Administration et contrôle

ASA r2

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/asa-r2/administer/upgrade-ontap.html on February 11, 2026. Always check docs.netapp.com for the latest.

Sommaire

Administration et contrôle

Mettre à niveau et rétablir ONTAP

Mise à niveau de ONTAP sur les systèmes de stockage ASA r2

Lorsque vous mettez à niveau votre logiciel ONTAP sur votre système ASA r2, vous pouvez bénéficier des nouvelles fonctionnalités ONTAP améliorées pour réduire les coûts, accélérer les charges de travail stratégiques, améliorer la sécurité et étendre la portée de la protection des données disponible pour votre entreprise.

Les mises à niveau du logiciel ONTAP pour les systèmes ASA r2 suivent le même processus que pour les autres systèmes ONTAP. Si vous avez un contrat SupportEdge actif pour le conseiller numérique Active IQ (également appelé conseiller numérique), vous devez "Préparez la mise à niveau avec Upgrade Advisor". Upgrade Advisor fournit des informations intelligentes qui vous aident à minimiser l'incertitude et les risques en évaluant votre cluster et en créant un plan de mise à niveau propre à votre configuration. Si vous n'avez pas de contrat SupportEdge actif pour le conseiller numérique Active IQ, vous devez "Préparez la mise à niveau sans Upgrade Advisor".

Après avoir préparé votre mise à niveau, il est recommandé d'effectuer les mises à niveau à l'aide de "Mise à niveau automatisée sans interruption (ANDU) depuis System Manager". ANDU exploite la technologie de basculement haute disponibilité d'ONTAP pour assurer le service des données sans interruption lors de la mise à niveau.

En savoir plus sur "Mises à niveau du logiciel ONTAP".

Rétablir ONTAP sur les systèmes de stockage ASA r2

Les restaurations du logiciel ONTAP pour les systèmes ASA r2 suivent le même processus que les restaurations pour les autres systèmes ONTAP .

La restauration d'un cluster ONTAP est perturbatrice. Vous devez mettre le cluster hors ligne pendant toute la durée de la restauration. Vous ne devez pas restaurer un cluster de production sans l'aide du support technique. Vous pouvez restaurer un nouveau cluster ou un cluster de test sans assistance. Si la restauration d'un nouveau système ou d'un cluster de test échoue ou réussit, mais que vous n'êtes pas satisfait des performances du cluster dans votre environnement de production, contactez le support technique pour obtenir de l'aide.

"Rétablir un cluster ONTAP" .

Rétablir les exigences pour les systèmes ASA r2

Certaines configurations de cluster ASA r2 nécessitent que vous preniez des mesures spécifiques avant de commencer une restauration du logiciel ONTAP .

Retour à ONTAP 9.17.1

Si vous revenez à ONTAP 9.17.1 sur un système ASA r2, vous devez effectuer les actions suivantes avant de commencer la restauration :

"équilibrage dynamique de l'espace"est activé par défaut 14 jours après la mise à niveau vers ONTAP 9.17.1 ou l'initialisation d'un nouveau cluster ONTAP 9.17.1 ASA r2. Vous ne pouvez pas revenir à la version ONTAP 9.17.1 sur votre système ASA r2 après l'activation de l'équilibrage dynamique de l'espace.

Si vous avez…	Avant de revenir en arrière, vous devriez…
Groupes de cohérence hiérarchique dans une relation de synchronisation active SnapMirror	"Supprimer la relation de synchronisation active SnapMirror".
Relations d'importation actives	Supprimez les relations d'importation actives. "Découvrez les relations d'importation".
Protection anti-ransomware activée	"Suspendre la protection anti-ransomware".

Mise à jour du firmware sur les systèmes de stockage ASA r2

Par défaut, ONTAP télécharge et met à jour automatiquement les fichiers système et de micrologiciel sur votre système ASA r2. Si vous souhaitez avoir la possibilité d'afficher les mises à jour recommandées avant de les télécharger et de les installer, vous pouvez utiliser ONTAP System Manager pour désactiver les mises à jour automatiques ou pour modifier les paramètres de mise à jour afin d'afficher les notifications des mises à jour disponibles avant d'effectuer une action.

Activer les mises à jour automatiques

Les mises à jour recommandées pour le micrologiciel de stockage, le micrologiciel SP/BMC et les fichiers système sont automatiquement téléchargées et installées sur votre système ASA r2 par défaut. Si les mises à jour automatiques ont été désactivées, vous pouvez les activer pour rétablir le comportement par défaut.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Sous **Mises à jour logicielles**, sélectionnez **Activer**.
3. Lisez le CLUF.
4. Acceptez les paramètres par défaut pour **Afficher la notification** des mises à jour recommandées. Vous pouvez également choisir de **Mettre à jour automatiquement** ou de **Rejeter automatiquement** les mises à jour recommandées.
5. Sélectionnez cette option pour confirmer que vos modifications de mise à jour seront appliquées à toutes les mises à jour actuelles et futures.
6. Sélectionnez **Enregistrer**.

Résultat

Les mises à jour recommandées sont automatiquement téléchargées et installées sur votre système ASA r2 en fonction de vos sélections de mises à jour.

Désactiver les mises à jour automatiques

Désactivez les mises à jour automatiques uniquement si vous souhaitez gérer entièrement les mises à jour vous-même. Avec les mises à jour automatiques désactivées, le système ne vous notifiera pas, ne téléchargera pas et n'installera pas de mises à jour. Vous êtes responsable de surveiller, télécharger, planifier

et installer toutes les mises à jour manuellement.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Sous **Mises à jour logicielles**, sélectionnez **Désactiver**.

Résultat

Les mises à jour automatiques sont désactivées. Vous devez régulièrement vérifier les mises à jour recommandées et décider si vous souhaitez effectuer une installation manuelle.

Afficher les mises à jour automatiques

Afficher la liste des mises à jour de firmware et de fichiers système qui ont été téléchargées sur le cluster et dont l'installation automatique est prévue Affichez également les mises à jour qui ont été installées automatiquement au préalable.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. À côté de **Mises à jour logicielles**, sélectionnez → , puis sélectionnez **Afficher toutes les mises à jour automatiques**.

Modifier les mises à jour automatiques

Vous pouvez choisir de télécharger et d'installer automatiquement les mises à jour recommandées pour votre micrologiciel de stockage, votre micrologiciel SP/BMC et vos fichiers système sur votre cluster, ou de faire en sorte que les mises à jour recommandées soient automatiquement rejetées. Si vous souhaitez contrôler manuellement l'installation ou le rejet des mises à jour, sélectionnez pour être averti lorsqu'une mise à jour recommandée est disponible ; vous pouvez alors sélectionner manuellement l'installation ou le rejet.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. À côté de **Mises à jour logicielles**, sélectionnez → , puis sélectionnez **Toutes les autres mises à jour**.
3. Mettre à jour les sélections pour les mises à jour automatiques.
4. Sélectionnez **Enregistrer**.

Résultat

Les mises à jour automatiques sont modifiées en fonction de vos sélections.

Mettre à jour le micrologiciel manuellement

Si vous souhaitez pouvoir afficher les mises à jour recommandées avant de les télécharger et de les installer, vous pouvez désactiver les mises à jour automatiques et mettre à jour votre micrologiciel manuellement.

Étapes

1. Téléchargez votre fichier de mise à jour du micrologiciel sur un serveur ou un client local.
2. Dans le Gestionnaire système, sélectionnez **Cluster > Présentation**, puis sélectionnez **Toutes les autres mises à jour**.
3. Sous **Mises à jour manuelles**, sélectionnez **Ajouter des fichiers de micrologiciel** ; puis sélectionnez **Télécharger depuis le serveur** ou **Télécharger depuis le client local**.

4. Installez le fichier de mise à jour du firmware.

Résultat

Votre micrologiciel est mis à jour.

Gestion de l'accès client aux machines virtuelles de stockage sur les systèmes de stockage ASA r2

Les unités de stockage d'un système ASA r2 sont contenues dans des machines virtuelles de stockage. Les VM de stockage sont utilisées pour transmettre des données à vos clients SAN. Utilisez ONTAP System Manager pour créer une LIF (interface réseau) pour vos clients SAN afin de se connecter à une VM de stockage et d'accéder aux données des unités de stockage. Vous pouvez également utiliser des sous-réseaux pour simplifier la création de LIF et les IPspaces afin de fournir à vos VM de stockage leur propre stockage, administration et routage sécurisés.

Créez une machine virtuelle de stockage

Lors de la configuration des clusters, votre machine virtuelle de stockage de données par défaut est créée. Toutes les nouvelles unités de stockage sont créées à l'intérieur de votre VM de stockage de données par défaut, sauf si vous créez et sélectionnez une autre VM de stockage. Vous pouvez créer une VM de stockage supplémentaire pour séparer vos unités de stockage pour différentes applications, différents services ou clients. Par exemple, vous pouvez créer une VM de stockage pour votre environnement de développement et une autre VM de stockage pour votre environnement de production, ou bien créer une VM de stockage pour votre département financier et une autre VM de stockage pour votre département marketing.

Étapes

1. Sélectionnez **Cluster > VM de stockage**.
2. Sélectionnez + Add.
3. Entrez un nom pour la machine virtuelle de stockage ou acceptez le nom par défaut.
4. Sous **configurer les protocoles**, sélectionnez les protocoles pour la machine virtuelle de stockage.

   Sélectionnez **IP** pour iSCSI et NVMe/TCP. Sélectionnez **FC** pour Fibre Channel ou NVMe/FC.

5. Sous **Storage VM administration**, sélectionnez **Manage Administrator account**, puis entrez le nom d'utilisateur et le mot de passe du compte administrateur.
6. Ajouter une interface réseau pour la VM de stockage
7. Sélectionnez **Enregistrer**.

Et la suite ?

Vous avez créé une VM de stockage. Vous pouvez maintenant utiliser la machine virtuelle de stockage pour "provisionner le stockage".

Créez les IPspaces

Un IPspace est un espace d'adresse IP distinct dans lequel résident les VM de stockage. Lorsque vous créez des IPspaces, vos machines virtuelles de stockage peuvent disposer de leur propre stockage, administration et routage sécurisés. Vous activez également les clients dans des domaines réseau distincts d'un point de vue

administratif pour utiliser des adresses IP redondantes à partir de la même plage de sous-réseaux d'adresses IP.

Vous devez créer un IPspace avant de pouvoir créer un sous-réseau.

Étapes

1. Sélectionnez **réseau > vue d'ensemble**.
2. Sous **IPspaces**, sélectionnez + Add.
3. Entrez un nom pour l'IPspace ou acceptez le nom par défaut.

   Un nom IPspace ne peut pas être « All » car « All » est un nom réservé au système.

4. Sélectionnez **Enregistrer**.

Et la suite ?

Maintenant que vous avez créé un IPspace, vous pouvez l'utiliser pour créer un sous-réseau.

Créer des sous-réseaux

Un sous-réseau vous permet d'allouer des blocs spécifiques d'adresses IPv4 ou IPv6 à utiliser lors de la création d'une LIF (interface réseau) . Un sous-réseau simplifie la création de LIF en vous permettant de spécifier le nom de sous-réseau à la place d'une adresse IP et d'un masque réseau spécifiques pour chaque LIF.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- L'"broadcast-domain"IPspace et l'emplacement où vous prévoyez d'ajouter le sous-réseau doivent déjà exister.

Étapes

1. Sélectionnez **réseau > vue d'ensemble**.
2. Sélectionnez **sous-réseaux**, puis sélectionnez + Add.
3. Entrez le nom du sous-réseau.

   Tous les noms de sous-réseau doivent être uniques au sein d'un IPspace.

4. Entrez l'adresse IP du sous-réseau et le masque de sous-réseau.
5. Spécifiez la plage d'adresses IP du sous-réseau.

   Lorsque vous spécifiez la plage d'adresses IP du sous-réseau, ne faites pas chevaucher les adresses IP avec d'autres sous-réseaux. Des problèmes de réseau peuvent se produire lorsque les adresses IP de sous-réseau se chevauchent et que différents sous-réseaux ou hôtes tentent d'utiliser la même adresse IP.

6. Sélectionnez le domaine de diffusion du sous-réseau.
7. Sélectionnez **Ajouter**.

Et la suite ?

Vous avez créé un sous-réseau que vous pouvez utiliser pour simplifier la création de vos LIF.

Créer une LIF (interface réseau)

Une LIF (interface réseau) est une adresse IP associée à un port physique ou logique. Créez des LIF sur les ports que vous souhaitez utiliser pour accéder à des données. Les VM de stockage fournissent des données aux clients via une ou plusieurs LIF. En cas de défaillance d'un composant, une LIF peut basculer ou être migrée vers un autre port physique, afin que la communication réseau ne soit pas interrompue.

Sur un système ASA r2, vous pouvez créer des LIF IP, FC et NVMe/FC. Une LIF de données IP peut traiter le trafic iSCSI et NVMe/TCP par défaut. Des LIF de données distinctes doivent être créées pour le trafic FC et NVMe/FC.

Si vous souhaitez activer le basculement automatique de LIF iSCSI, vous devez créer une LIF IP pour le trafic iSCSI uniquement. Lorsque le basculement automatique de LIF iSCSI est activé, en cas de basculement du stockage, la LIF iSCSI IP est automatiquement migrée de son nœud ou port de rattachement vers son nœud ou port partenaire haute disponibilité, puis de nouveau une fois le basculement terminé. Ou, si le port d'une LIF iSCSI IP est défectueux, la LIF est automatiquement migrée vers un port sain de son nœud de rattachement actuel, puis revient sur son port d'origine une fois le port refonctionnel.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur le `up` statut administratif.
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, le sous-réseau doit déjà exister.
- Une LIF gérant le trafic intracluster entre des nœuds ne doit pas se trouver sur le même sous-réseau que le trafic de gestion d'une LIF ou encore le trafic de données géré par une LIF.

Étapes

1. Sélectionnez **réseau > vue d'ensemble**.
2. Sélectionnez **interfaces réseau**, puis sélectionnez + Add .
3. Sélectionnez le type et le protocole d'interface, puis la VM de stockage.
4. Entrez un nom pour la LIF ou acceptez le nom par défaut.
5. Sélectionnez le nœud de départ de l'interface réseau, puis entrez l'adresse IP et le masque de sous-réseau.
6. Sélectionnez **Enregistrer**.

Résultat

Vous avez créé une LIF pour l'accès aux données.

Et la suite ?

Vous pouvez utiliser l'interface de ligne de commande (CLI) ONTAP pour créer un LIF iSCSI uniquement avec basculement automatique.

Créer une stratégie de service LIF iSCSI uniquement personnalisée

Si vous souhaitez créer des LIF iSCSI uniquement avec basculement LIF automatique, vous devez d'abord créer une stratégie de service LIF iSCSI uniquement personnalisée.

Vous devez utiliser l'interface de ligne de commande (CLI) ONTAP pour créer la stratégie de service personnalisée.

Étape

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Créer une stratégie de service LIF iSCSI uniquement personnalisée :

```
network interface service-policy create -vserver <storage_VM_name>
-policy <service_policy_name> -services data-core,data-iscsi
```

3. Vérifiez que la politique de service a été créée :

```
network interface service-policy show -policy <service_policy_name>
```

4. Renvoyer le niveau de privilège à l'administrateur :

```
set -privilege admin
```

Créer des LIF uniquement iSCSI avec basculement automatique des LIF

Si des LIF iSCSI présentes sur la VM de stockage ne sont pas activées pour le basculement automatique des LIF, vos LIF nouvellement créées ne seront pas non plus activées pour le basculement automatique des LIF. Si le basculement automatique des LIF n'est pas activé et qu'un événement de basculement se produit, vos LIF iSCSI ne migreront pas.

Avant de commencer

Vous devez avoir créé une stratégie de service LIF iSCSI uniquement personnalisée.

Étapes

1. Créez des LIF uniquement iSCSI avec basculement automatique des LIF :

```
network interface create -vserver <storage_VM_name> -lif
<iscsi_lif_name> -service-policy <service_policy_name> -home-node
<home_node> -home-port <port_name> -address <ip_address> -netmask
<netmask> -failover-policy sfo-partner-only -status-admin up
```

   - Il est recommandé de créer deux LIF iSCSI sur chaque nœud, un pour la structure A et l'autre pour la structure B. Cela assure la redondance et l'équilibrage de charge de votre trafic iSCSI. Dans l'exemple suivant, quatre LIF iSCSI sont créés : deux sur chaque nœud et un pour chaque structure.

```
network interface create -vserver svm1 -lif iscsi-lif-01a -service
-policy custom-data-iscsi -home-node node1 -home-port e2b -address
<node01-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-01b -service
-policy custom-data-iscsi -home-node node1 -home-port e4b -address
<node01-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-02a -service
-policy custom-data-iscsi -home-node node2 -home-port e2b -address
<node02-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-02b -service
-policy custom-data-iscsi -home-node node2 -home-port e4b -address
<node02-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up
```

- Si vous utilisez des VLAN, ajustez le `home-port` paramètre pour inclure les informations de port VLAN pour la structure iSCSI respective, par exemple, `-home-port e2b-<iSCSI-A-VLAN>` pour la structure iSCSI A et `-home-port e4b-<iSCSI-B-VLAN>` .
- Si vous utilisez des groupes d'interfaces (ifgroups) avec des VLAN, ajustez le `home-port` paramètre pour inclure le port VLAN approprié, par exemple, `-home-port a0a-<iSCSI-A-VLAN>` pour la structure iSCSI A et `-home-port a0a-<iSCSI-B-VLAN>` pour la structure iSCSI B où `a0a` est le ifgroup et a0a-<iSCSI-A-VLAN> et a0a-<iSCSI-B-VLAN> sont les ports VLAN respectifs pour la structure iSCSI A et la structure iSCSI B.

2. Vérifiez que les LIF iSCSI ont été créés :

```
network interface show -lif iscsi*
```

Modification d'une LIF (interfaces réseau)

Les LIF peuvent être désactivées ou renommées selon les besoins. Vous pouvez également modifier l'adresse IP et le masque de sous-réseau de la LIF.

Description de la tâche

ONTAP utilise le protocole NTP (Network Time Protocol) pour synchroniser l'heure sur le cluster. Après avoir modifié les adresses IP LIF, vous devrez peut-être mettre à jour la configuration NTP pour éviter les échecs de synchronisation. Pour plus d'informations, reportez-vous à l'article de la base de connaissances"La synchronisation NTP échoue après le changement d'IP LIF" .

Étapes

1. Sélectionnez **réseau > Présentation**, puis **interfaces réseau**.

2. Passez le curseur sur l'interface réseau que vous souhaitez modifier, puis sélectionnez ⋮.
3. Sélectionnez **Modifier**.
4. Vous pouvez désactiver l'interface réseau, renommer l'interface réseau, modifier l'adresse IP ou modifier le masque de sous-réseau.
5. Sélectionnez **Enregistrer**.

Résultat

Votre LIF a été modifiée.

Gestion de la mise en réseau des clusters sur les systèmes de stockage ASA r2

Vous pouvez utiliser ONTAP System Manager pour administrer le réseau de stockage de base sur votre système ASA r2. Par exemple, vous pouvez ajouter un domaine de diffusion ou réaffecter des ports à un autre domaine de diffusion.

Ajouter un domaine de diffusion

Utilisez les domaines de diffusion pour simplifier la gestion de votre réseau de clusters en regroupant les ports réseau appartenant au même réseau de couche 2. Les machines virtuelles de stockage peuvent ensuite utiliser les ports du groupe pour le trafic de données ou de gestion.

Le broadcast domain « Default » et le broadcast « Cluster » sont créés lors du setup des cluster. Le broadcast domain « Default » contient les ports inclus dans l'IPspace « Default ». Ces ports servent principalement à transmettre des données. Les ports de management des clusters et de management des nœuds sont également présents dans ce broadcast domain. Le broadcast « Cluster » contient les ports situés dans le « Cluster » IPspace. Ces ports sont utilisés pour la communication de cluster et incluent tous les ports de cluster de tous les nœuds du cluster.

Vous pouvez créer d'autres domaines de diffusion après l'initialisation de votre cluster. Lorsque vous créez un broadcast domain, un failover group contenant les mêmes ports est automatiquement créé.

Description de la tâche

L'unité de transmission maximale (MTU) des ports ajoutés à un domaine de diffusion est mise à jour vers la valeur MTU définie dans le domaine de diffusion.

Étapes

1. Dans System Manager, sélectionnez **réseau > Présentation**.
2. Sous **domaines de diffusion**, sélectionnez + Add.
3. Entrez un nom pour le domaine de diffusion ou acceptez le nom par défaut.

   Tous les noms de domaine de diffusion doivent être uniques au sein d'un IPspace.

4. Sélectionnez l'IPspace pour le broadcast domain.

   Si vous ne spécifiez pas de nom IPspace, le broadcast domain est créé dans le « Default » IPspace.

5. Entrez l'unité de transmission maximale (MTU).

   MTU est le plus grand paquet de données qui peut être accepté dans votre domaine de diffusion.

6. Sélectionnez les ports souhaités, puis sélectionnez **Enregistrer**.

Résultat

Vous avez ajouté un nouveau domaine de diffusion.

Réaffectez des ports à un autre domaine de diffusion

Les ports ne peuvent appartenir qu'à un seul domaine de diffusion. Si vous souhaitez modifier le domaine de diffusion auquel appartient un port, vous devez réaffecter le port de son domaine de diffusion existant à un nouveau domaine de diffusion.

Étapes

1. Dans System Manager, sélectionnez **réseau > Présentation**.
2. Sous **Broadcast Domains**, sélectionnez ⋮ en regard du nom de domaine, puis sélectionnez **Edit**.
3. Désélectionnez les ports Ethernet que vous souhaitez réaffecter à un autre domaine.
4. Sélectionnez le domaine de diffusion auquel vous souhaitez réaffecter le port, puis sélectionnez **réaffecter**.
5. Sélectionnez **Enregistrer**.

Résultat

Vous avez réattribué des ports à un autre domaine de diffusion.

Créer un VLAN

Un VLAN est constitué de ports de commutateur regroupés dans un domaine de diffusion. Les VLAN vous permettent d'améliorer la sécurité, d'isoler les problèmes et de limiter les chemins disponibles au sein de votre infrastructure réseau IP.

Avant de commencer

Les commutateurs déployés sur le réseau doivent soit être conformes aux normes IEEE 802.1Q, soit disposer d'une implémentation spécifique au fournisseur de VLAN.

Description de la tâche

- Un VLAN ne peut pas être créé sur un port de groupe d'interfaces ne contenant aucun port membre.
- Lorsque vous configurez un VLAN sur un port pour la première fois, le port risque de tomber en panne, entraînant une déconnexion temporaire du réseau. Les ajouts de VLAN ultérieurs au même port n'affectent pas l'état du port.
- Vous ne devez pas créer de VLAN sur une interface réseau avec le même identifiant que le VLAN natif du commutateur. Par exemple, si l'interface réseau e0b est sur un VLAN 10 natif, vous ne devez pas créer de VLAN e0b-10 sur cette interface.

Étapes

1. Dans System Manager, sélectionnez **réseau > ports Ethernet**, puis sélectionnez + VLAN.
2. Sélectionnez le nœud et le domaine de diffusion pour le VLAN.
3. Sélectionnez le port du VLAN.

   Le VLAN ne peut pas être connecté à un port hébergeant une LIF de cluster ou à des ports assignés au cluster IPspace.

4. Entrez un ID de VLAN.

5. Sélectionnez **Enregistrer**.

Résultat

Vous avez créé un VLAN pour améliorer la sécurité, isoler les problèmes et limiter les chemins disponibles au sein de votre infrastructure réseau IP.

Surveillez l'utilisation et augmentez la capacité

Surveillance des performances du cluster et de l'unité de stockage sur les systèmes de stockage ASA r2

Utilisez ONTAP System Manager pour surveiller les performances globales de votre cluster et les performances de certaines unités de stockage afin de déterminer l'impact de la latence, des IOPS et du débit sur vos applications stratégiques. Les performances peuvent être surveillées sur plusieurs périodes allant d'une heure à un an.

Supposons par exemple qu'une application stratégique connaît une latence élevée et un faible débit. Lorsque vous consultez les performances du cluster au cours des cinq derniers jours ouvrables, vous remarquez une baisse des performances à la même heure chaque jour. Ces informations vous permettent de déterminer si l'application stratégique est en concurrence avec les ressources du cluster lorsqu'un processus non critique commence à s'exécuter en arrière-plan. Vous pouvez ensuite modifier votre règle de qualité de service pour limiter l'impact de la charge de travail non critique sur les ressources système et vous assurer que votre charge de travail stratégique respecte les objectifs de débit minimaux.

Contrôle des performances du cluster

Utilisez les metrics de performance du cluster pour déterminer si vous devez déplacer des charges de travail afin de minimiser la latence et d'optimiser les IOPS et le débit pour vos applications stratégiques.

Étapes

1. Dans System Manager, sélectionnez **Dashboard**.
2. Sous **Performance**, affichez la latence, les IOPS et le débit du cluster par heure, jour, semaine, mois ou année.
3. Sélectionnez  pour télécharger les données de performances.

Et la suite ?

Utilisez vos metrics de performance du cluster pour déterminer si vous devez modifier vos règles de qualité de service ou effectuer d'autres ajustements de vos charges de travail applicatives afin d'optimiser les performances globales de votre cluster.

Surveiller les performances de l'unité de stockage

Utilisez les metrics de performance de l'unité de stockage pour déterminer l'impact de certaines applications sur la latence, les IOPS et le débit.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Sélectionnez l'unité de stockage que vous souhaitez surveiller, puis sélectionnez **Présentation**.
3. Sous **Performance**, affichez la latence, les IOPS et le débit de l'unité de stockage par heure, jour,

semaine, mois ou année.

4. Sélectionnez pour télécharger les données de performances.

Et la suite ?

Utilisez les metrics de performance de votre unité de stockage pour déterminer si vous devez modifier les règles de QoS attribuées à vos unités de stockage afin de réduire la latence et d'optimiser les IOPS et le débit.

Surveillez l'utilisation du cluster et des unités de stockage sur les systèmes de stockage ASA r2

Utilisez ONTAP System Manager pour surveiller l'utilisation du stockage et vous assurer que vous disposez de la capacité de stockage nécessaire pour gérer vos charges de travail actuelles et futures.

Surveillance de l'utilisation du cluster

Surveillez régulièrement la quantité de stockage consommée par votre cluster afin de vous assurer que, si nécessaire, vous êtes prêt à étendre la capacité du cluster avant de manquer d'espace.

Étapes

1. Dans System Manager, sélectionnez **Dashboard**.
2. Sous **capacité**, affichez la quantité d'espace physique utilisé et la quantité d'espace disponible sur votre cluster.

   Le taux de réduction des données représente l'espace économisé grâce à l'efficacité du stockage.

Et la suite ?

Si l'espace de votre cluster est insuffisant ou s'il ne dispose pas de la capacité nécessaire pour répondre à un nouveau besoin, envisagez d'"ajouter de nouveaux lecteurs"augmenter votre capacité de stockage avec votre système ASA r2.

Surveiller l'utilisation de la zone de disponibilité du stockage

Chaque paire haute disponibilité d'un système ASA r2 utilise un pool de stockage commun appelé *zone de disponibilité du stockage*. La zone de disponibilité du stockage a accès à tous les disques disponibles dans le système de stockage et est visible pour les deux nœuds de la paire haute disponibilité.

Si votre cluster comporte 4 nœuds ou plus, vous pouvez afficher la quantité d'espace utilisée par la zone de disponibilité du stockage pour chaque paire haute disponibilité. Cette métrique n'est pas disponible pour les clusters à 2 nœuds.

Étapes

1. Dans System Manager, sélectionnez **Cluster**, puis **Présentation**.

   Un récapitulatif de l'utilisation de la zone de disponibilité du stockage s'affiche pour chaque paire HA dans le cluster.

2. Si vous souhaitez obtenir des mesures plus détaillées, sélectionnez une disponibilité spécifique du stockage.

   Sous **vue d'ensemble**, la capacité de la zone de disponibilité du stockage, la quantité d'espace utilisé et le

taux de réduction des données sont affichés.

Sous **unités de stockage**, une liste de toutes les unités de stockage de la zone de disponibilité de stockage s'affiche.

Et la suite ?

Si le niveau d'espace de votre zone de disponibilité du stockage est faible, envisagez "déplacer les unités de stockage"d'utiliser une autre zone de disponibilité du stockage pour équilibrer l'utilisation du stockage dans le cluster.

Surveiller l'utilisation de l'unité de stockage

Surveillez la quantité de stockage consommée par une unité de stockage afin d'augmenter de manière proactive la taille de l'unité de stockage en fonction des besoins de votre entreprise.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Sélectionnez l'unité de stockage que vous souhaitez surveiller, puis sélectionnez **Présentation**.
3. Sous **stockage**, affichez ce qui suit :
   - Taille de votre unité de stockage
   - Quantité d'espace utilisé
   - Ratio de réduction de données

     Le taux de réduction des données représente l'espace économisé grâce à l'efficacité du stockage
   - Snapshot utilisé

     Snapshot utilisé représente la quantité de stockage utilisée par les snapshots.

Et la suite ?

Si votre unité de stockage approche de "modifier l'unité de stockage"sa capacité, vous devez augmenter sa taille.

Augmentez la capacité de stockage sur les systèmes de stockage ASA r2

Ajoutez des disques à un nœud ou à un tiroir pour augmenter la capacité de stockage de votre système ASA r2.

Utilisez NetApp Hardware Universe pour préparer l'installation d'un nouveau lecteur

Avant d'installer un nouveau disque sur un nœud ou une étagère, utilisez NetApp Hardware Universe pour vérifier que le disque que vous souhaitez ajouter est pris en charge par votre système ASA r2 et pour identifier l'emplacement approprié pour le nouveau disque. Les emplacements appropriés pour l'ajout de disques varient en fonction du modèle du système et de la version ONTAP . Dans certains cas, il est nécessaire d'ajouter les disques à des emplacements spécifiques, dans l'ordre.

Étapes

1. Passez à "NetApp Hardware Universe"l' .
2. Sous **produits**, sélectionnez vos configurations matérielles.

3. Sélectionnez votre système ASA r2.
4. Sélectionnez votre version ONTAP, puis **Afficher les résultats**.
5. Sous le graphique, sélectionnez **cliquez ici pour voir d'autres vues**, puis choisissez la vue qui correspond à votre configuration.
6. Utilisez l'affichage de votre configuration pour vérifier que votre nouveau lecteur est pris en charge et que le logement approprié est installé.

Résultat

Vous avez confirmé que votre nouveau lecteur est pris en charge et que vous connaissez le logement approprié pour l'installation.

Installez un nouveau lecteur sur ASA r2

Le nombre minimum de disques que vous devez ajouter en une seule procédure est de six. L'ajout d'un disque unique peut réduire les performances.

Description de la tâche

Vous devez répéter les étapes de cette procédure pour chaque lecteur.

Étapes

1. Mettez-vous à la terre.
2. Retirez délicatement le cadre de la face avant du système.
3. Insérez le nouveau lecteur dans le logement approprié.
   a. Avec la poignée de came en position ouverte, utilisez les deux mains pour insérer le nouvel entraînement.
   b. Poussez jusqu'à ce que l'entraînement s'arrête.
   c. Fermez la poignée de came de façon à ce que le lecteur soit bien en place dans le plan médian et que la poignée s'enclenche.

      Assurez-vous de fermer lentement la poignée de came de manière à ce qu'elle s'aligne correctement sur la face de l'entraînement.

4. Vérifiez que le voyant d'activité du lecteur (vert) est allumé.
   - SI le voyant est fixe, le disque est sous tension.
   - Si le voyant clignote, le lecteur est sous tension et les E/S sont en cours. Le voyant clignote également si le micrologiciel du lecteur est en cours de mise à jour.

     Le firmware des disques est automatiquement mis à jour (sans interruption) sur les nouveaux lecteurs qui ne disposent pas de versions de micrologiciel actuelles.

5. Si votre nœud est configuré pour l'affectation automatique des disques, vous pouvez attendre que ONTAP attribue automatiquement les nouveaux disques à un nœud. Si votre nœud n'est pas configuré pour l'affectation automatique des disques ou si vous préférez, vous pouvez attribuer les disques manuellement.

   Les nouveaux disques ne sont pas reconnus tant qu'ils ne sont pas attribués à un nœud.

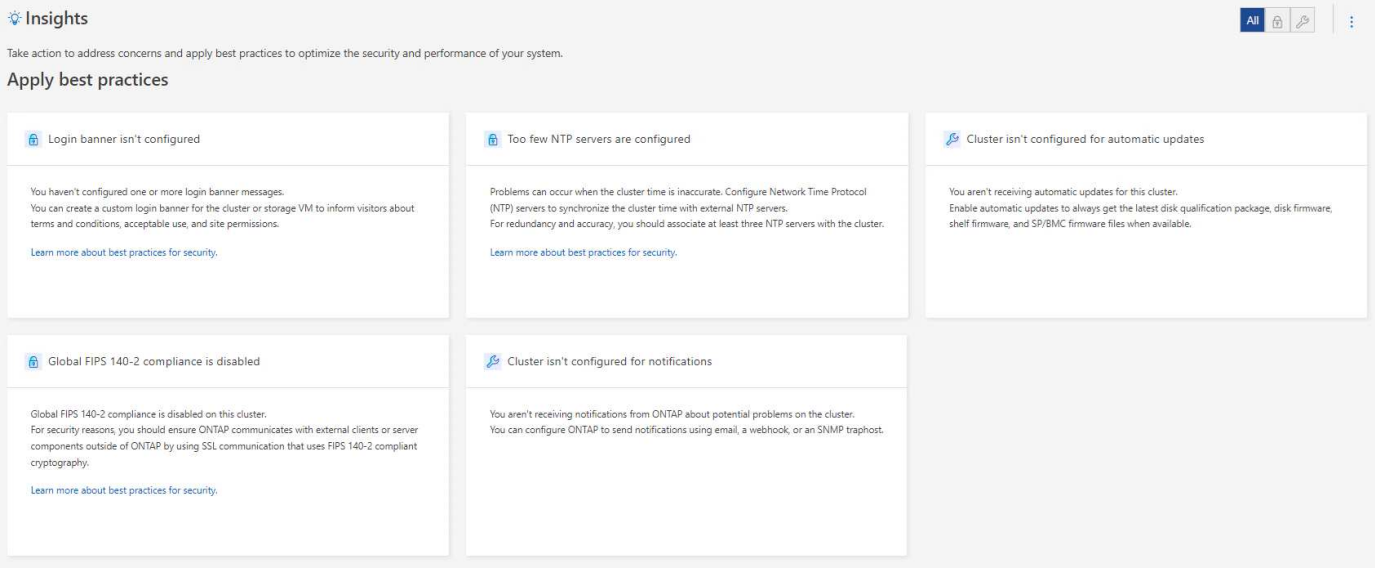
Et la suite ?

Une fois les nouveaux disques reconnus, vérifiez qu'ils ont été ajoutés et que leur propriété est correctement spécifiée.

Optimisez la sécurité et les performances du cluster grâce aux informations exploitables du système de stockage ASA r2

Consultez *Insights* dans ONTAP System Manager pour identifier les meilleures pratiques et les modifications de configuration que vous pouvez implémenter sur votre système ASA r2 afin d'optimiser la sécurité et les performances du cluster.

Par exemple, supposons que vos serveurs NTP (Network Time Protocol) soient configurés pour votre cluster. Cependant, vous ne savez pas que le nombre de serveurs NTP requis par la gestion optimale de l'heure du cluster est inférieur à celui recommandé. Pour vous aider à prévenir les problèmes susceptibles de se produire lorsque l'heure du cluster est inexacte, Insights vous informera que vous avez configuré trop peu de serveurs NTP et vous propose des options pour en savoir plus sur ce problème, le corriger ou le rejeter.



Étapes

1. Dans System Manager, sélectionnez **Insights**.
2. Examinez les recommandations.

Et la suite

Exécutez toutes les actions nécessaires pour mettre en œuvre les meilleures pratiques et optimiser la sécurité et les performances de votre cluster.

Affichage des tâches et événements de cluster sur les systèmes de stockage ASA r2

Utilisez ONTAP System Manager pour afficher la liste des erreurs ou alertes qui se sont produites dans votre système ainsi que les actions correctives recommandées. Vous pouvez également afficher les journaux d'audit du système et la liste des tâches actives, terminées ou ayant échoué.

Étapes

1. Dans System Manager, sélectionnez **Events & Jobs**.
2. Afficher les événements et les tâches du cluster

Pour afficher ceci…	Procédez comme ça…
Événements de cluster	Sélectionnez **Events**, puis **Event log**.
Suggestions Active IQ	Sélectionnez **événements**, puis **Active IQ suggestions**.
Alertes système	a. Sélectionnez **alertes système**. b. Sélectionnez l'alerte système pour laquelle vous souhaitez effectuer l'action. c. Accuser réception ou supprimer l'alerte.
Tâches de cluster	Sélectionnez **travaux**.
Journaux d'audit	Sélectionnez **journaux d'audit**.

Envoyez des notifications par e-mail pour les événements du cluster et les journaux d'audit

Configurez votre système pour qu'il envoie une notification à des adresses e-mail spécifiques en cas d'entrée de journal d'audit ou d'événement de cluster.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. En regard de **gestion des notifications**, sélectionnez ⋮.
3. Pour configurer une destination d'événement, sélectionnez **Afficher les destinations d'événement**, puis **destinations d'événement**. Pour configurer une destination de journal d'audit, sélectionnez **Afficher les destinations d'audit**, puis **destinations de journal d'audit**.
4. Sélectionnez + Add.
5. Entrez les informations de destination, puis sélectionnez **Ajouter**.

Résultat

L'adresse e-mail que vous avez ajoutée recevra à présent les notifications par e-mail spécifiées pour les événements du cluster et les journaux d'audit.

Gérer des nœuds

Ajoutez des nœuds ASA r2 à un cluster ONTAP

À partir d' ONTAP 9.16.1, les systèmes de stockage ASA r2 prennent en charge jusqu'à 12 nœuds par cluster. Une fois les nouveaux nœuds d'une paire HA câblés et mis sous tension, vous devez les joindre au cluster.

Avant de commencer

Rassemblez les informations suivantes :

- Adresse IP du nœud
- Adresse IP de l'interface réseau intercluster
- Le masque de sous-réseau intercluster
- La passerelle réseau intercluster
- Pour configurer le gestionnaire de clés intégré OKM, vous devez disposer de la phrase de passe OKM.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Présentation**.
2. Sélectionnez ⋮ en regard du nœud que vous souhaitez joindre au cluster, puis sélectionnez **Ajouter un nœud**
3. Entrez l'adresse IP de chaque nœud.
4. Indiquez l'adresse IP, le masque de sous-réseau et la passerelle de l'interface réseau intercluster.
5. Si vous souhaitez configurer le gestionnaire de clés intégré OKM, entrez la phrase de passe OKM.

   Configurer le gestionnaire de clés intégré pour le chiffrement est sélectionné par défaut.

6. Sélectionnez **Ajouter**.

Résultat

La nouvelle paire haute disponibilité est jointe au cluster.

Et la suite ?

Une fois que vous avez ajouté la nouvelle paire haute disponibilité au cluster, vous pouvez "Activez l'accès aux données à partir de vos hôtes SAN" accéder à vos nouveaux nœuds.

Redémarrez un nœud sur un système de stockage ASA r2

Vous devrez peut-être redémarrer un nœud pour effectuer des opérations de maintenance, de dépannage, de mise à jour logicielle ou d'autres tâches d'administration. Lorsqu'un nœud est redémarré, son partenaire haute disponibilité exécute automatiquement un basculement. Le nœud partenaire effectue ensuite un rétablissement automatique après la remise en ligne du nœud rebooté.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Présentation**.
2. Sélectionnez ⋮ en regard du nœud que vous souhaitez redémarrer, puis sélectionnez **redémarrer**.
3. Entrez la raison pour laquelle vous redémarrez le nœud, puis sélectionnez **redémarrer**.

   La raison pour laquelle vous entrez pour le redémarrage est enregistrée dans le journal d'audit du système.

Et la suite ?

Pendant le redémarrage du nœud, son partenaire haute disponibilité effectue un basculement afin qu'il n'y ait aucune interruption du service de données. Une fois le redémarrage terminé, le partenaire HA effectue un retour.

Renommez un nœud sur un système de stockage ASA r2

Vous pouvez utiliser ONTAP System Manager pour renommer un nœud sur votre système ASA r2. Vous devrez peut-être renommer un nœud pour l'aligner sur les conventions de nommage de votre entreprise ou pour d'autres raisons d'ordre administratif.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Présentation**.
2. Sélectionnez ⋮ en regard du nœud que vous souhaitez renommer, puis sélectionnez **Renommer**.
3. Entrez le nouveau nom du nœud, puis sélectionnez **Renommer**.

Résultat

Le nouveau nom est appliqué au nœud.

Gestion des comptes et des rôles utilisateur sur les systèmes de stockage ASA r2

Utilisez System Manager pour configurer l'accès au contrôleur de domaine Active Directory, l'authentification LDAP et SAML pour vos comptes d'utilisateurs. Créez des rôles de compte utilisateur pour définir des fonctions spécifiques que les utilisateurs affectés aux rôles peuvent exécuter sur votre cluster.

Configurer l'accès au contrôleur de domaine Active Directory

Configurez l'accès du contrôleur de domaine Active Directory (AD) à votre cluster ou à votre machine virtuelle de stockage afin de pouvoir activer l'accès au compte AD.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Dans la section **sécurité**, sous **Active Directory**, sélectionnez **configurer**.

Et la suite ?

Vous pouvez désormais activer l'accès au compte AD sur votre système ASA r2.

Configurer LDAP

Configurez un serveur LDAP (Lightweight Directory Access Protocol) pour gérer de manière centralisée les informations utilisateur à des fins d'authentification.

Avant de commencer

Vous devez avoir généré une demande de signature de certificat et ajouté un certificat numérique de serveur signé par l'autorité de certification.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Dans la section **sécurité**, en regard de **LDAP**, sélectionnez ⚙.

3. Entrez le serveur LDAP et les informations de liaison nécessaires, puis sélectionnez **Enregistrer**.

Et la suite ?

Vous pouvez désormais utiliser LDAP pour les informations utilisateur et l'authentification.

Configurez l'authentification SAML

L'authentification SAML (Security assertion Markup Language) permet aux utilisateurs d'être authentifiés par un fournisseur d'identité sécurisé (IDP) au lieu des fournisseurs de services directs tels qu'Active Directory et LDAP.

Avant de commencer

- Le IDP que vous envisagez d'utiliser pour l'authentification à distance doit être configuré.

  Pour plus d'informations sur la configuration, reportez-vous à la documentation IDP.

- Vous devez avoir l'URI du IDP.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Sous **sécurité**, en regard de **authentification SAML**, sélectionnez .
3. Sélectionnez **Activer l'authentification SAML**.
4. Entrez l'URL de l'IDP et l'adresse IP du système hôte, puis sélectionnez **Enregistrer**.

   Une fenêtre de confirmation affiche les informations sur les métadonnées, qui ont été automatiquement copiées dans le presse-papiers.

5. Accédez au système IDP que vous avez spécifié, puis copiez les métadonnées de votre presse-papiers pour mettre à jour les métadonnées du système.
6. Revenez à la fenêtre de confirmation dans System Manager, puis sélectionnez **J'ai configuré l'IDP avec l'URI hôte ou les métadonnées**.
7. Sélectionnez **Déconnexion** pour activer l'authentification basée sur SAML.

   Le système IDP affiche un écran d'authentification.

Et la suite ?

Vous pouvez désormais utiliser l'authentification SAML pour vos comptes d'utilisateurs.

Créer des rôles de compte d'utilisateur

Les rôles des administrateurs de cluster et des administrateurs des VM de stockage sont automatiquement créés lors de l'initialisation du cluster. Créez des rôles de compte d'utilisateur supplémentaires pour définir des fonctions spécifiques que les utilisateurs affectés aux rôles peuvent exécuter sur votre cluster.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Dans la section **sécurité**, en regard de **utilisateurs et rôles**, sélectionnez .
3. Sous **rôles**, sélectionnez + Add.
4. Sélectionnez les attributs de rôle.

Pour ajouter plusieurs attributs, sélectionnez + Add .

5. Sélectionnez **Enregistrer**.

Résultat

Un nouveau compte utilisateur est créé et peut être utilisé sur votre système ASA r2.

Créez un compte administrateur

Créez un compte utilisateur administrateur pour permettre à l'utilisateur du compte d'effectuer des actions spécifiques sur votre cluster en fonction du rôle attribué au compte. Pour améliorer la sécurité du compte, configurez l'authentification multifacteur (MFA) lorsque vous créez le compte.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Dans la section **sécurité**, en regard de **utilisateurs et rôles**, sélectionnez →.
3. Sous **utilisateurs**, sélectionnez + Add .
4. Entrez un nom d'utilisateur, puis sélectionnez un rôle à attribuer à l'utilisateur.
5. Sélectionnez la méthode de connexion utilisateur et la méthode d'authentification.
6. Pour activer MFA, sélectionnez + Add , puis sélectionnez une méthode de connexion secondaire et une méthode d'authentification
7. Saisissez un mot de passe pour l'utilisateur.
8. Sélectionnez **Enregistrer**.

Résultat

Un nouveau compte administrateur est créé et peut être utilisé sur votre cluster ASA r2.

Gestion des certificats de sécurité sur les systèmes de stockage ASA r2

Utilisez des certificats de sécurité numériques pour vérifier l'identité des serveurs distants.

Le protocole OCSP (Online Certificate Status Protocol) valide le statut des demandes de certificat numérique des services ONTAP à l'aide de connexions SSL et TLS (transport Layer Security).

Générer une demande de signature de certificat

Générez une requête de signature de certificat (CSR) pour créer une clé privée qui peut être utilisée pour générer un certificat public.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Sous **sécurité**, en regard de **certificats**, sélectionnez →; puis sélectionnez + Generate CSR.
3. Saisissez le nom commun du sujet, puis sélectionnez le pays.
4. Si vous souhaitez modifier les valeurs par défaut du GSR, sélectionnez utilisation de la touche étendue ou ajoutez des noms de substitution d'objet, sélectionnez ↙↗ More options; puis effectuez les mises à jour

souhaitées.

5. Sélectionnez **generate**.

Résultat

Vous avez généré une RSC à laquelle vous pouvez utiliser pour générer un certificat public.

Ajoutez une autorité de certification approuvée

ONTAP fournit un ensemble par défaut de certificats racine approuvés pour les applications utilisant TLS (transport Layer Security). Vous pouvez ajouter des autorités de certification approuvées supplémentaires si nécessaire.

Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Sous **sécurité**, en regard de **certificats**, sélectionnez →.
3. Sélectionnez **autorités de certification approuvées**.
4. Entrez ou importez les détails du certificat, puis sélectionnez + Add.

Résultat

Vous avez ajouté une nouvelle autorité de certification approuvée à votre système ASA r2.

Renouveler ou supprimer une autorité de certification approuvée

Les autorités de certification de confiance doivent être renouvelées chaque année. Si vous ne souhaitez pas renouveler un certificat expiré, vous devez le supprimer.

Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Sous **sécurité**, en regard de **certificats**, sélectionnez →.
3. Sélectionnez **autorités de certification approuvées**.
4. Sélectionnez l'autorité de certification de confiance que vous souhaitez renouveler ou supprimer.
5. Renouvelez ou supprimez l'autorité de certification.

Pour renouveler l'autorité de certification, procédez comme suit…	Pour supprimer l'autorité de certification, procédez comme suit…
a. Sélectionnez ⋮, puis **Renew**. b. Entrez ou importez les informations du certificat, puis sélectionnez **Renew**.	a. Sélectionnez ⋮, puis **Supprimer**. b. Confirmez que vous souhaitez supprimer, puis sélectionnez **Supprimer**.

Résultat

Vous avez renouvelé ou supprimé une autorité de certification approuvée existante sur votre système ASA r2.

Ajoutez un certificat client/serveur ou des autorités de certification locales

Ajoutez un certificat client/serveur ou des autorités de certification locales pour activer des services Web sécurisés.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Sous **sécurité**, en regard de **certificats**, sélectionnez →.
3. Sélectionnez **certificats client/serveur** ou **autorités de certification locales**.
4. Ajoutez les informations du certificat, puis sélectionnez + Add.

Résultat

Vous avez ajouté un nouveau certificat client/serveur ou des autorités locales à votre système ASA r2.

Renouvelez ou supprimez un certificat client/serveur ou des autorités de certification locales

Les certificats client/serveur et les autorités de certification locales doivent être renouvelés chaque année. Si vous ne souhaitez pas renouveler un certificat expiré ou les autorités de certification locales, vous devez les supprimer.

Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Sous **sécurité**, en regard de certificats, sélectionnez →.
3. Sélectionnez **certificats client/serveur** ou **autorités de certification locales**.
4. Sélectionnez le certificat que vous souhaitez renouveler ou supprimer.
5. Renouvelez ou supprimez l'autorité de certification.

Pour renouveler l'autorité de certification, procédez comme suit…	Pour supprimer l'autorité de certification, procédez comme suit…
a. Sélectionnez ⋮, puis **Renew**. b. Entrez ou importez les informations du certificat, puis sélectionnez **Renew**.	Sélectionnez ⋮, puis **Supprimer**.

Résultat

Vous avez renouvelé ou supprimé un certificat client/serveur existant ou une autorité de certification locale sur votre système ASA r2.

Vérifiez la connectivité hôte sur votre système de stockage ASA r2

En cas de problème avec les opérations de données hôte, vous pouvez utiliser ONTAP System Manager pour vérifier que la connexion entre l'hôte et le système de stockage ASA r2 est active.

Étapes

1. Dans System Manager, sélectionnez **Host**.

   L'état de la connectivité hôte est indiqué en regard du nom du groupe d'hôtes comme suit :

- **OK** : indique que tous les initiateurs sont connectés aux deux nœuds.
- **Partiellement connecté** : indique que certains des initiateurs ne sont pas connectés aux deux nœuds.
- **Aucun connecté** : indique qu'aucun initiateur n'est connecté.

Et la suite ?

Effectuez des mises à jour sur votre hôte pour corriger les problèmes de connectivité. ONTAP revérifie l'état de la connexion toutes les quinze minutes.

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.