Gérer les services Web

ONTAP 9

NetApp
February 13, 2026

Sommaire

Gérer les services Web

Présentation de la gestion des services Web

Vous pouvez activer ou désactiver un service Web pour le cluster ou une machine virtuelle de stockage (SVM), afficher les paramètres des services web et contrôler si les utilisateurs d'un rôle peuvent accéder à un service web.

Vous pouvez gérer les services web du cluster ou d'un SVM des manières suivantes :

- Activation ou désactivation d'un service Web spécifique
- Spécifier si l'accès à un service Web est limité à un seul HTTP crypté (SSL)
- Affichage de la disponibilité des services Web
- Autoriser ou interdire aux utilisateurs d'un rôle d'accéder à un service Web
- Affichage des rôles autorisés à accéder à un service Web

Pour qu'un utilisateur puisse accéder à un service Web, toutes les conditions suivantes doivent être remplies :

- L'utilisateur doit être authentifié.

  Par exemple, un service Web peut demander un nom d'utilisateur et un mot de passe. La réponse de l'utilisateur doit correspondre à un compte valide.

- L'utilisateur doit être configuré avec la méthode d'accès correcte.

  L'authentification ne réussit que pour les utilisateurs disposant de la méthode d'accès correcte pour le service Web donné. Pour le service Web de l'API ONTAP `ontapi`), les utilisateurs doivent avoir le `ontapi` méthode d'accès. Pour tous les autres services Web, les utilisateurs doivent avoir le `http` méthode d'accès.

  > Vous utilisez le `security login` commandes permettant de gérer les méthodes d'accès et d'authentification des utilisateurs.

- Le service Web doit être configuré pour permettre le rôle de contrôle d'accès de l'utilisateur.

  > Vous utilisez le `vserver services web access` commandes permettant de contrôler l'accès d'un rôle à un service web.

Si un pare-feu est activé, la politique de pare-feu de la LIF à utiliser pour les services Web doit être configurée de manière à autoriser HTTP ou HTTPS.

Si vous utilisez HTTPS pour l'accès aux services Web, SSL pour le cluster ou le SVM qui offre le service Web doit également être activé et vous devez fournir un certificat numérique pour le cluster ou SVM.

Gérer l'accès aux services Web ONTAP

Un service Web est une application que les utilisateurs peuvent accéder via HTTP ou HTTPS. L'administrateur du cluster peut configurer le moteur de protocole Web,

configurer SSL, activer un service Web et permettre aux utilisateurs d'un rôle d'accéder à un service Web.

Depuis ONTAP 9.6, les services Web suivants sont pris en charge :

- Infrastructure du processeur de service (`spi`)

  Ce service met à disposition les fichiers log, core dump et MIB des nœuds pour l'accès HTTP ou HTTPS via la LIF de cluster management ou une LIF de node-management. Le paramètre par défaut est `enabled`.

  Lors d'une demande d'accès aux fichiers journaux ou aux fichiers de vidage de mémoire d'un nœud, le `spi` Le service Web crée automatiquement un point de montage d'un nœud vers le volume racine d'un autre nœud où résident les fichiers. Il n'est pas nécessaire de créer manuellement le point de montage.

- Les API ONTAP (`ontapi`)

  Ce service vous permet d'exécuter des API ONTAP pour exécuter des fonctions administratives avec un programme distant. Le paramètre par défaut est `enabled`.

  Ce service peut être requis pour certains outils de gestion externes. Par exemple, si vous utilisez System Manager, vous devez laisser ce service activé.

- Détection Data ONTAP (`disco`)

  Ce service permet aux applications de gestion externes de découvrir le cluster sur le réseau. Le paramètre par défaut est `enabled`.

- Diagnostics du support (`supdiag`)

  Ce service contrôle l'accès à un environnement privilégié sur le système afin d'aider à l'analyse et à la résolution des problèmes. Le paramètre par défaut est `disabled`. Vous ne devez activer ce service que si vous y êtes invité par le support technique.

- System Manager (`sysmgr`)

  Ce service contrôle la disponibilité de System Manager, qui est inclus avec ONTAP. Le paramètre par défaut est `enabled`. Ce service est pris en charge uniquement sur le cluster.

- Mise à jour du contrôleur BMC (Baseboard Management Controller) du micrologiciel (`FW_BMC`)

  Ce service vous permet de télécharger les fichiers du micrologiciel BMC. Le paramètre par défaut est `enabled`.

- Documentation ONTAP (`docs`)

  Ce service fournit un accès à la documentation ONTAP. Le paramètre par défaut est `enabled`.

- API RESTful ONTAP (`docs_api`)

  Ce service permet d'accéder à la documentation de l'API RESTful ONTAP. Le paramètre par défaut est `enabled`.

- Téléchargement de fichiers (`fud`)

  Ce service permet le téléchargement et le téléchargement de fichiers. Le paramètre par défaut est `enabled`.

- Messagerie ONTAP (`ontapmsg`)

  Ce service prend en charge une interface de publication et d'abonnement qui vous permet de vous abonner à des événements. Le paramètre par défaut est `enabled`.

- Portail ONTAP (`portal`)

  Ce service implémente la passerelle dans un serveur virtuel. Le paramètre par défaut est `enabled`.

- Interface ONTAP RESTful (`rest`)

  Ce service prend en charge une interface RESTful qui permet de gérer à distance tous les éléments de l'infrastructure du cluster. Le paramètre par défaut est `enabled`.

- Prise en charge des fournisseurs de services SAML (`saml`)

  Ce service fournit des ressources pour prendre en charge le fournisseur de services SAML. Le paramètre par défaut est `enabled`.

- Fournisseur de services SAML (`saml-sp`)

  Ce service offre des services tels que les métadonnées SP et le service client d'assertion au fournisseur de services. Le paramètre par défaut est `enabled`.

Depuis ONTAP 9.7, les services supplémentaires suivants sont pris en charge :

- Fichiers de sauvegarde de configuration (`backups`)

  Ce service vous permet de télécharger les fichiers de sauvegarde de configuration. Le paramètre par défaut est `enabled`.

- Sécurité ONTAP (`security`)

  Ce service prend en charge la gestion des jetons CSRF pour une authentification améliorée. Le paramètre par défaut est `enabled`.

Gérer le moteur de protocole Web dans ONTAP

Vous pouvez configurer le moteur de protocole Web sur le cluster pour contrôler si l'accès Web est autorisé et quelles versions SSL peuvent être utilisées. Vous pouvez également afficher les paramètres de configuration du moteur de protocole Web.

Vous pouvez gérer le moteur de protocole Web au niveau du cluster de plusieurs manières :

- Vous pouvez indiquer si les clients distants peuvent utiliser HTTP ou HTTPS pour accéder au contenu du service Web à l'aide de l' `system services web modify` commande avec `-external` paramètre.

- Vous pouvez spécifier si SSLv3 doit être utilisé pour un accès Web sécurisé à l'aide de l' `security config modify` commande avec `-supported-protocol` paramètre.
  Par défaut, SSLv3 est désactivé. La sécurité de la couche de transport 1.0 (TLSv1) est activée et elle peut être désactivée si nécessaire.

  Pour en savoir plus, `security config modify` consultez le "Référence de commande ONTAP".

- Vous pouvez activer le mode de conformité Federal information Processing Standard (FIPS) 140-2 pour les interfaces de service Web du plan de contrôle à l'échelle du cluster.

  Par défaut, le mode de conformité FIPS 140-2 est désactivé.

  - **Lorsque le mode de conformité FIPS 140-2 est désactivé**
    Vous pouvez activer le mode de conformité FIPS 140-2 en configurant le `is-fips-enabled` paramètre à `true` pour le `security config modify` et en utilisant la commande `security config show` commande pour confirmer le statut en ligne.
  - **Lorsque le mode de conformité FIPS 140-2 est activé**
    - À partir de ONTAP 9.11.1, TLSv1, TLSv1.1 et SSLv3 sont désactivés et seuls TSLv1.2 et TSLv1.3 restent activés. Elle affecte d'autres systèmes et communications internes et externes à ONTAP 9. Si vous activez le mode de conformité FIPS 140-2 puis désactivez-le, TLSv1, TLSv1.1 et SSLv3 restent désactivés. TLSv1.2 ou TLSSS3.3 restent activés en fonction de la configuration précédente.
    - Pour les versions de ONTAP antérieures à 9.11.1, TLSv1 et SSLv3 sont tous deux désactivés et seuls les modèles TLSv1.1 et TLSv1.2 restent activés. ONTAP vous empêche d'activer à la fois TLSv1 et SSLv3 lorsque le mode de conformité FIPS 140-2 est activé. Si vous activez le mode de conformité FIPS 140-2 puis désactivez-le, TLSv1 et SSLv3 restent désactivés, mais TLSv1.2 ou les deux TLSv1.1 et TLSv1.2 sont activés en fonction de la configuration précédente.

- Vous pouvez afficher la configuration de la sécurité au niveau du cluster à l'aide de `system security config show` commande.

  Pour en savoir plus, `security config show` consultez le "Référence de commande ONTAP".

Si le pare-feu est activé, la politique de pare-feu pour l'interface logique (LIF) à utiliser pour les services Web doit être configurée de manière à autoriser l'accès HTTP ou HTTPS.

Si vous utilisez HTTPS pour l'accès aux services Web, SSL pour le cluster ou la machine virtuelle de stockage (SVM) qui offre le service Web doit également être activé, et vous devez fournir un certificat numérique pour le cluster ou la SVM.

Dans les configurations MetroCluster, les modifications de paramètre apportées au moteur de protocole Web sur un cluster ne sont pas répliquées sur le cluster partenaire.

Commandes ONTAP pour la gestion du moteur de protocole Web

Vous utilisez le `system services web` commandes permettant de gérer le moteur de protocole web. Vous utilisez le `system services firewall policy create` et `network interface modify` commandes permettant d'autoriser les demandes d'accès web à passer par le pare-feu.

Les fonctions que vous recherchez…	Utilisez cette commande…
Configurer le moteur de protocole Web au niveau du cluster : • Activez ou désactivez le moteur de protocole Web pour le cluster • Activez ou désactivez SSLv3 pour le cluster • Activer ou désactiver la conformité FIPS 140-2 pour des services web sécurisés (HTTPS)	`system services web modify`
Afficher la configuration du moteur de protocole Web au niveau du cluster, déterminer si les protocoles Web sont fonctionnels dans tout le cluster et indiquer si la conformité FIPS 140-2 est activée et en ligne	`system services web show`
Afficher la configuration du moteur de protocole Web au niveau du nœud et l'activité de gestion du service Web pour les nœuds du cluster	`system services web node show`
Créez une politique de pare-feu ou ajoutez un service de protocole HTTP ou HTTPS à une politique de pare-feu existante pour permettre aux demandes d'accès Web de passer par le pare-feu	`system services firewall policy create` Réglage du `-service` paramètre à `http` ou `https` permet aux demandes d'accès web de passer par le pare-feu.
Associer une politique de pare-feu à une LIF	`network interface modify` Vous pouvez utiliser le `-firewall-policy` Paramètre pour modifier la politique de pare-feu d'une LIF.

Informations associées

- "modification de l'interface réseau"

Configurer l'accès aux services Web ONTAP

La configuration de l'accès aux services Web permet aux utilisateurs autorisés d'utiliser HTTP ou HTTPS pour accéder au contenu du service sur le cluster ou sur un SVM (Storage Virtual machine).

Étapes

1. Si un pare-feu est activé, assurez-vous que l'accès HTTP ou HTTPS est configuré dans la politique de pare-feu pour la LIF qui sera utilisée pour les services Web :

   Vous pouvez vérifier si un pare-feu est activé à l'aide du `system services firewall show` commande.

a. Pour vérifier que HTTP ou HTTPS est configuré dans la stratégie de pare-feu, utilisez le `system services firewall policy show` commande.

   Vous définissez le `-service` paramètre du `system services firewall policy create` commande à `http` ou `https` pour activer la stratégie de prise en charge de l'accès web.

b. Pour vérifier que la politique de pare-feu prenant en charge HTTP ou HTTPS est associée au LIF qui fournit des services Web, utilisez le `network interface show` commande avec `-firewall -policy` paramètre.

   Pour en savoir plus, `network interface show` consultez le "Référence de commande ONTAP".

   Vous utilisez le `network interface modify` commande avec `-firewall-policy` Paramètre pour mettre la politique de pare-feu en vigueur pour une LIF.

Pour en savoir plus, `network interface modify` consultez le "Référence de commande ONTAP".

2. Pour configurer le moteur de protocole Web au niveau du cluster et rendre le contenu du service Web accessible, utilisez le `system services web modify` commande.
3. Si vous prévoyez d'utiliser des services Web sécurisés (HTTPS), activez SSL et fournissez les informations de certificat numérique pour le cluster ou la SVM à l'aide du `security ssl modify` commande.

   Pour en savoir plus, `security ssl modify` consultez le "Référence de commande ONTAP".

4. Pour activer un service Web pour le cluster ou un SVM, utilisez le `vserver services web modify` commande.

   Vous devez répéter cette étape pour chaque service que vous souhaitez activer pour le cluster ou la SVM.

5. Pour autoriser un rôle permettant d'accéder aux services web sur le cluster ou SVM, utilisez la `vserver services web access create` commande.

   Le rôle auquel vous accordez l'accès doit déjà exister. Vous pouvez afficher les rôles existants à l'aide de la `security login role show` commande ou création de nouveaux rôles à l'aide de la commande `security login role create` commande.

   Pour en savoir plus sur `security login role show` et `security login role create` dans le "Référence de commande ONTAP".

6. Pour un rôle autorisé à accéder à un service Web, assurez-vous que ses utilisateurs sont également configurés avec la méthode d'accès correcte en vérifiant la sortie du `security login show` commande.

   Pour accéder au service Web de l'API ONTAP `ontapi`), un utilisateur doit être configuré avec le `ontapi` méthode d'accès. Pour accéder à tous les autres services Web, un utilisateur doit être configuré avec le `http` méthode d'accès.

   Pour en savoir plus, `security login show` consultez le "Référence de commande ONTAP".

> Vous utilisez `security login create` la commande pour ajouter une méthode d'accès à un utilisateur. Pour en savoir plus, `security login create` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des services Web

Vous utilisez le `vserver services web` Commandes permettant de gérer la disponibilité des services web pour le cluster ou une machine virtuelle de stockage (SVM). Vous utilisez le `vserver services web access` commandes permettant de contrôler l'accès d'un rôle à un service web.

Les fonctions que vous recherchez…	Utilisez cette commande…
Configurer un service web pour le cluster ou anSVM : • Activer ou désactiver un service Web • Spécifiez si seul HTTPS peut être utilisé pour accéder à un service Web	`vserver services web modify`
Afficher la configuration et la disponibilité des services web pour le cluster ou anSVM	`vserver services web show`
Autoriser un rôle à accéder à un service web sur le cluster ou anSVM	`vserver services web access create`
Afficher les rôles autorisés pour accéder aux services web sur le cluster ou anSVM	`vserver services web access show`
Empêcher un rôle d'accéder à un service Web sur le cluster ou anSVM	`vserver services web access delete`

Informations associées

"Référence de commande ONTAP"

Commandes de gestion des points de montage sur les nœuds ONTAP

Le `spi` le service web crée automatiquement un point de montage d'un nœud vers le volume racine d'un autre nœud lors d'une demande d'accès aux fichiers journaux ou fichiers « core » du nœud. Bien que vous n'ayez pas besoin de gérer manuellement les points de montage, vous pouvez le faire en utilisant le `system node root-mount` commandes.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer manuellement un point de montage d'un nœud vers le volume racine d'un autre nœud	`system node root-mount create` Un seul point de montage peut exister d'un nœud à un autre.

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche les points de montage existants sur les nœuds du cluster, y compris le moment où un point de montage a été créé et son état actuel	`system node root-mount show`
Supprimez un point de montage d'un nœud vers le volume racine d'un autre nœud et force les connexions vers le point de montage à fermer	`system node root-mount delete`

Informations associées

"Référence de commande ONTAP"

Gérer SSL dans ONTAP

Utilisez le `security ssl` Commandes permettant de gérer le protocole SSL pour le cluster ou une machine virtuelle de stockage (SVM). Le protocole SSL améliore la sécurité de l'accès au Web en utilisant un certificat numérique pour établir une connexion chiffrée entre un serveur Web et un navigateur.

Vous pouvez gérer SSL pour le cluster ou une machine virtuelle de stockage (SVM) de la manière suivante :

- Activation de SSL
- Génération et installation d'un certificat numérique et son association au cluster ou à la SVM
- Affichage de la configuration SSL pour voir si SSL a été activé et, le cas échéant, le nom du certificat SSL
- Configuration de politiques de pare-feu pour le cluster ou SVM, de sorte que les demandes d'accès Web puissent passer par
- Définition des versions SSL pouvant être utilisées
- Limiter l'accès aux requêtes HTTPS uniquement pour un service Web

Commandes pour la gestion de SSL

Vous utilisez le `security ssl` Commandes permettant de gérer le protocole SSL pour le cluster ou une machine virtuelle de stockage (SVM).

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez le protocole SSL pour le cluster ou un SVM et associez un certificat numérique à celui-ci	`security ssl modify`
Afficher la configuration SSL et le nom du certificat pour le cluster ou un SVM	`security ssl show`

Pour en savoir plus sur `security ssl modify` et `security ssl show` dans le "Référence de commande ONTAP".

Utiliser HSTS pour les services Web ONTAP

HTTP Strict Transport Security (HSTS) est un mécanisme de sécurité web qui protège les sites web contre les attaques de type « man-in-the-middle », telles que les attaques par rétrogradation de protocole et le détournement de cookies. En imposant l'utilisation du protocole HTTPS, HSTS garantit le chiffrement de toutes les communications entre le navigateur de l'utilisateur et le serveur. Depuis ONTAP 9.17.1, ONTAP peut imposer les connexions HTTPS pour les services web ONTAP .

> Le protocole HSTS est appliqué par le navigateur web uniquement après l'établissement d'une connexion HTTPS sécurisée initiale avec ONTAP. Si le navigateur n'établit pas de connexion sécurisée initiale, le protocole HSTS ne sera pas appliqué. Consultez la documentation de votre navigateur pour plus d'informations sur la gestion du protocole HSTS.

Description de la tâche

- À partir de la version 9.17.1, HSTS est activé par défaut pour les clusters ONTAP nouvellement installés. Lors de la mise à niveau vers la version 9.17.1, HSTS n'est pas activé par défaut. Vous devez l'activer après la mise à niveau.
- HSTS est pris en charge pour tous "Services Web ONTAP" .

Avant de commencer

- Des privilèges avancés sont requis pour les tâches suivantes.

Afficher la configuration HSTS

Vous pouvez afficher la configuration HSTS actuelle pour vérifier si elle est activée et afficher le paramètre d'âge maximum.

Étapes

1. Utilisez le `system services web show` commande pour afficher la configuration actuelle des services Web, y compris les paramètres HSTS :

```
cluster-1::system services web*> show

                   External Web Services: true
                               HTTP Port: 80
                              HTTPS Port: 443
                         Protocol Status: online
                     Per Address Limit: 80
                    Wait Queue Capacity: 192
                           HTTP Enabled: true
                 CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                           HSTS Enabled: true
                  HSTS max age (Seconds): 63072000
```

Activer HSTS et définir l'âge maximum

À partir d' ONTAP 9.17.1, HSTS est activé par défaut sur le nouveau cluster ONTAP . Si vous mettez à niveau un cluster existant vers la version 9.17.1 ou ultérieure, vous devez activer manuellement HSTS pour imposer l'utilisation du protocole HTTPS. Vous pouvez activer HSTS et définir l'âge maximal. Vous pouvez modifier cet âge maximal à tout moment si HSTS est activé. Une fois HSTS activé, les navigateurs commenceront à appliquer les connexions sécurisées uniquement après l'établissement d'une connexion sécurisée initiale.

Étapes

1. Utilisez le `system services web modify` commande pour activer HSTS ou modifier l'âge maximum :

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age` Spécifie la durée en secondes pendant laquelle le navigateur doit se souvenir d'appliquer le protocole HTTPS. La valeur par défaut est de 63 072 000 secondes (deux ans).

Désactiver HSTS

Les navigateurs enregistrent le paramètre d'âge maximal HSTS à chaque connexion et continuent d'appliquer HSTS pendant toute la durée de la connexion, même si HSTS est désactivé sur ONTAP. Après sa désactivation, le navigateur peut mettre jusqu'à la durée maximale configurée pour arrêter d'appliquer HSTS. Si une connexion sécurisée devient impossible pendant ce temps, les navigateurs appliquant HSTS n'autoriseront pas l'accès aux services web ONTAP jusqu'à la résolution du problème ou l'expiration de l'âge maximal du navigateur.

Étapes

1. Désactiver HSTS à l'aide du `system services web modify` commande:

```
system services web modify -hsts-enabled false
```

Informations associées

"RFC 6797 - Sécurité de transport HTTP stricte (HSTS)"

Résoudre les problèmes d'accès au service Web ONTAP

Des erreurs de configuration provoquent des problèmes d'accès au service Web. Vous pouvez corriger les erreurs en vous assurant que la LIF, la politique de pare-feu, le moteur de protocole Web, les services Web, les certificats numériques, et l'autorisation d'accès utilisateur sont toutes correctement configurées.

Le tableau suivant vous aide à identifier et à résoudre les erreurs de configuration du service Web :

Ce problème d'accès…	Se produit en raison de cette erreur de configuration…	Pour résoudre l'erreur…
Votre navigateur Web renvoie un `unable to connect` ou `failure to establish a connection` erreur lorsque vous essayez d'accéder à un service web.	Votre LIF n'est peut-être pas configurée correctement.	Assurez-vous de pouvoir envoyer une requête ping à la LIF qui fournit le service Web. Vous utilisez `network ping` la commande pour envoyer une requête ping à une LIF.
Votre pare-feu est peut-être configuré de manière incorrecte.	Assurez-vous qu'une politique de pare-feu est configurée pour prendre en charge HTTP ou HTTPS et que la politique est attribuée à la LIF qui fournit le service Web. Vous utilisez le `system services firewall policy` commandes permettant de gérer les politiques de pare-feu. Vous utilisez le `network interface modify` commande avec `-firewall-policy` Paramètre pour associer une policy à une LIF.	Votre moteur de protocole Web peut être désactivé.

Ce problème d'accès…	Se produit en raison de cette erreur de configuration…	Pour résoudre l'erreur…
Assurez-vous que le moteur de protocole Web est activé pour que les services Web soient accessibles. Vous utilisez le `system services web` commandes permettant de gérer le moteur de protocole web pour le cluster.	Votre navigateur Web renvoie un `not found` erreur lorsque vous essayez d'accéder à un service web.	Le service Web est peut-être désactivé.
Assurez-vous que chaque service Web auquel vous souhaitez autoriser l'accès est activé individuellement. Vous utilisez le `vserver services web modify` commande permettant d'activer un service web pour l'accès.	Le navigateur Web ne parvient pas à se connecter à un service Web avec le nom de compte et le mot de passe d'un utilisateur.	L'utilisateur ne peut pas être authentifié, la méthode d'accès n'est pas correcte ou l'utilisateur n'est pas autorisé à accéder au service Web.

Ce problème d'accès…	Se produit en raison de cette erreur de configuration…	Pour résoudre l'erreur…
Assurez-vous que le compte utilisateur existe et est configuré avec la méthode d'accès et la méthode d'authentification appropriées. Assurez-vous également que le rôle de l'utilisateur est autorisé à accéder au service Web. Vous utilisez le `security login` commandes permettant de gérer les comptes utilisateurs, leurs méthodes d'accès et leurs méthodes d'authentification. Pour accéder au service Web de l'API ONTAP, vous devez utiliser le `ontapi` méthode d'accès. L'accès à tous les autres services Web nécessite le `http` méthode d'accès. Vous utilisez le `vserver services web access` commandes permettant de gérer l'accès d'un rôle à un service web.	Vous vous connectez à votre service Web via HTTPS et votre navigateur Web indique que votre connexion est interrompue.	Il se peut que vous n'ayez pas activé SSL sur le cluster ou la machine virtuelle de stockage (SVM) qui fournit le service Web.

Ce problème d'accès…	Se produit en raison de cette erreur de configuration…	Pour résoudre l'erreur…
S'assurer que le cluster ou le SVM a activé SSL et que le certificat numérique est valide. Vous utilisez le `security ssl` Commandes permettant de gérer la configuration SSL des serveurs HTTP et du `security certificate show` commande permettant d'afficher les informations relatives au certificat numérique.	Vous vous connectez à votre service Web via HTTPS et votre navigateur Web indique que la connexion n'est pas fiable.	Vous utilisez peut-être un certificat numérique auto-signé.

Informations associées

- "Quelles sont les meilleures pratiques de configuration réseau pour ONTAP?"
- "ping réseau"
- "modification de l'interface réseau"
- "certificat de sécurité générer-csr"
- "installation du certificat de sécurité"
- "certificat de sécurité afficher"
- "sécurité SSL"