importants pour envoyer des notifications par e-mail :

   ```
   event notification create -filter-name important-events -destinations storage-
   admins
   ```

Configuration des événements EMS importants pour transférer des notifications à un serveur syslog

Pour enregistrer les notifications des événements les plus graves sur un serveur syslog,

vous devez configurer l'EMS pour transférer les notifications des événements qui signalent une activité importante.

Ce dont vous avez besoin

Le DNS doit être configuré sur le cluster pour résoudre le nom du serveur syslog.

Description de la tâche

Si votre environnement ne contient pas encore de serveur syslog pour les notifications d'événements, vous devez d'abord en créer un. Si votre environnement contient déjà un serveur syslog pour la journalisation des événements à partir d'autres systèmes, vous pouvez l'utiliser pour les notifications d'événements importantes.

Vous pouvez effectuer cette tâche à n'importe quel moment du cluster en entrant les commandes sur l'interface de ligne de commandes de ONTAP.

Depuis ONTAP 9.12.1, les événements EMS peuvent être envoyés vers un port désigné sur un serveur syslog distant via le protocole TLS (transport Layer Security). Deux nouveaux paramètres sont disponibles :

`tcp-encrypted`

Quand `tcp-encrypted` est spécifié pour le `syslog-transport`, ONTAP vérifie l'identité de l'hôte de destination en validant son certificat. La valeur par défaut est `udp-unencrypted`.

`syslog-port`

La valeur par défaut `syslog-port` le paramètre dépend du réglage de l' `syslog-transport` paramètre. Si `syslog-transport` est défini sur `tcp-encrypted`, `syslog-port` a la valeur par défaut 6514.

Pour plus d'informations, reportez-vous à la `event notification destination create` page de manuel.

Étapes

1. Créer une destination de serveur syslog pour les événements importants :

   `event notification destination create -name` *`syslog-ems`* `-syslog` *`syslog-server-address`* `-syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}`

   À partir de ONTAP 9.12.1, les valeurs suivantes peuvent être spécifiées pour `syslog-transport`:

   - `udp-unencrypted` - Protocole de datagramme utilisateur sans sécurité
   - `tcp-unencrypted` - Protocole de contrôle de transmission sans sécurité
   - `tcp-encrypted` - Protocole de contrôle de transmission avec TLS (transport Layer Security)

   Le protocole par défaut est `udp-unencrypted`.

2. Configurez les événements importants pour transférer des notifications au serveur syslog :

   `event notification create -filter-name` *`important-events`* `-destinations` *`syslog-ems`*

Configurez les Traphosts SNMP pour recevoir des notifications d'événement

Pour recevoir des notifications d'événements sur un Traphost SNMP, vous devez

configurer un Traphost.

Ce dont vous avez besoin

- Les traps SNMP doivent être activés sur le cluster.

  Les interruptions SNMP et SNMP sont activées par défaut.

- Le DNS doit être configuré sur le cluster pour résoudre les noms de Traphost.

Description de la tâche

Si aucun Traphost SNMP n'est déjà configuré pour recevoir des notifications d'événements (traps SNMP), vous devez en ajouter un.

Vous pouvez effectuer cette tâche à tout moment du cluster en entrant les commandes sur la ligne de commande ONTAP.

Étape

1. Si votre environnement ne dispose pas déjà d'un Traphost SNMP configuré pour recevoir des notifications d'événement, ajoutez-en un :

   `system snmp traphost add -peer-address` *`snmp_traphost_name`*

   Toutes les notifications d'événements prises en charge par SNMP par défaut sont transmises au Traphost SNMP.

Configurez les événements EMS importants pour transférer les notifications vers une application webhook

Vous pouvez configurer ONTAP pour transférer des notifications d'événements importantes vers une application de connexion Web. Les étapes de configuration nécessaires dépendent du niveau de sécurité que vous choisissez.

Préparez-vous à configurer le transfert d'événements EMS

Vous devez tenir compte de plusieurs concepts et exigences avant de configurer ONTAP pour transférer les notifications d'événements vers une application webhook.

Application Webhook

Vous avez besoin d'une application webhook capable de recevoir les notifications d'événements ONTAP. Un webhook est une routine de rappel définie par l'utilisateur qui étend la capacité de l'application ou du serveur distant où il s'exécute. Les patères sont appelés ou activés par le client (dans ce cas ONTAP) en envoyant une requête HTTP à l'URL de destination. Plus précisément, ONTAP envoie une requête HTTP POST au serveur hébergeant l'application webhook avec les détails de notification d'événement formatés en XML.

Options de sécurité

Plusieurs options de sécurité sont disponibles en fonction de l'utilisation du protocole TLS (transport Layer Security). L'option choisie détermine la configuration ONTAP requise.

TLS est un protocole cryptographique largement utilisé sur Internet. Il assure la confidentialité ainsi que l'intégrité et l'authentification des données à l'aide d'un ou de plusieurs certificats de clé publique. Les certificats sont émis par les autorités de certification de confiance.

HTTP

Vous pouvez utiliser HTTP pour transporter les notifications d'événement. Avec cette configuration, la connexion n'est pas sécurisée. Les identités du client ONTAP et de l'application webhook ne sont pas vérifiées. En outre, le trafic réseau n'est pas chiffré ni protégé. Voir "Configurez une destination de connexion Web pour utiliser HTTP" pour en savoir plus sur la configuration.

HTTPS

Pour plus de sécurité, vous pouvez installer un certificat sur le serveur hébergeant la routine webhook. Le protocole HTTPS est utilisé par ONTAP pour vérifier l'identité du serveur d'application webhook ainsi que par les deux parties pour assurer la confidentialité et l'intégrité du trafic réseau. Voir "Configurez une destination Webhook pour utiliser HTTPS" pour en savoir plus sur la configuration.

HTTPS avec authentification mutuelle

Vous pouvez améliorer encore la sécurité HTTPS en installant un certificat client sur le système ONTAP émettant les requêtes webbook. En plus de la vérification par ONTAP de l'identité du serveur d'applications webhook et de la protection du trafic réseau, l'application webhook vérifie l'identité du client ONTAP. Cette authentification bidirectionnelle par poste est appelée *Mutual TLS*. Voir "Configurez une destination de connexion Web pour utiliser HTTPS avec authentification mutuelle" pour en savoir plus sur la configuration.

Informations associées

- "Protocole TLS (transport Layer Security) version 1.3"

Configurez une destination de connexion Web pour utiliser HTTP

Vous pouvez configurer ONTAP pour transférer des notifications d'événements vers une application de webhook à l'aide de HTTP. Il s'agit de l'option la moins sécurisée, mais la plus simple à configurer.

Étapes

1. Créer une nouvelle destination `restapi-ems` pour recevoir les événements :

   ```
   event notification destination create -name restapi-ems -rest-api-url
   http://<webhook-application>
   ```

   Dans la commande ci-dessus, vous devez utiliser le schéma **HTTP** pour la destination.

2. Créez une notification reliant le `important-events` filtrer avec le `restapi-ems` destination :

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Configurez une destination Webhook pour utiliser HTTPS

Vous pouvez configurer ONTAP pour transférer les notifications d'événements vers une application de connexion Internet à l'aide de HTTPS. ONTAP utilise le certificat de serveur pour confirmer l'identité de l'application webhook et sécuriser le trafic réseau.

Avant de commencer

- Générez une clé privée et un certificat pour le serveur d'applications webhook

- Disponibilité du certificat racine pour l'installation dans ONTAP

Étapes

1. Installez la clé privée du serveur et les certificats appropriés sur le serveur hébergeant votre application webhook. Les étapes de configuration spécifiques dépendent du serveur.
2. Installez le certificat racine du serveur dans ONTAP :

   ```
   security certificate install -type server-ca
   ```

   La commande demande le certificat.

3. Créer le `restapi-ems` destination pour recevoir les événements :

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application>
   ```

   Dans la commande ci-dessus, vous devez utiliser le schéma **HTTPS** pour la destination.

4. Créez la notification qui lie le `important-events` filtrer avec le nouveau `restapi-ems` destination :

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Configurez une destination de connexion Web pour utiliser HTTPS avec authentification mutuelle

Vous pouvez configurer ONTAP pour transférer les notifications d'événements vers une application webhook en utilisant HTTPS avec authentification mutuelle. Avec cette configuration, il y a deux certificats. ONTAP utilise le certificat de serveur pour confirmer l'identité de l'application webhook et sécuriser le trafic réseau. De plus, l'application hébergeant le webhook utilise le certificat client pour confirmer l'identité du client ONTAP.

Avant de commencer

Vous devez effectuer les opérations suivantes avant de configurer ONTAP :

- Générez une clé privée et un certificat pour le serveur d'applications webhook
- Disponibilité du certificat racine pour l'installation dans ONTAP
- Générez une clé privée et un certificat pour le client ONTAP

Étapes

1. Effectuez les deux premières étapes de la tâche "Configurez une destination Webhook pour utiliser HTTPS" Pour installer le certificat de serveur afin que ONTAP puisse vérifier l'identité du serveur.
2. Installez les certificats racine et intermédiaire appropriés sur l'application webhook pour valider le certificat client.
3. Installez le certificat client dans ONTAP :

   ```
   security certificate install -type client
   ```

   La commande demande la clé privée et le certificat.

4. Créer le `restapi-ems` destination pour recevoir les événements :

   ```
   event notification destination create -name restapi-ems -rest-api-url
   ```

```
https://<webhook-application> -certificate-authority <issuer of the client
certificate> -certificate-serial <serial of the client certificate>
```

Dans la commande ci-dessus, vous devez utiliser le schéma **HTTPS** pour la destination.

5. Créez la notification qui lie le `important-events` filtrer avec le nouveau `restapi-ems` destination :

```
event notification create -filter-name important-events -destinations restapi-
ems
```

Mettre à jour le mappage d'événements EMS obsolète

Modèles de mappage d'événements EMS

Avant ONTAP 9.0, les événements EMS ne pouvaient être mappés qu'à des destinations d'événement en fonction de la correspondance du modèle de nom d'événement. La commande ONTAP définit (`event destination`, `event route`) Qui utilisent ce modèle continue d'être disponible dans les dernières versions de ONTAP, mais ils ont été obsolètes à partir de ONTAP 9.0.

Depuis ONTAP 9.0, la meilleure pratique pour le mappage de destination d'événements EMS ONTAP consiste à utiliser le modèle de filtre d'événements plus évolutif dans lequel la correspondance de modèles est effectuée sur plusieurs champs, à l'aide du `event filter`, `event notification`, et `event notification destination` jeux de commandes.

Si votre mappage EMS est configuré à l'aide des commandes obsolètes, vous devez mettre à jour votre mappage pour utiliser le `event filter`, `event notification`, et `event notification destination` jeux de commandes.

Il existe deux types de destinations d'événements :

1. **Destinations générées par le système** : il existe cinq destinations d'événements générées par le système (créées par défaut)
   - `allevents`
   - `asup`
   - `criticals`
   - `pager`
   - `traphost`

     Certaines des destinations générées par le système sont à des fins spéciales. Par exemple, la destination d'asup achemine les événements callhome.* vers le module AutoSupport dans ONTAP pour générer des messages AutoSupport.
2. **Destinations créées par l'utilisateur** : elles sont créées manuellement à l'aide de `event destination create` commande.

```
cluster-1::event*> destination show
                                                                    Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
traphost          -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
test              test@xyz.com      -                  -
false
traphost          -                 -                  -
false
6 entries were displayed.
```

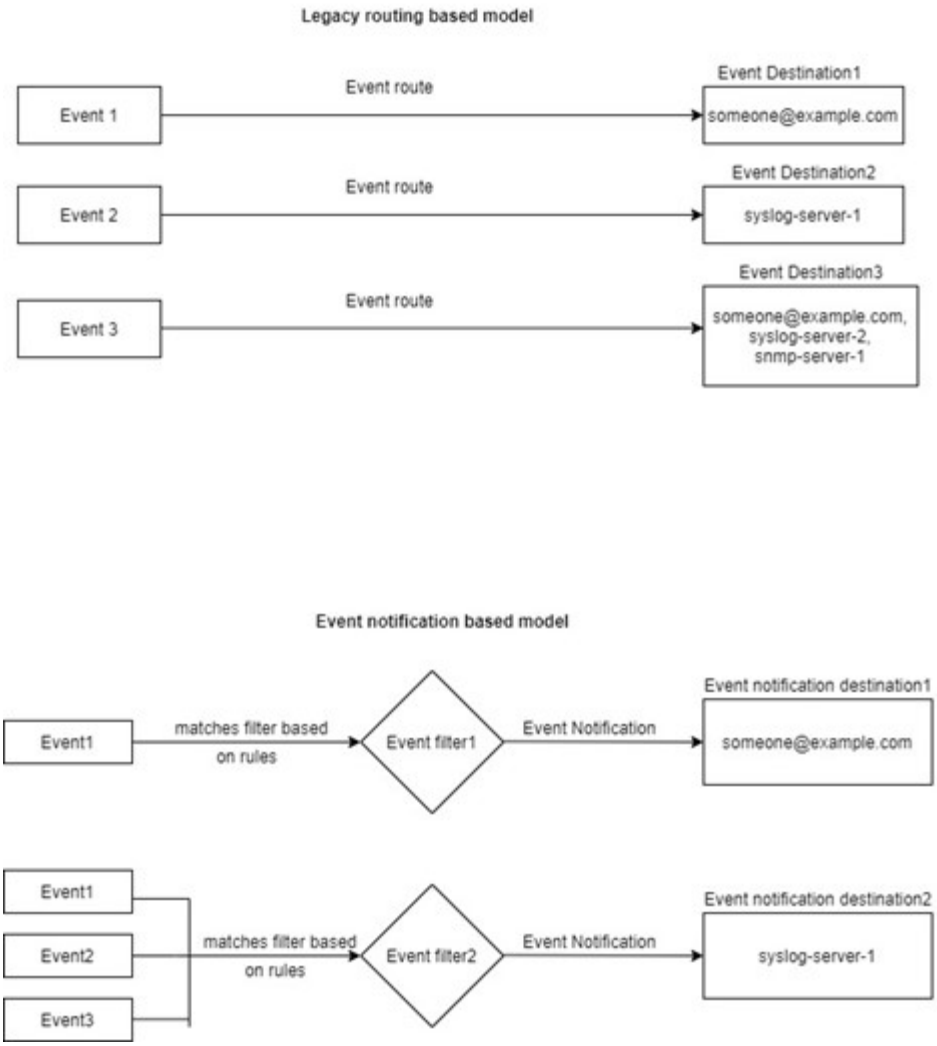
Dans le modèle obsolète, les événements EMS sont mappés individuellement vers une destination à l'aide de l'`event route add-destinations` commande.

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                                  Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

Le nouveau mécanisme plus évolutif de notification d'événements EMS est basé sur des filtres d'événements et des destinations de notification d'événements. Pour plus d'informations sur le nouveau mécanisme de notification d'événements, reportez-vous à l'article suivant de la base de connaissances :

- "Présentation du système de gestion des événements pour ONTAP 9"



Mettre à jour le mappage des événements EMS à partir des commandes ONTAP obsolètes

Si votre mappage d'événements EMS est actuellement configuré à l'aide des jeux de commandes ONTAP obsolètes (`event destination`, `event route`), vous devez suivre cette procédure pour mettre à jour votre mappage pour utiliser l' `event filter`, `event notification`, et `event notification destination` jeux de commandes.

Étapes

1. Répertorie toutes les destinations d'événements du système à l'aide du `event destination show` commande.

```
cluster-1::event*> destination show

Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

2. Pour chaque destination, répertoriez les événements qui lui sont mappés à l'aide de l' `event route show -destinations <destination name>` commande.

```
cluster-1::event*> route show -destinations test
                                                                  Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

3. Créer un correspondant `event filter` qui inclut tous ces sous-ensembles d'événements.
Par exemple, si vous souhaitez inclure uniquement le `raid.aggr.*` les événements, utilisez un caractère générique pour le `message-name` paramètre lors de la création du filtre. Vous pouvez également créer des filtres pour des événements uniques.

> Vous pouvez créer jusqu'à 50 filtres d'événements.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. Créez un `event notification destination` pour chacune des `event destination` Terminaux (SMTP/SNMP/syslog)

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name            Type        Destination
--------------  ----------  --------------------
dest1           email       test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost   snmp        - (from "system snmp traphost")
2 entries were displayed.
```

5. Créez une notification d'événement en mappant le filtre d'événement à la destination de notification d'événement.

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                    Destinations
---- ------------------------------ -----------------
1    default-trap-events            snmp-traphost
2    asup_events                    dest1
2 entries were displayed.
```

6. Répétez les étapes 1 à 1-5 pour chaque `event destination` cela a un `event route` mappage.

> Les événements routés vers des destinations SNMP doivent être mappés à l' `snmp-traphost` destination de la notification d'événement. La destination de Traphost SNMP utilise le Traphost configuré par le système.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

               Destination Name: snmp-traphost
             Type of Destination: snmp
                     Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```

Informations sur le copyright

Informations sur les marques commerciales