



Authentification et contrôle d'accès

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/concept_authentication_access_control_overview.html on April 24, 2024. Always check docs.netapp.com for the latest.

Sommaire

- Authentification et contrôle d'accès 1
 - Présentation de l'authentification et du contrôle d'accès 1
 - Gestion de l'authentification administrateur et du RBAC 1
- Authentification et autorisation via OAuth 2.0 86
- Configurez l'authentification SAML 108
- Gérer les services Web 115
- Vérifiez l'identité des serveurs distants à l'aide de certificats 126
- Authentifier mutuellement le cluster et un serveur KMIP 129

Authentification et contrôle d'accès

Présentation de l'authentification et du contrôle d'accès

Vous pouvez gérer l'authentification de cluster ONTAP et le contrôle d'accès aux services Web ONTAP.

À l'aide de System Manager ou de l'interface de ligne de commandes, vous pouvez contrôler et sécuriser l'accès des clients et des administrateurs au cluster et au stockage.

Si vous utilisez System Manager classique (disponible uniquement dans ONTAP 9.7 et versions antérieures), reportez-vous à ["System Manager Classic \(ONTAP 9.0 à 9.7\)"](#)

Authentification et autorisation du client

ONTAP authentifie un ordinateur client et un utilisateur en vérifiant son identité avec une source de confiance. ONTAP autorise un utilisateur à accéder à un fichier ou à un répertoire en comparant les informations d'identification de l'utilisateur aux autorisations configurées sur le fichier ou le répertoire.

Authentification de l'administrateur et RBAC

Les administrateurs utilisent des comptes de connexion locaux ou distants pour s'authentifier auprès du cluster et de la machine virtuelle de stockage. Le contrôle d'accès basé sur des rôles (RBAC) détermine les commandes à laquelle un administrateur a accès.

Gestion de l'authentification administrateur et du RBAC

Authentification de l'administrateur et présentation du RBAC avec l'interface de ligne de commande

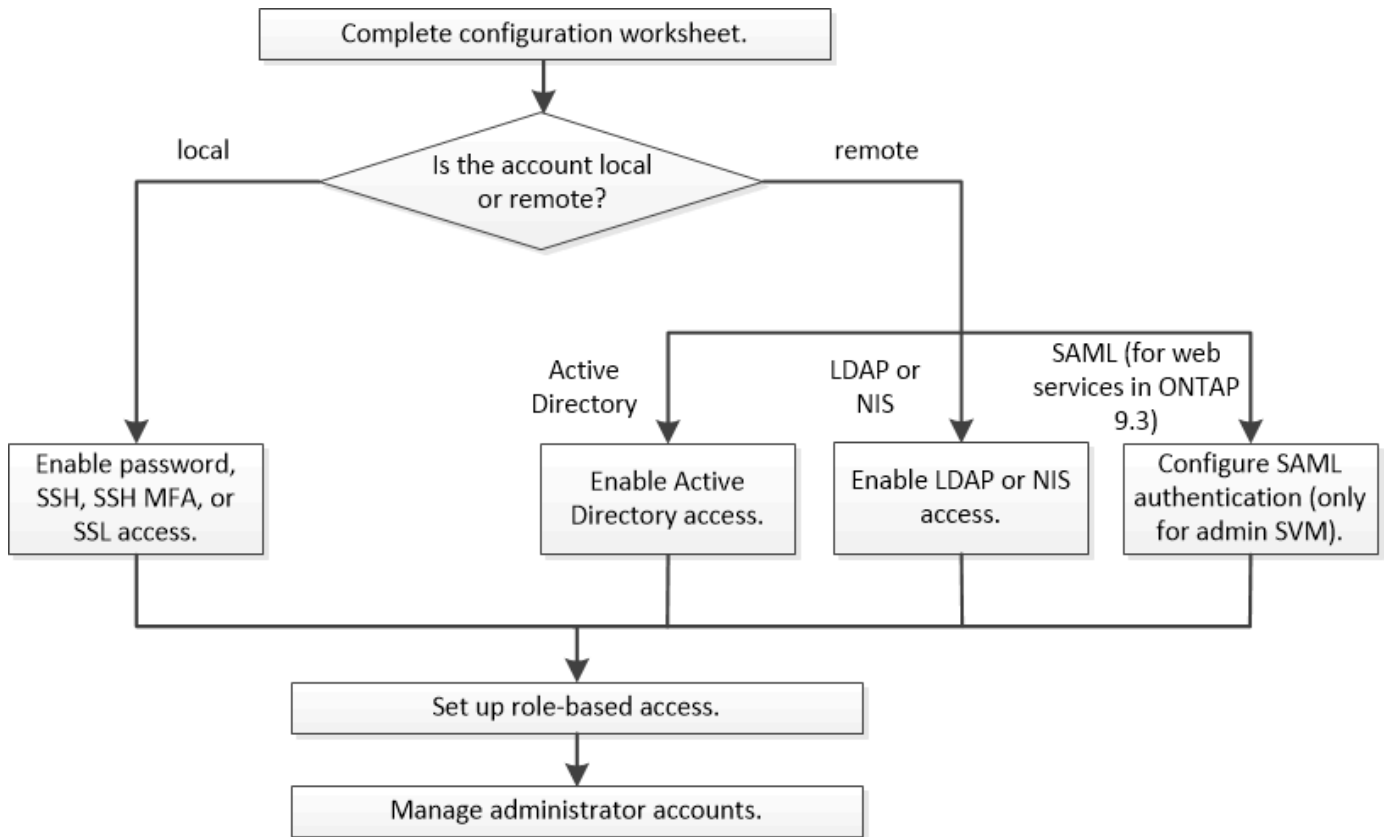
Vous pouvez activer des comptes de connexion pour les administrateurs du cluster ONTAP et des serveurs virtuels de stockage. Vous pouvez également utiliser le contrôle d'accès basé sur des rôles pour définir les fonctionnalités des administrateurs.

Vous activez les comptes de connexion et le RBAC de l'une des manières suivantes :

- Vous souhaitez utiliser l'interface de ligne de commandes ONTAP et non System Manager, ni un outil de création de scripts automatisé.
- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.
- Vous n'utilisez pas SNMP pour collecter des informations relatives au cluster.

Authentification de l'administrateur et flux de travail RBAC

Vous pouvez activer l'authentification pour les comptes d'administrateur local ou les comptes d'administrateur distant. Les informations de compte d'un compte local résident sur le système de stockage et les informations de compte d'un compte distant se trouvent ailleurs. Chaque compte peut avoir un rôle prédéfini ou un rôle personnalisé.



Vous pouvez activer les comptes d'administrateur local pour accéder à une machine virtuelle de stockage (SVM) d'administration ou à un SVM de données avec les types d'authentification suivants :

- Mot de passe
- Clé publique SSH
- Certificat SSL
- Authentification multifacteur SSH (MFA)

Depuis ONTAP 9.3, l'authentification avec mot de passe et clé publique est prise en charge.

Vous pouvez activer les comptes d'administrateur distant pour accéder à un SVM d'administration ou à un SVM de données avec les types d'authentification suivants :

- Active Directory
- Authentification SAML (uniquement pour le SVM d'administration)

Depuis ONTAP 9.3, l'authentification SAML permet d'accéder à la SVM d'administration à l'aide de l'un des services web suivants : service Processor Infrastructure, ONTAP API ou System Manager.

- Depuis la version ONTAP 9.4, l'authentification SSH MFA peut être utilisée pour les utilisateurs distants sur des serveurs LDAP ou NIS. L'authentification avec nsswitch et la clé publique est prise en charge.

Feuilles de calcul pour l'authentification de l'administrateur et la configuration du RBAC

Avant de créer des comptes de connexion et de configurer le contrôle d'accès basé sur des rôles (RBAC), vous devez rassembler les informations de chaque élément des

feuilles de configuration.

Créer ou modifier des comptes de connexion

Vous fournissez ces valeurs avec le `security login create` Lorsque vous activez les comptes de connexion pour accéder à une VM de stockage. Vous fournissez les mêmes valeurs avec le `security login modify` Lorsque vous modifiez la façon dont un compte accède à une VM de stockage.

Champ	Description	Votre valeur
<code>-vserver</code>	Nom de la VM de stockage auquel le compte accède. La valeur par défaut est le nom de la VM de stockage admin du cluster.	
<code>-user-or-group-name</code>	Nom d'utilisateur ou nom de groupe du compte. La définition d'un nom de groupe permet d'accéder à chaque utilisateur du groupe. Vous pouvez associer un nom d'utilisateur ou un nom de groupe à plusieurs applications.	
<code>-application</code>	L'application utilisée pour accéder à la VM de stockage : <ul style="list-style-type: none">• <code>http</code>• <code>ontapi</code>• <code>snmp</code>• <code>ssh</code>	

-authmethod	<p>Méthode utilisée pour authentifier le compte :</p> <ul style="list-style-type: none"> • <code>cert</code> Pour l'authentification par certificat SSL • <code>domain</code> Pour l'authentification Active Directory • <code>nsswitch</code> Pour l'authentification LDAP ou NIS • <code>password</code> pour l'authentification par mot de passe utilisateur • <code>publickey</code> pour l'authentification par clé publique • <code>community</code> Pour les chaînes de communauté SNMP • <code>usm</code> Pour le modèle de sécurité utilisateur SNMP • <code>saml</code> Pour l'authentification SAML (Security assertion Markup Language) 	
-remote-switch-ipaddress	<p>L'adresse IP du commutateur distant. Le commutateur distant peut être un commutateur de cluster surveillé par le moniteur d'état du commutateur du cluster (CSHM) ou un commutateur Fibre Channel (FC) surveillé par le moniteur d'état du MetroCluster (MCC-HM). Cette option n'est applicable que lorsque l'application est <code>snmp</code> et la méthode d'authentification est <code>usm</code>.</p>	
-role	<p>Rôle de contrôle d'accès attribué au compte :</p> <ul style="list-style-type: none"> • Pour le cluster (la VM de stockage admin), la valeur par défaut est <code>admin</code>. • Pour une VM de stockage de données, la valeur par défaut est <code>vsadmin</code>. 	

-comment	(Facultatif) texte descriptif pour le compte. Vous devez inclure le texte entre guillemets (").	
-is-ns-switch-group	Indique si le compte est un compte de groupe LDAP ou un compte de groupe NIS (yes ou no).	
-second-authentication-method	<p>Deuxième méthode d'authentification en cas d'authentification multifacteur :</p> <ul style="list-style-type: none"> • none si vous n'utilisez pas l'authentification multi-facteurs, valeur par défaut • publickey pour l'authentification par clé publique lorsque l'authmethod est un mot de passe ou un nsswitch • password pour l'authentification par mot de passe utilisateur lorsque authmethod est la clé publique • nsswitch pour l'authentification par mot de passe utilisateur lorsque la méthode d'authentification est publickey <p>L'ordre d'authentification est toujours la clé publique suivie du mot de passe.</p>	
-is-ldap-fastbind	À partir de ONTAP 9.11.1, lorsque la valeur est définie sur true, active la liaison rapide LDAP pour l'authentification nsswitch ; la valeur par défaut est false. Pour utiliser LDAP FAST bind, le -authentication-method la valeur doit être définie sur nsswitch. "Découvrez ldap fastbind pour l'authentification nsswitch."	

Configurer les informations de sécurité Cisco Duo

Vous fournissez ces valeurs avec le `security login duo create` Lorsque vous activez l'authentification à deux facteurs Cisco Duo avec des connexions SSH pour une machine virtuelle de stockage.

Champ	Description	Votre valeur
<code>-vserver</code>	La VM de stockage (appelée vServer dans l'interface de ligne de commandes ONTAP) à laquelle s'appliquent les paramètres d'authentification Duo.	
<code>-integration-key</code>	Votre clé d'intégration, obtenue lors de l'enregistrement de votre application SSH auprès de Duo.	
<code>-secret-key</code>	Votre clé secrète, obtenue lors de l'enregistrement de votre application SSH auprès de Duo.	
<code>-api-host</code>	<p>Le nom d'hôte de l'API, obtenu lors de l'enregistrement de votre application SSH auprès de Duo. Par exemple :</p> <div><pre>api- <HOSTNAME>.duosecurity.com</pre></div>	
<code>-fail-mode</code>	En cas d'erreurs de service ou de configuration qui empêchent l'authentification Duo, l'échec <code>safe</code> (autoriser l'accès) ou <code>secure</code> (refuser l'accès). La valeur par défaut est <code>safe</code> , Ce qui signifie que l'authentification Duo est ignorée si elle échoue en raison d'erreurs telles que le serveur d'API Duo inaccessible.	

-http-proxy	<p>Utilisez le proxy HTTP spécifié. Si le proxy HTTP nécessite une authentification, incluez les informations d'identification dans l'URL du proxy. Par exemple :</p> <pre>http- proxy=http://username :password@proxy.examp le.org:8080</pre>	
-autopush	<p>Soit <code>true</code> ou <code>false</code>. La valeur par défaut est <code>false</code>. Si <code>true</code>, Duo envoie automatiquement une demande de connexion Push au téléphone de l'utilisateur et revient à un appel téléphonique si Push n'est pas disponible. Notez que cela désactive efficacement l'authentification par mot de passe. Si <code>false</code>, l'utilisateur est invité à choisir une méthode d'authentification.</p> <p>Lorsqu'il est configuré avec <code>autopush = true</code>, nous recommandons le réglage <code>max-prompts = 1</code>.</p>	

<code>-max-prompts</code>	<p>Si un utilisateur ne parvient pas à s'authentifier avec un second facteur, Duo invite l'utilisateur à s'authentifier à nouveau. Cette option définit le nombre maximal d'invites affichées par Duo avant de refuser l'accès. Doit être de 1, 2, ou 3. La valeur par défaut est 1.</p> <p>Par exemple, quand <code>max-prompts = 1</code>, l'utilisateur doit s'authentifier avec succès à la première invite, tandis que si <code>max-prompts = 2</code>, si l'utilisateur saisit des informations incorrectes à l'invite initiale, il sera invité à s'authentifier à nouveau.</p> <p>Lorsqu'il est configuré avec <code>autopush = true</code>, nous recommandons le réglage <code>max-prompts = 1</code>.</p> <p>Pour la meilleure expérience, un utilisateur avec seulement l'authentification de clé publique aura toujours <code>max-prompts</code> réglé sur 1.</p>	
<code>-enabled</code>	<p>Activez l'authentification Duo à deux facteurs. Réglez sur <code>true</code> par défaut. Lorsqu'elle est activée, l'authentification Duo à deux facteurs est appliquée lors de la connexion SSH en fonction des paramètres configurés. Lorsque Duo est désactivé (défini sur <code>false</code>), l'authentification Duo est ignorée.</p>	

Définissez des rôles personnalisés

Vous fournissez ces valeurs avec le `security login role create` commande lorsque vous définissez un rôle personnalisé.

Champ	Description	Votre valeur
<code>-vserver</code>	(Facultatif) nom de la VM de stockage (appelée vServer dans l'interface de ligne de commandes ONTAP) associée au rôle.	

-role	Nom du rôle.	
-cmddirname	Répertoire de la commande ou de la commande auquel le rôle donne accès. Vous devez inclure les noms des sous-répertoires de commandes entre guillemets ("). Par exemple : "volume snapshot". Vous devez entrer DEFAULT pour spécifier tous les répertoires de commandes.	
-access	<p>(Facultatif) le niveau d'accès du rôle. Pour les répertoires de commandes :</p> <ul style="list-style-type: none"> • none (la valeur par défaut pour les rôles personnalisés) refuse l'accès aux commandes dans le répertoire de commande • readonly permet l'accès au show commandes dans le répertoire de commande et ses sous-répertoires • all donne accès à toutes les commandes du répertoire de commande et de ses sous-répertoires <p>Pour <i>commandes non intrinsèques</i> (commandes qui ne se terminent pas dans create, modify, delete, ou show) :</p> <ul style="list-style-type: none"> • none (la valeur par défaut pour les rôles personnalisés) refuse l'accès à la commande • readonly n'est pas applicable • all accorde l'accès à la commande <p>Pour accorder ou refuser l'accès aux commandes intrinsèques, vous devez spécifier le répertoire de commande.</p>	

-query	(Facultatif) l'objet de requête utilisé pour filtrer le niveau d'accès, qui est spécifié sous la forme d'une option valide pour la commande ou d'une commande dans le répertoire de commandes. Vous devez inclure l'objet de requête entre guillemets ("). Par exemple, si le répertoire de commande est <code>volume</code> , l'objet requête " <code>-aggr aggr0</code> " activation de l'accès pour le système <code>aggr0</code> agrégat uniquement.	
--------	--	--

Associer une clé publique à un compte d'utilisateur

Vous fournissez ces valeurs avec le `security login publickey create` Commande lorsque vous associez une clé publique SSH à un compte d'utilisateur.

Champ	Description	Votre valeur
-vserver	(Facultatif) Nom de la VM de stockage auquel le compte accède.	
-username	Nom d'utilisateur du compte. La valeur par défaut, <code>admin</code> , qui est le nom par défaut de l'administrateur du cluster.	
-index	Numéro d'index de la clé publique. La valeur par défaut est 0 si la clé est la première clé créée pour le compte ; sinon, la valeur par défaut est un plus que le numéro d'index existant le plus élevé pour le compte.	
-publickey	Clé publique OpenSSH. Vous devez inclure la clé entre guillemets (").	
-role	Rôle de contrôle d'accès attribué au compte.	
-comment	(Facultatif) texte descriptif pour la clé publique. Vous devez inclure le texte entre guillemets (").	

-x509-certificate	<p>(Facultatif) à partir de ONTAP 9.13.1, vous permet de gérer l'association de certificats X.509 avec la clé publique SSH.</p> <p>Lorsque vous associez un certificat X.509 à la clé publique SSH, ONTAP vérifie lors de la connexion SSH si ce certificat est valide. S'il a expiré ou a été révoqué, la connexion est interdite et la clé publique SSH associée est désactivée. Valeurs possibles :</p> <ul style="list-style-type: none"> • <code>install</code>: Installez le certificat X.509 codé PEM spécifié et associez-le à la clé publique SSH. Incluez le texte intégral du certificat que vous souhaitez installer. • <code>modify</code>: Mettez à jour le certificat X.509 codé PEM existant avec le certificat spécifié et associez-le à la clé publique SSH. Inclure le texte complet du nouveau certificat. • <code>delete</code>: Supprimez l'association de certificat X.509 existante avec la clé publique SSH. 	
-------------------	--	--

Installez un certificat numérique de serveur signé par une autorité de certification

Vous fournissez ces valeurs avec le `security certificate generate-csr` Lorsque vous générez une requête de signature de certificat numérique (RSC) à utiliser pour authentifier une machine virtuelle de stockage en tant que serveur SSL.

Champ	Description	Votre valeur
-common-name	Nom du certificat, qui est soit un nom de domaine complet (FQDN) ou un nom commun personnalisé.	
-size	Nombre de bits dans la clé privée. Plus la valeur est élevée, plus la clé est sécurisée. La valeur par défaut est 2048. Les valeurs possibles sont 512, 1024, 1536, et 2048.	

<code>-country</code>	Pays de la machine virtuelle de stockage, sous un code à deux lettres. La valeur par défaut est <code>US</code> . Consultez les pages de manuel pour obtenir une liste de codes.	
<code>-state</code>	État ou province de la machine virtuelle de stockage.	
<code>-locality</code>	Localité de la VM de stockage.	
<code>-organization</code>	Organisation de la machine virtuelle de stockage.	
<code>-unit</code>	Unité dans l'organisation de la machine virtuelle de stockage.	
<code>-email-addr</code>	Adresse e-mail de l'administrateur du contact pour la machine virtuelle de stockage.	
<code>-hash-function</code>	Fonction de hachage cryptographique pour la signature du certificat. La valeur par défaut est <code>SHA256</code> . Les valeurs possibles sont <code>SHA1</code> , <code>SHA256</code> , et <code>MD5</code> .	

Vous fournissez ces valeurs avec le `security certificate install` Lorsque vous installez un certificat numérique signé par une autorité de certification pour l'authentification du cluster ou de la machine virtuelle de stockage en tant que serveur SSL. Seules les options pertinentes pour la configuration des comptes sont présentées dans le tableau suivant.

Champ	Description	Votre valeur
<code>-vserver</code>	Nom de la machine virtuelle de stockage sur laquelle le certificat doit être installé.	

-type	<p>Le type de certificat :</p> <ul style="list-style-type: none"> • <code>server</code> pour les certificats de serveur et les certificats intermédiaires • <code>client-ca</code> Pour le certificat de clé publique de l'autorité de certification racine du client SSL • <code>server-ca</code> Pour le certificat de clé publique de l'autorité de certification racine du serveur SSL dont ONTAP est un client • <code>client</code> Pour un certificat numérique et une clé privée auto-signés ou signés par une autorité de certification pour ONTAP en tant que client SSL 	
-------	--	--

Configurez l'accès au contrôleur de domaine Active Directory

Vous fournissez ces valeurs avec le `security login domain-tunnel create` Commande lorsque vous avez déjà configuré un serveur SMB pour une machine virtuelle de stockage de données et que vous souhaitez configurer la machine virtuelle de stockage en tant que passerelle ou *tunnel* pour l'accès du contrôleur de domaine Active Directory au cluster.

Champ	Description	Votre valeur
-vserver	Nom de la VM de stockage pour laquelle le serveur SMB a été configuré.	

Vous fournissez ces valeurs avec le `vserver active-directory create` Lorsque vous n'avez pas configuré de serveur SMB et que vous souhaitez créer un compte d'ordinateur de machine virtuelle de stockage sur le domaine Active Directory.


Champ	Description	Votre valeur
-vserver	Nom de la machine virtuelle de stockage pour laquelle vous souhaitez créer un compte d'ordinateur Active Directory.	
-account-name	Nom NetBIOS du compte ordinateur.	
-domain	Le nom de domaine complet (FQDN).	

-ou	Unité organisationnelle du domaine. La valeur par défaut est CN=Computers. ONTAP ajoute cette valeur au nom de domaine pour produire le nom distinctif d'Active Directory.	
-----	--	--

Configurez l'accès aux serveurs LDAP ou NIS

Vous fournissez ces valeurs avec le `vserver services name-service ldap client create` Lorsque vous créez une configuration client LDAP pour la VM de stockage.

Seules les options pertinentes pour la configuration des comptes sont affichées dans le tableau suivant :

Champ	Description	Votre valeur
-vserver	Nom de la VM de stockage pour la configuration client.	
-client-config	Nom de la configuration client.	
-ldap-servers	Liste séparée par des virgules d'adresses IP et de noms d'hôte pour les serveurs LDAP auxquels le client se connecte.	
-schema	Schéma utilisé par le client pour effectuer des requêtes LDAP.	
-use-start-tls	<p>Si le client utilise Start TLS pour chiffrer la communication avec le serveur LDAP (<code>true</code> ou <code>false</code>).</p> <div>  <p>Le protocole Start TLS est pris en charge uniquement pour l'accès aux machines virtuelles de stockage de données. Elle n'est pas prise en charge pour l'accès aux machines virtuelles de stockage d'administration.</p> </div>	

Vous fournissez ces valeurs avec le `vserver services name-service ldap create` Lorsque vous associez une configuration client LDAP à la machine virtuelle de stockage.

Champ	Description	Votre valeur
<code>-vserver</code>	Nom de la machine virtuelle de stockage à laquelle la configuration client doit être associée.	
<code>-client-config</code>	Nom de la configuration client.	
<code>-client-enabled</code>	Indique si la VM de stockage peut utiliser la configuration client LDAP (true ou false).	

Vous fournissez ces valeurs avec le `vserver services name-service nis-domain create` Lorsque vous créez une configuration de domaine NIS sur une machine virtuelle de stockage.

Champ	Description	Votre valeur
<code>-vserver</code>	Nom de la machine virtuelle de stockage sur laquelle la configuration de domaine doit être créée.	
<code>-domain</code>	Le nom du domaine.	
<code>-active</code>	Indique si le domaine est actif (true ou false).	
<code>-servers</code>	ONTAP 9.0, 9.1 : liste séparée par des virgules d'adresses IP pour les serveurs NIS utilisés par la configuration de domaine.	
<code>-nis-servers</code>	Liste séparée par des virgules d'adresses IP et de noms d'hôte pour les serveurs NIS utilisés par la configuration de domaine.	

Vous fournissez ces valeurs avec le `vserver services name-service ns-switch create` commande lorsque vous spécifiez l'ordre de recherche des sources de service de noms.

Champ	Description	Votre valeur
<code>-vserver</code>	Nom de la machine virtuelle de stockage sur laquelle l'ordre de recherche de service de noms doit être configuré.	

-database	<p>La base de données du service de noms :</p> <ul style="list-style-type: none"> • <code>hosts</code> Pour les services de noms DNS et de fichiers • <code>group</code> Pour les fichiers, LDAP et services de noms NIS • <code>passwd</code> Pour les fichiers, LDAP et services de noms NIS • <code>netgroup</code> Pour les fichiers, LDAP et services de noms NIS • <code>namemap</code> Pour les fichiers et les services de noms LDAP 	
-sources	<p>Ordre dans lequel rechercher les sources de service de noms (dans une liste séparée par des virgules) :</p> <ul style="list-style-type: none"> • <code>files</code> • <code>dns</code> • <code>ldap</code> • <code>nis</code> 	

Configurez l'accès SAML

À partir de ONTAP 9.3, vous fournissez ces valeurs à `security saml-sp create` Commande pour configurer l'authentification SAML.

Champ	Description	Votre valeur
-idp-uri	Adresse FTP ou adresse HTTP de l'hôte IDP (Identity Provider) à partir duquel les métadonnées IDP peuvent être téléchargées.	
-sp-host	Nom d'hôte ou adresse IP de l'hôte SAML Service Provider (système ONTAP). Par défaut, l'adresse IP de la LIF de cluster-management est utilisée.	

<code>-cert-ca</code> et <code>-cert-serial</code> , ou <code>-cert-common-name</code>	Détails du certificat de serveur de l'hôte du fournisseur de services (système ONTAP). Vous pouvez saisir soit le certificat du fournisseur de services émettant l'autorité de certification (CA) et le numéro de série du certificat, soit le nom commun du certificat de serveur.	
<code>-verify-metadata-server</code>	Indique si l'identité du serveur de métadonnées IDP doit être validée (<code>true</code> ou <code>false</code>). Il est recommandé de toujours définir cette valeur sur <code>true</code> .	

Créer des comptes de connexion

Présentation de la création de comptes de connexion

Vous pouvez activer les comptes d'administrateur des clusters et des SVM locaux ou distants. Un compte local est un compte dans lequel les informations de compte, la clé publique ou le certificat de sécurité résident sur le système de stockage. Les informations de compte AD sont stockées sur un contrôleur de domaine. Les comptes LDAP et NIS résident sur des serveurs LDAP et NIS.

Administrateurs Cluster et SVM

Un *cluster Administrator* accède au SVM d'admin pour le cluster. La SVM d'admin et un administrateur du cluster avec le nom réservé `admin` sont automatiquement créées lorsque le cluster est configuré.

Un administrateur de cluster avec la valeur par défaut `admin` le rôle peut administrer l'ensemble du cluster et ses ressources. L'administrateur du cluster peut créer d'autres administrateurs de cluster disposant de différents rôles selon les besoins.

Un *administrateur SVM* accède à un SVM de données. L'administrateur du cluster crée des SVM de données et des administrateurs SVM si nécessaire.

Les administrateurs du SVM sont affectés à `vsadmin` rôle par défaut. L'administrateur du cluster peut attribuer différents rôles aux administrateurs du SVM si nécessaire.

Respecter les conventions de nom

Les noms génériques suivants ne peuvent pas être utilisés pour les comptes d'administrateur du cluster distant et du SVM :

- « adm »
- « bac »
- « cli »

- « démon »
- « ftp »
- « jeux »
- « arrêter »
- « lp »
- « courrier »
- « homme »
- « naroot »
- « NetApp »
- « actualités »
- « personne »
- « opérateur »
- « racine »
- « arrêt »
- « sshd »
- « sync »
- « sys »
- « uuucp »
- « www »

Rôles fusionnés

Si vous activez plusieurs comptes distants pour le même utilisateur, l'utilisateur est affecté à l'Union de tous les rôles spécifiés pour les comptes. C'est-à-dire, si un compte LDAP ou NIS est affecté à `vsadmin` Et le compte de groupe AD pour le même utilisateur est affecté à `vsadmin-volume` Rôle, l'utilisateur AD se connecte avec les fonctions plus inclusives `vsadmin` capacités. Les rôles sont définis comme *fusionnés*.

Activez l'accès au compte local

Activer la présentation de l'accès au compte local

Un compte local est un compte dans lequel les informations de compte, la clé publique ou le certificat de sécurité résident sur le système de stockage. Vous pouvez utiliser le `security login create` Commande pour permettre aux comptes locaux d'accéder à un admin ou un SVM de données.

Activer l'accès au compte par mot de passe

Vous pouvez utiliser le `security login create` Commande permettant aux comptes d'administrateur d'accéder à un admin ou un SVM de données avec un mot de passe. Après avoir saisi la commande, vous êtes invité à saisir le mot de passe.

Description de la tâche

Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion,

vous pouvez utiliser le `security login modify` commande permettant d'ajouter le rôle ultérieurement.

Avant de commencer

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

Étape

1. Activer les comptes d'administrateur local pour accéder à un SVM via un mot de passe :

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

La commande suivante active le compte d'administrateur du cluster `admin1` avec le prédéfini `backup` Rôle d'accès à la SVM d'`adminengCluster` à l'aide d'un mot de passe. Après avoir saisi la commande, vous êtes invité à saisir le mot de passe.

```
cluster1::>security login create -vserver engCluster -user-or-group-name  
admin1 -application ssh -authmethod password -role backup
```

Activez les comptes de clé publique SSH

Vous pouvez utiliser le `security login create` Commande permettant aux comptes d'administrateur d'accéder à un SVM de données ou `admin` avec une clé publique SSH.

Description de la tâche

- Vous devez associer la clé publique au compte avant que le compte puisse accéder à la SVM.

[Association d'une clé publique à un compte d'utilisateur](#)

Vous pouvez effectuer cette tâche avant ou après avoir activé l'accès au compte.

- Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser le `security login modify` commande permettant d'ajouter le rôle ultérieurement.

Si vous souhaitez activer le mode FIPS sur votre cluster, vous devez reconfigurer les comptes de clés publiques SSH existants sans les algorithmes de clé pris en charge avec un type de clé pris en charge. Les comptes doivent être reconfigurés avant l'activation de FIPS, sinon l'authentification de l'administrateur échouera.

Le tableau suivant indique les algorithmes de type de clé hôte pris en charge pour les connexions ONTAP SSH. Ces types de clés ne s'appliquent pas à la configuration de l'authentification publique SSH.

Version de ONTAP	Types de clés pris en charge en mode FIPS	Types de clés pris en charge en mode non FIPS

9.11.1 et versions ultérieures	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 et versions antérieures	ecdsa-sha2-nistp256 ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa



La prise en charge de l'algorithme de clé hôte ssh-ed25519 a été supprimée à partir de ONTAP 9.11.1.

Pour plus d'informations, voir ["Configurez la sécurité réseau à l'aide de FIPS"](#).

Avant de commencer

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

Étape

1. Activer les comptes d'administrateur local pour accéder à un SVM à l'aide d'une clé publique SSH :

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

La commande suivante active le compte d'administrateur du SVM `svmadmin1` avec le prédéfini `vsadmin-volume` Rôle d'accès à la `SVMengData1` Utilisation d'une clé publique SSH :

```
cluster1::>security login create -vserver engData1 -user-or-group-name
svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
```

Une fois que vous avez terminé

Si vous n'avez pas associé de clé publique au compte administrateur, vous devez le faire avant que le compte puisse accéder à la SVM.

[Association d'une clé publique à un compte d'utilisateur](#)

Activez les comptes d'authentification multifacteur (MFA)

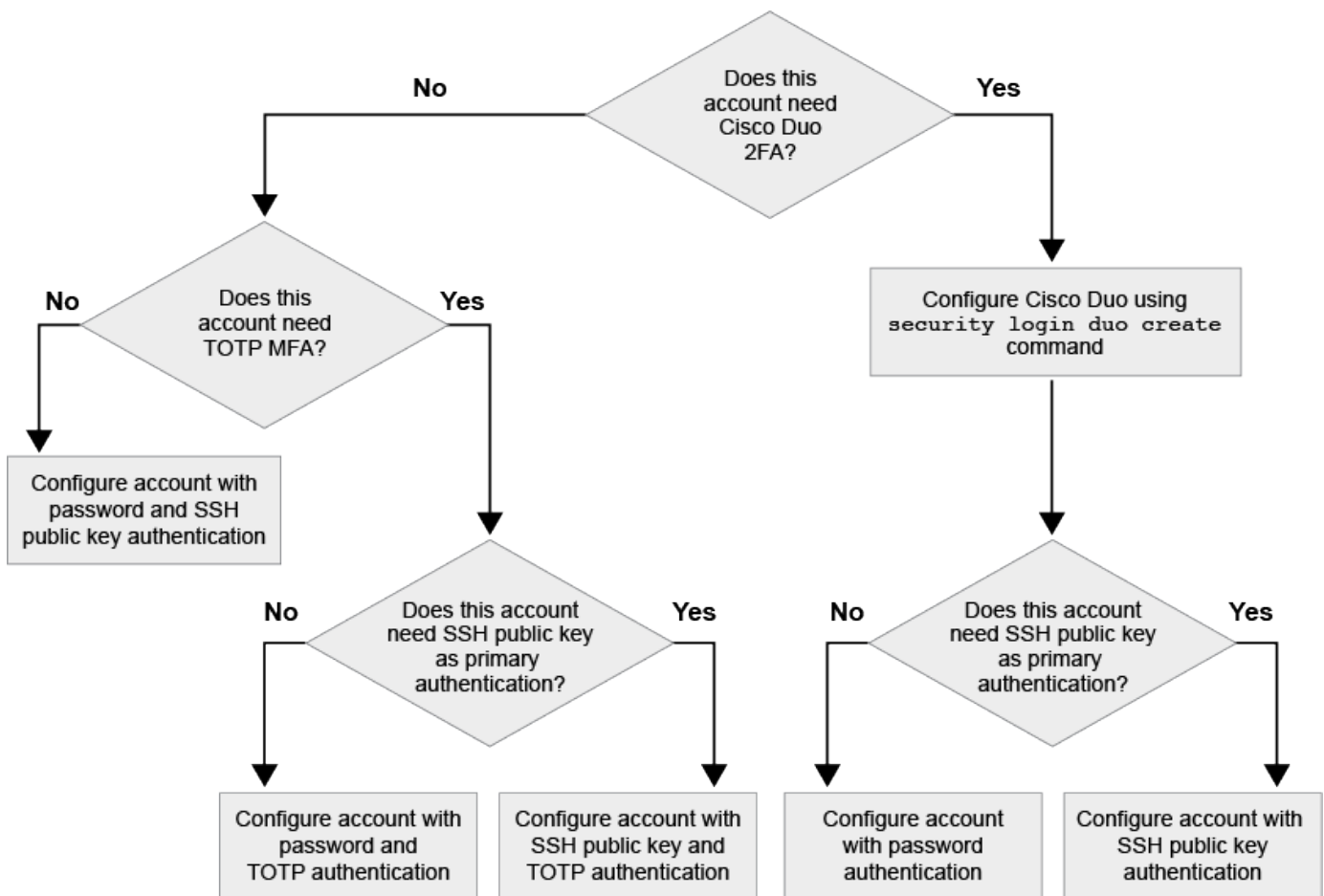
Présentation de l'authentification multifacteur

L'authentification multifacteur (MFA) vous permet d'améliorer la sécurité en exigeant que les utilisateurs fournissent deux méthodes d'authentification pour se connecter à un administrateur ou à une VM de stockage des données.

Selon votre version de ONTAP, vous pouvez utiliser une clé publique SSH, un mot de passe utilisateur et un mot de passe à usage unique (TOTP) pour l'authentification multifacteur. Lorsque vous activez et configurez Cisco Duo (ONTAP 9.14.1 et versions ultérieures), il sert de méthode d'authentification supplémentaire, en complément des méthodes existantes pour tous les utilisateurs.

Disponible à partir de...	Première méthode d'authentification	Deuxième méthode d'authentification
ONTAP 9.14.1	Clé publique SSH	TOTP
	Mot de passe utilisateur	TOTP
	Clé publique SSH	Duo Cisco
	Mot de passe utilisateur	Duo Cisco
ONTAP 9.13.1	Clé publique SSH	TOTP
	Mot de passe utilisateur	TOTP
ONTAP 9.3	Clé publique SSH	Mot de passe utilisateur

Si l'authentification multifacteur est configurée, l'administrateur du cluster doit d'abord activer le compte utilisateur local. Le compte doit alors être configuré par l'utilisateur local.



Activez l'authentification multifacteur

L'authentification multifacteur (MFA) vous permet d'améliorer la sécurité en exigeant que

les utilisateurs fournissent deux méthodes d'authentification pour se connecter à un administrateur ou à un SVM de données.

Description de la tâche

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser le `security login modify` commande permettant d'ajouter le rôle ultérieurement.

"Modification du rôle attribué à un administrateur"

- Si vous utilisez une clé publique pour l'authentification, vous devez associer la clé publique au compte avant que le compte puisse accéder à la SVM.

"Associer une clé publique à un compte d'utilisateur"

Vous pouvez effectuer cette tâche avant ou après avoir activé l'accès au compte.

- À partir de ONTAP 9.12.1, vous pouvez utiliser les périphériques d'authentification matérielle Yubikey pour le client SSH MFA en utilisant les normes d'authentification FIDO2 (Fast Identity Online) ou PIV (Personal Identity Verification).

Activez MFA avec la clé publique SSH et le mot de passe utilisateur

Depuis la version ONTAP 9.3, l'administrateur du cluster peut configurer des comptes utilisateurs locaux pour se connecter à MFA à l'aide d'une clé publique SSH et d'un mot de passe utilisateur.

1. Activer MFA sur le compte utilisateur local avec la clé publique SSH et le mot de passe utilisateur :

```
security login create -vserver <svm_name> -user-or-group-name  
<user_name> -application ssh -authentication-method <password|publickey>  
-role admin -second-authentication-method <password|publickey>
```

La commande suivante nécessite un compte d'administrateur du SVM `admin2` avec le prédéfini `admin` Rôle de connexion à la SVM `engData1` Avec une clé publique SSH et un mot de passe utilisateur :

```
cluster-1::> security login create -vserver engData1 -user-or-group-name  
admin2 -application ssh -authentication-method publickey -role admin  
-second-authentication-method password
```

```
Please enter a password for user 'admin2':
```

```
Please enter it again:
```

```
Warning: To use public-key authentication, you must create a public key  
for user "admin2".
```

Activez MFA avec TOTP

À partir de ONTAP 9.13.1, vous pouvez améliorer la sécurité en exigeant des utilisateurs locaux qu'ils se

connectent à un administrateur ou à un SVM de données à l'aide d'une clé publique SSH ou d'un mot de passe utilisateur et d'un mot de passe à usage unique (TOTP) basé sur le temps. Une fois le compte activé pour MFA avec TOTP, l'utilisateur local doit se connecter à ["terminez la configuration"](#).

TOTP est un algorithme informatique qui utilise l'heure actuelle pour générer un mot de passe à usage unique. Si TOTP est utilisé, il s'agit toujours de la deuxième forme d'authentification après la clé publique SSH ou le mot de passe utilisateur.

Avant de commencer

Vous devez être administrateur du stockage pour effectuer ces tâches.

Étapes

Vous pouvez configurer MFA avec un mot de passe utilisateur ou une clé publique SSH comme première méthode d'authentification et TOTP comme deuxième méthode d'authentification.

Activer MFA avec mot de passe utilisateur et TOTP

1. Activez un compte utilisateur pour l'authentification multifacteur avec un mot de passe utilisateur et un TOTP.

Pour les nouveaux comptes utilisateur

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

Pour les comptes utilisateur existants

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

2. Vérifier que MFA avec TOTP est activé :

```
security login show
```

Activez MFA avec clé publique SSH et TOTP

1. Activez un compte utilisateur pour l'authentification multifacteur avec une clé publique SSH et un TOTP.

Pour les nouveaux comptes utilisateur

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

Pour les comptes utilisateur existants

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

2. Vérifier que MFA avec TOTP est activé :

```
security login show
```

Une fois que vous avez terminé

- Si vous n'avez pas associé de clé publique au compte administrateur, vous devez le faire avant que le compte puisse accéder à la SVM.

["Association d'une clé publique à un compte d'utilisateur"](#)

- L'utilisateur local doit se connecter pour terminer la configuration MFA avec TOTP.

["Configurer le compte utilisateur local pour MFA avec TOTP"](#)

Informations associées

En savoir plus sur ["Authentification multifactorielle dans ONTAP 9 \(TR-4647\)"](#).

Configurer le compte utilisateur local pour MFA avec TOTP

À partir de la ONTAP 9.13.1, les comptes utilisateur peuvent être configurés avec l'authentification multifacteur (MFA) avec un mot de passe à usage unique (TOTP).

Avant de commencer

- L'administrateur du stockage doit ["Activez MFA avec TOTP"](#) comme deuxième méthode d'authentification pour votre compte utilisateur.
- La méthode d'authentification de votre compte utilisateur principal doit être un mot de passe utilisateur ou une clé SSH publique.
- Vous devez configurer votre application TOTP pour qu'elle fonctionne avec votre smartphone et créer votre clé secrète TOTP.

TOTP est pris en charge par diverses applications d'authentificateur telles que Google Authenticator.

Étapes

1. Connectez-vous à votre compte utilisateur avec votre méthode d'authentification actuelle.

Votre méthode d'authentification actuelle doit être un mot de passe utilisateur ou une clé publique SSH.

2. Créez la configuration TOTP sur votre compte :

```
security login totp create -vserver "<svm_name>" -username  
"<account_username >"
```

3. Vérifiez que la configuration TOTP est activée sur votre compte :

```
security login totp show -vserver "<svm_name>" -username  
"<account_username>"
```

Réinitialiser la clé secrète TOTP

Pour protéger la sécurité de votre compte, si votre clé secrète TOTP est compromise ou perdue, vous devez la désactiver et en créer une nouvelle.

Réinitialisez le TOTP si votre clé est compromise

Si votre clé secrète TOTP est compromise, mais que vous y avez toujours accès, vous pouvez supprimer la clé compromise et en créer une nouvelle.

1. Connectez-vous à votre compte utilisateur avec votre mot de passe utilisateur ou votre clé publique SSH et votre clé secrète TOTP compromise.
2. Supprimez la clé secrète TOTP compromise :

```
security login totp delete -vserver <svm_name> -username  
<account_username>
```

3. Créez une nouvelle clé secrète TOTP :

```
security login totp create -vserver <svm_name> -username  
<account_username>
```

4. Vérifiez que la configuration TOTP est activée sur votre compte :

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

Réinitialisez le TOTP en cas de perte de votre clé

Si votre clé secrète TOTP est perdue, contactez votre administrateur de stockage à l'adresse "[faites désactiver la clé](#)". Une fois votre clé désactivée, vous pouvez utiliser votre première méthode d'authentification pour vous connecter et configurer un nouveau TOTP.

Avant de commencer

La clé secrète TOTP doit être désactivée par un administrateur de stockage.

Si vous ne possédez pas de compte d'administrateur de stockage, contactez votre administrateur de stockage pour que la clé soit désactivée.

Étapes

1. Une fois le secret TOTP désactivé par un administrateur de stockage, utilisez votre méthode d'authentification principale pour vous connecter à votre compte local.
2. Créez une nouvelle clé secrète TOTP :

```
security login totp create -vserver <svm_name> -username  
<account_username >
```

3. Vérifiez que la configuration TOTP est activée sur votre compte :

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

Désactiver la clé secrète TOTP pour le compte local

Si la clé secrète TOTP (Time-based password) d'un utilisateur local est perdue, la clé perdue doit être désactivée par un administrateur de stockage avant que l'utilisateur puisse créer une nouvelle clé secrète TOTP.

Description de la tâche

Cette tâche ne peut être effectuée qu'à partir d'un compte d'administrateur de cluster.

Étape

1. Désactiver la clé secrète TOTP :

```
security login totp delete -vserver "<svm_name>" -username  
"<account_username>"
```

Activez les comptes de certificat SSL

Vous pouvez utiliser le `security login create` Commande pour permettre aux comptes d'administrateur d'accéder à un SVM d'administration ou de données avec un certificat SSL.

Description de la tâche

- Vous devez installer un certificat numérique de serveur signé par une autorité de certification pour que le compte puisse accéder à la SVM.

[Génération et installation d'un certificat de serveur signé par une autorité de certification](#)

Vous pouvez effectuer cette tâche avant ou après avoir activé l'accès au compte.

- Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez ajouter le rôle ultérieurement avec le `security login modify` commande.

[Modification du rôle attribué à un administrateur](#)



Pour les comptes d'administrateur de cluster, l'authentification par certificat est prise en charge avec `http`, `ontapi`, et `rest` en termes de latence. Pour les comptes d'administrateur SVM, l'authentification par certificat est prise en charge uniquement avec `ontapi` et `rest` en termes de latence.

Étape

1. Activer les comptes d'administrateur local pour accéder à un SVM à l'aide d'un certificat SSL :

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["Pages de manuel ONTAP par version"](#).

La commande suivante active le compte d'administrateur du SVM `svmadmin2` avec la valeur par défaut `vsadmin` Rôle d'accès à la SVM `engData2` Utilisation d'un certificat numérique SSL.

```
cluster1::>security login create -vserver engData2 -user-or-group-name  
svmadmin2 -application ontapi -authmethod cert
```

Une fois que vous avez terminé

Si vous n'avez pas installé de certificat numérique serveur signé par une autorité de certification, vous devez le faire avant que le compte puisse accéder à la SVM.

Génération et installation d'un certificat de serveur signé par une autorité de certification

Activez l'accès au compte Active Directory

Vous pouvez utiliser le `security login create` Commande pour permettre aux utilisateurs ou groupes Active Directory (AD) d'accéder à un SVM d'administration ou de données. Tout utilisateur du groupe AD peut accéder à la SVM avec le rôle attribué au groupe.

Description de la tâche

- Vous devez configurer l'accès du contrôleur AD domain au cluster ou au SVM avant que le compte ne puisse accéder au SVM.

Configuration de l'accès au contrôleur de domaine Active Directory

Vous pouvez effectuer cette tâche avant ou après avoir activé l'accès au compte.

- À partir de ONTAP 9.13.1, vous pouvez utiliser une clé publique SSH comme méthode d'authentification principale ou secondaire avec un mot de passe utilisateur AD.

Si vous choisissez d'utiliser une clé publique SSH comme authentification principale, aucune authentification AD n'a lieu.

- Vous pouvez utiliser ONTAP 9.11.1 depuis ["LDAP Fast bind pour l'authentification nsswitch"](#) S'il est pris en charge par le serveur LDAP AD.

- Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser le `security login modify` commande permettant d'ajouter le rôle ultérieurement.

Modification du rôle attribué à un administrateur



L'accès au compte du groupe D'ANNONCES est pris en charge uniquement avec le `SSH`, `ontapi`, et `rest` en termes de latence. Les groupes AD ne sont pas pris en charge avec l'authentification de clé publique `SSH`, qui est couramment utilisée pour l'authentification multifacteur.

Avant de commencer

- L'heure du cluster doit être synchronisée sur dans les cinq minutes qui suivent l'heure sur le contrôleur de domaine AD.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étape

1. Activer les comptes d'utilisateur ou d'administrateur de groupe AD pour accéder à un SVM :

Pour les utilisateurs AD :

Version ONTAP	Authentification principale	Authentification secondaire	Commande
9.13.1 et versions ultérieures	Clé publique	Aucune	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role></pre>

Version ONTAP	Authentification principale	Authentification secondaire	Commande
9.13.1 et versions ultérieures	Domaine	Clé publique	<p>Pour un nouvel utilisateur</p> <pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre> <p>Pour un utilisateur existant</p> <pre>security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre>
9.0 et versions ultérieures	Domaine	Aucune	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap- fastbind true]</pre>

Pour les groupes AD :

Version ONTAP	Authentification principale	Authentification secondaire	Commande
9.0 et versions ultérieures	Domaine	Aucune	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap- fastbind true]</pre>

Pour connaître la syntaxe complète des commandes, voir ["Feuilles de travail pour l'authentification administrateur et la configuration RBAC"](#)

Une fois que vous avez terminé

Si vous n'avez pas configuré l'accès au contrôleur AD domain au cluster ou au SVM, vous devez le faire avant que le compte puisse accéder au SVM.

Configuration de l'accès au contrôleur de domaine Active Directory

Activez l'accès aux comptes LDAP ou NIS

Vous pouvez utiliser le `security login create` Commande pour activer les comptes utilisateur LDAP ou NIS pour accéder à un SVM de données ou admin Si vous n'avez pas configuré l'accès au serveur LDAP ou NIS au SVM, vous devez le faire avant que le compte puisse accéder à la SVM.

Description de la tâche

- Les comptes de groupe ne sont pas pris en charge.
- Vous devez configurer l'accès des serveurs LDAP ou NIS au SVM avant que le compte ne puisse accéder au SVM.

Configuration de l'accès aux serveurs LDAP ou NIS

Vous pouvez effectuer cette tâche avant ou après avoir activé l'accès au compte.

- Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser le `security login modify` commande permettant d'ajouter le rôle ultérieurement.

Modification du rôle attribué à un administrateur

- Depuis la version ONTAP 9.4, l'authentification multifacteur (MFA) est prise en charge pour les utilisateurs distants sur des serveurs LDAP ou NIS.
- Vous pouvez utiliser ONTAP 9.11.1 depuis ["LDAP Fast bind pour l'authentification nsswitch"](#) S'il est pris en charge par le serveur LDAP.
- En raison d'un problème LDAP connu, vous ne devez pas utiliser le ' : ' (Deux-points) dans n'importe quel champ d'informations de compte d'utilisateur LDAP (par exemple, `gecos`, `userPassword`, etc.). Dans le cas contraire, l'opération de recherche échoue pour cet utilisateur.

Avant de commencer

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

Étapes

1. Activer les comptes utilisateurs ou groupes LDAP ou NIS pour accéder à un SVM :

```
security login create -vserver SVM_name -user-or-group-name user_name
-application application -authmethod nsswitch -role role -comment comment -is
-ns-switch-group yes|no [-is-ldap-fastbind true]
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

"Création ou modification de comptes de connexion"

La commande suivante active le compte d'administrateur de cluster LDAP ou NIS `guest2` avec le prédéfini `backup` Rôle d'accès à la SVM d'`adminengCluster`.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
guest2 -application ssh -authmethod nsswitch -role backup
```

2. Activer la connexion MFA pour les utilisateurs LDAP ou NIS :

```
security login modify -user-or-group-name rem_usr1 -application ssh
-authentication-method nsswitch -role admin -is-ns-switch-group no -second
-authentication-method publickey
```

La méthode d'authentification peut être spécifiée comme `publickey` et deuxième méthode d'authentification en tant que `nsswitch`.

L'exemple suivant montre que l'authentification MFA est activée :

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

Une fois que vous avez terminé

Si vous n'avez pas configuré l'accès au serveur LDAP ou NIS au SVM, vous devez le faire avant que le compte puisse accéder à la SVM.

Configuration de l'accès aux serveurs LDAP ou NIS

Gestion des rôles de contrôle d'accès

Gérer la présentation des rôles de contrôle d'accès

Le rôle attribué à un administrateur détermine les commandes auxquelles l'administrateur a accès. Vous attribuez le rôle lorsque vous créez le compte pour l'administrateur. Vous pouvez attribuer un autre rôle ou définir des rôles personnalisés selon vos besoins.

Modifiez le rôle attribué à un administrateur

Vous pouvez utiliser le `security login modify` Commande pour modifier le rôle d'un compte d'administrateur de cluster ou de SVM. Vous pouvez affecter un rôle prédéfini ou personnalisé.

Avant de commencer

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

Étape

1. Modifier le rôle d'un administrateur de cluster ou de SVM :

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

"Création ou modification de comptes de connexion"

La commande suivante permet de changer le rôle du compte d'administrateur du cluster AD
DOMAIN1\guest1 au prédéfini readonly rôle.

```
cluster1::>security login modify -vserver engCluster -user-or-group-name  
DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
```

La commande suivante permet de changer le rôle des comptes administrateur du SVM dans le compte AD
group DOMAIN1\adgroup au personnalisé vol_role rôle.

```
cluster1::>security login modify -vserver engData -user-or-group-name  
DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
```

Définissez des rôles personnalisés

Vous pouvez utiliser le `security login role create` commande pour définir un rôle personnalisé. Vous pouvez exécuter la commande autant de fois que nécessaire pour obtenir la combinaison exacte de fonctions que vous souhaitez associer au rôle.

Description de la tâche

- Un rôle, qu'il soit prédéfini ou personnalisé, accorde ou refuse l'accès aux commandes ou aux répertoires de commandes ONTAP.

Un répertoire de commande (`volume`, par exemple) est un groupe de commandes et de sous-répertoires de commandes associés. Sauf comme décrit dans cette procédure, l'octroi ou le refus de l'accès à un répertoire de commandes accorde ou refuse l'accès à chaque commande du répertoire et de ses sous-répertoires.

- L'accès aux commandes ou aux sous-répertoires spécifiques remplace l'accès au répertoire parent.

Si un rôle est défini à l'aide d'un répertoire de commandes, puis qu'il est défini à nouveau avec un niveau d'accès différent pour une commande spécifique ou pour un sous-répertoire du répertoire parent, le niveau d'accès spécifié pour la commande ou le sous-répertoire remplace celui du parent.



Vous ne pouvez pas attribuer un administrateur SVM un rôle qui donne accès à une commande ou au répertoire de commande disponible uniquement pour le `admin` administrateur du cluster --par exemple, le `security` répertoire de commande.

Avant de commencer

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

Étape

1. Définissez un rôle personnalisé :

```
security login role create -vserver SVM_name -role role -cmddirname  
command_or_directory_name -access access_level -query query
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

Les commandes suivantes permettent d'accorder le `vol_role` rôle accès complet aux commandes dans `volume` le répertoire de commande et l'accès en lecture seule aux commandes de l'`volume snapshot` sous-répertoire.

```
cluster1::>security login role create -role vol_role -cmddirname  
"volume" -access all  
  
cluster1::>security login role create -role vol_role -cmddirname "volume  
snapshot" -access readonly
```

Les commandes suivantes permettent d'accorder le `SVM_storage` accès en lecture seule du rôle aux commandes dans `storage` répertoire de commandes, pas d'accès aux commandes dans le `storage encryption` sous-répertoire et accès complet au `storage aggregate plex offline` commande non intrinsèque.

```
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage" -access readonly  
  
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage encryption" -access none  
  
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage aggregate plex offline" -access all
```

Rôles prédéfinis pour les administrateurs du cluster

Les rôles prédéfinis des administrateurs du cluster doivent répondre à la plupart des besoins. Vous pouvez créer des rôles personnalisés selon vos besoins. Par défaut un administrateur de cluster se voit attribuer le paramétrage prédéfini `admin` rôle.

Le tableau suivant répertorie les rôles prédéfinis pour les administrateurs du cluster :

Ce rôle...	Dispose de ce niveau d'accès...	Aux commandes ou répertoires de commandes suivants

admin	tous	Tous les répertoires de commandes (DEFAULT)
admin-no-fsa (disponible à partir de ONTAP 9.12.1)	Lecture/écriture	<ul style="list-style-type: none"> • Tous les répertoires de commandes (DEFAULT) • security login rest-role • security login role
Lecture seule	<ul style="list-style-type: none"> • security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics 	Aucune
volume file show-disk-usage	AutoSupport	tous
<ul style="list-style-type: none"> • set • system node autosupport 	Aucune	Tous les autres répertoires de commandes (DEFAULT)
sauvegarde	tous	vserver services ndmp
lecture seule	volume	Aucune

Tous les autres répertoires de commandes (DEFAULT)	lecture seule	tous
<ul style="list-style-type: none"> • security login password <p>Pour la gestion du mot de passe local et des informations clés du compte utilisateur</p> <ul style="list-style-type: none"> • set 	Aucune	security
lecture seule	Tous les autres répertoires de commandes (DEFAULT)	Aucune



Le autosupport le rôle est affecté au prédéfini autosupport Compte, utilisé par AutoSupport OnDemand. ONTAP vous empêche de modifier ou de supprimer le autosupport compte. ONTAP vous empêche également d'attribuer le autosupport rôle vers d'autres comptes utilisateur.

Rôles prédéfinis pour les administrateurs des SVM

Les rôles prédéfinis des administrateurs des SVM devraient répondre à la plupart des besoins. Vous pouvez créer des rôles personnalisés selon vos besoins. Par défaut un administrateur SVM est affecté au prédéfini `vsadmin` rôle.

Le tableau suivant répertorie les rôles prédéfinis pour les administrateurs du SVM :

Nom du rôle	Capacités
vsadmin	<ul style="list-style-type: none"> • Gestion du mot de passe local et des informations clés du compte utilisateur • Gestion des volumes, à l'exception des déplacements de volumes • Gestion des quotas, des qtrees, des copies Snapshot et des fichiers • Gestion des LUN • Exécution d'opérations SnapLock, sauf suppression privilégiée • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Surveillance des tâches • Surveillance des connexions réseau et de l'interface réseau • Contrôle de l'état de santé de la SVM

volume vsadmin	<ul style="list-style-type: none"> • Gestion du mot de passe local et des informations clés du compte utilisateur • Gestion des volumes, y compris les déplacements de volumes • Gestion des quotas, des qtrees, des copies Snapshot et des fichiers • Gestion des LUN • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Surveillance de l'interface réseau • Contrôle de l'état de santé de la SVM
protocole vsadmin	<ul style="list-style-type: none"> • Gestion du mot de passe local et des informations clés du compte utilisateur • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Gestion des LUN • Surveillance de l'interface réseau • Contrôle de l'état de santé de la SVM
sauvegarde vsadmin	<ul style="list-style-type: none"> • Gestion du mot de passe local et des informations clés du compte utilisateur • Gestion des opérations NDMP • Opérations de lecture/écriture d'un volume restauré • Gestion des relations SnapMirror et des copies Snapshot • Affichage des volumes et des informations réseau

vsadmin-snaplock	<ul style="list-style-type: none"> • Gestion du mot de passe local et des informations clés du compte utilisateur • Gestion des volumes, à l'exception des déplacements de volumes • Gestion des quotas, des qtrees, des copies Snapshot et des fichiers • Exécution d'opérations SnapLock, y compris la suppression privilégiée • Configuration des protocoles : NFS et SMB • Configuration des services : DNS, LDAP et NIS • Surveillance des tâches • Surveillance des connexions réseau et de l'interface réseau
vsadmin-readdisponible	<ul style="list-style-type: none"> • Gestion du mot de passe local et des informations clés du compte utilisateur • Contrôle de l'état de santé de la SVM • Surveillance de l'interface réseau • Affichage des volumes et des LUN • Affichage des services et protocoles

Contrôlez l'accès administrateur

Le rôle attribué à un administrateur détermine les fonctions que l'administrateur peut exécuter avec System Manager. Les rôles prédéfinis pour les administrateurs du cluster et des VM de stockage sont fournis par System Manager. Vous attribuez le rôle lorsque vous créez le compte de l'administrateur ou vous pouvez lui attribuer un autre rôle ultérieurement.

En fonction de la manière dont vous avez activé l'accès au compte, vous devrez peut-être effectuer l'une des opérations suivantes :

- Associer une clé publique à un compte local.
- Installez un certificat numérique de serveur signé par une autorité de certification.
- Configuration de l'accès AD, LDAP ou NIS.

Vous pouvez effectuer ces tâches avant ou après l'activation de l'accès au compte.

Attribution d'un rôle à un administrateur

Attribuez un rôle à un administrateur, comme suit :

Étapes


1. Sélectionnez **Cluster > Paramètres**.
2. Sélectionnez ➔ À côté de **utilisateurs et rôles**.

3. Sélectionnez **+ Add** Sous **utilisateurs**.
4. Spécifiez un nom d'utilisateur et sélectionnez un rôle dans le menu déroulant pour **role**.
5. Spécifiez une méthode de connexion et un mot de passe pour l'utilisateur.

Modification du rôle d'un administrateur

Modifiez le rôle d'un administrateur comme suit :

Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Sélectionnez le nom de l'utilisateur dont vous souhaitez modifier le rôle, puis cliquez sur le bouton  s'affiche en regard du nom d'utilisateur.
3. Cliquez sur **Modifier**.
4. Sélectionnez un rôle dans le menu déroulant pour **role**.

Gérez les comptes d'administrateur

Gérer la présentation des comptes d'administrateur

Selon la manière dont vous avez activé l'accès au compte, vous devrez peut-être associer une clé publique à un compte local, installer un certificat numérique de serveur signé par une autorité de certification ou configurer l'accès AD, LDAP ou NIS. Vous pouvez effectuer toutes ces tâches avant ou après l'activation de l'accès au compte.

Associer une clé publique à un compte d'administrateur

Pour l'authentification de clé publique SSH, vous devez associer la clé publique à un compte d'administrateur avant que le compte puisse accéder à la SVM. Vous pouvez utiliser le `security login publickey create` commande permettant d'associer une clé à un compte d'administrateur.

Description de la tâche

Si vous authentifiez un compte via SSH avec un mot de passe et une clé publique SSH, le compte est authentifié d'abord par la clé publique.

Avant de commencer

- Vous devez avoir généré la clé SSH.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Associer une clé publique à un compte d'administrateur :

```
security login publickey create -vserver SVM_name -username user_name -index  
index -publickey certificate -comment comment
```

Pour obtenir la syntaxe complète de la commande, reportez-vous à la fiche de référence de ["Association d'une clé publique à un compte d'utilisateur"](#).

2. Vérifiez la modification en affichant la clé publique :

```
security login publickey show -vserver SVM_name -username user_name -index  
index
```

Exemple

La commande suivante associe une clé publique au compte d'administrateur du SVM `svmadmin1`. Pour la SVM `engData1`. La clé publique est affectée à l'index numéro 5.

```
cluster1::> security login publickey create -vserver engData1 -username  
svmadmin1 -index 5 -publickey  
"<key text>"
```

Gérer les clés publiques SSH et les certificats X.509 pour un compte d'administrateur

Pour une sécurité accrue de l'authentification SSH avec des comptes d'administrateur, vous pouvez utiliser `security login publickey`. Ensemble de commandes pour gérer la clé publique SSH et son association avec les certificats X.509.

Associer une clé publique et un certificat X.509 à un compte d'administrateur

À partir de ONTAP 9.13.1, vous pouvez associer un certificat X.509 à la clé publique que vous associez au compte d'administrateur. Cela vous donne la sécurité supplémentaire des vérifications d'expiration ou de révocation des certificats lors de la connexion SSH à ce compte.

Description de la tâche

Si vous authentifiez un compte via SSH avec une clé publique SSH et un certificat X.509, ONTAP vérifie la validité du certificat X.509 avant de s'authentifier avec la clé publique SSH. La connexion SSH sera refusée si le certificat a expiré ou a été révoqué et la clé publique sera automatiquement désactivée.

Avant de commencer

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Vous devez avoir généré la clé SSH.
- Si vous n'avez besoin que de vérifier l'expiration du certificat X.509, vous pouvez utiliser un certificat auto-signé.
- Si vous avez besoin de vérifier l'expiration et la révocation du certificat X.509 :
 - Vous devez avoir reçu le certificat d'une autorité de certification (CA).
 - Vous devez installer la chaîne de certificats (certificats CA intermédiaire et racine) à l'aide de `security certificate install` commandes.
 - Vous devez activer OCSP pour SSH. Reportez-vous à la section ["Vérifiez que les certificats numériques sont valides à l'aide du protocole OCSP"](#) pour obtenir des instructions.

Étapes

1. Associer une clé publique et un certificat X.509 à un compte d'administrateur :

```
security login publickey create -vserver SVM_name -username user_name -index  
index -publickey certificate -x509-certificate install
```

Pour obtenir la syntaxe complète de la commande, reportez-vous à la fiche de référence de ["Association d'une clé publique à un compte d'utilisateur"](#).

2. Vérifiez la modification en affichant la clé publique :

```
security login publickey show -vserver SVM_name -username user_name -index index
```

Exemple

La commande suivante associe une clé publique et un certificat X.509 au compte d'administrateur du SVM svmin2 Pour la SVM engData2. Le numéro d'index 6 est attribué à la clé publique.

```
cluster1::> security login publickey create -vserver engData2 -username svmin2 -index 6 -publickey "<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

Supprimez l'association de certificat de la clé publique SSH d'un compte d'administrateur

Vous pouvez supprimer l'association de certificat actuelle de la clé publique SSH du compte, tout en conservant la clé publique.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Supprimez l'association de certificat X.509 d'un compte d'administrateur et conservez la clé publique SSH existante :

```
security login publickey modify -vserver SVM_name -username user_name -index index -x509-certificate delete
```

2. Vérifiez la modification en affichant la clé publique :

```
security login publickey show -vserver SVM_name -username user_name -index index
```

Exemple

La commande suivante supprime l'association de certificat X.509 du compte d'administrateur du SVM svmin2 Pour la SVM engData2 au numéro d'index 6.

```
cluster1::> security login publickey modify -vserver engData2 -username svmin2 -index 6 -x509-certificate delete
```

Supprimez la clé publique et l'association de certificat d'un compte d'administrateur

Vous pouvez supprimer la clé publique actuelle et la configuration de certificat d'un compte.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Supprimez la clé publique et une association de certificat X.509 d'un compte d'administrateur :

```
security login publickey delete -vserver SVM_name -username user_name -index index
```

2. Vérifiez la modification en affichant la clé publique :

```
security login publickey show -vserver SVM_name -username user_name -index index
```

Exemple

La commande suivante supprime une clé publique et un certificat X.509 du compte d'administrateur du SVM svmadmin3 Pour la SVM engData3 au numéro d'index 7.

```
cluster1::> security login publickey delete -vserver engData3 -username svmadmin3 -index 7
```

Configurez Cisco Duo 2FA pour les connexions SSH

À partir de ONTAP 9.14.1, vous pouvez configurer ONTAP pour qu'il utilise Cisco Duo pour l'authentification à deux facteurs (2FA) pendant les connexions SSH. Vous configurez Duo au niveau du cluster et il s'applique par défaut à tous les comptes utilisateur. Vous pouvez également configurer Duo au niveau de la machine virtuelle de stockage (anciennement vServer), auquel cas il s'applique uniquement aux utilisateurs de cette machine virtuelle de stockage. Si vous activez et configurez Duo, il sert de méthode d'authentification supplémentaire, en complément des méthodes existantes pour tous les utilisateurs.

Si vous activez l'authentification Duo pour les connexions SSH, les utilisateurs devront inscrire un périphérique lors de leur prochaine connexion à l'aide de SSH. Pour plus d'informations sur l'inscription, reportez-vous au Cisco Duo ["documentation d'inscription"](#).

Vous pouvez utiliser l'interface de ligne de commande ONTAP pour effectuer les tâches suivantes avec Cisco Duo :

- [Configurez Cisco Duo](#)
- [Modifier la configuration Cisco Duo](#)
- [Supprimez la configuration Cisco Duo](#)
- [Afficher la configuration Cisco Duo](#)
- [Supprimer un groupe Duo](#)

- [Afficher les groupes Duo](#)
- [Contourner l'authentification Duo pour les utilisateurs](#)

Configurez Cisco Duo

Vous pouvez créer une configuration Cisco Duo pour l'ensemble du cluster ou pour une VM de stockage spécifique (appelée vServer dans l'interface de ligne de commande ONTAP) à l'aide de `security login duo create` commande. Dans ce cas, Cisco Duo est activé pour les connexions SSH pour ce cluster ou cette machine virtuelle de stockage.

Étapes

1. Connectez-vous au panneau d'administration Cisco Duo.
2. Accédez à **applications > application UNIX**.
3. Enregistrez votre clé d'intégration, votre clé secrète et le nom d'hôte de l'API.
4. Connectez-vous à votre compte ONTAP à l'aide de SSH.
5. Activez l'authentification Cisco Duo pour cette machine virtuelle de stockage, en remplaçant les informations de votre environnement par les valeurs entre parenthèses :

```
security login duo create \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME>
```

Pour plus d'informations sur les paramètres requis et facultatifs pour cette commande, reportez-vous à la section ["Feuilles de calcul pour l'authentification de l'administrateur et la configuration du RBAC"](#).

Modifier la configuration Cisco Duo

Vous pouvez modifier la façon dont Cisco Duo authentifie les utilisateurs (par exemple, le nombre d'invites d'authentification données ou le proxy HTTP utilisé). Si vous devez modifier la configuration Cisco Duo pour une machine virtuelle de stockage (appelée vServer dans l'interface de ligne de commande ONTAP), vous pouvez utiliser `security login duo modify` commande.

Étapes

1. Connectez-vous au panneau d'administration Cisco Duo.
2. Accédez à **applications > application UNIX**.
3. Enregistrez votre clé d'intégration, votre clé secrète et le nom d'hôte de l'API.
4. Connectez-vous à votre compte ONTAP à l'aide de SSH.
5. Modifiez la configuration Cisco Duo pour cette machine virtuelle de stockage en remplaçant les informations mises à jour de votre environnement par les valeurs entre parenthèses :

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-prompts 1|2|3 \
-max-unenrolled-logins <NUM_LOGINS> \
-is-enabled true|false \
-fail-mode safe|secure
```

Supprimez la configuration Cisco Duo

Vous pouvez supprimer la configuration Cisco Duo, ce qui supprime la nécessité pour les utilisateurs SSH de s'authentifier à l'aide de Duo lors de la connexion. Pour supprimer la configuration Cisco Duo d'une machine virtuelle de stockage (appelée vServer dans l'interface de ligne de commande ONTAP), vous pouvez utiliser `security login duo delete` commande.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Supprimez la configuration Cisco Duo pour cette machine virtuelle de stockage, en remplaçant le nom de votre machine virtuelle de stockage par `<STORAGE_VM_NAME>`:

```
security login duo delete -vserver <STORAGE_VM_NAME>
```

Cette opération supprime définitivement la configuration Cisco Duo pour cette machine virtuelle de stockage.

Afficher la configuration Cisco Duo

Vous pouvez afficher la configuration Cisco Duo existante pour une machine virtuelle de stockage (appelée vServer dans l'interface de ligne de commande ONTAP) à l'aide de `security login duo show` commande.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Affiche la configuration Cisco Duo pour cette machine virtuelle de stockage. Si vous le souhaitez, vous pouvez utiliser le `vserver` Paramètre permettant de spécifier une machine virtuelle de stockage, en remplaçant le nom de la machine virtuelle de stockage par `<STORAGE_VM_NAME>`:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

Vous devez voir les résultats similaires à ce qui suit :

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

Créez un groupe Duo

Vous pouvez demander à Cisco Duo d'inclure uniquement les utilisateurs d'un certain groupe d'utilisateurs Active Directory, LDAP ou local dans le processus d'authentification Duo. Si vous créez un groupe Duo, seuls les utilisateurs de ce groupe sont invités à s'authentifier Duo. Vous pouvez créer un groupe Duo à l'aide du `security login duo group create` commande. Lorsque vous créez un groupe, vous pouvez exclure certains utilisateurs de ce groupe du processus d'authentification Duo.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Créez le groupe Duo en remplaçant les informations de votre environnement par les valeurs entre parenthèses. Si vous omettez le `-vserver` le groupe est créé au niveau du cluster :

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local. Utilisateurs que vous spécifiez avec le facultatif `-exclude-users` Le paramètre ne sera pas inclus dans le processus d'authentification Duo.

Afficher les groupes Duo

Vous pouvez afficher les entrées de groupe Cisco Duo existantes à l'aide du `security login duo group show` commande.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Affichez les entrées du groupe Duo, en remplaçant les informations de votre environnement par les valeurs entre parenthèses. Si vous omettez le `-vserver` paramètre, le groupe s'affiche au niveau du cluster :

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME> -exclude-users <USER1, USER2>
```

Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local. Utilisateurs que vous spécifiez avec le facultatif `-exclude-users` le paramètre ne s'affiche pas.

Supprimer un groupe Duo

Vous pouvez supprimer une entrée de groupe Duo à l'aide du `security login duo group delete` commande. Si vous supprimez un groupe, les utilisateurs de ce groupe ne sont plus inclus dans le processus d'authentification Duo.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Supprimez l'entrée de groupe Duo, en remplaçant les informations de votre environnement par les valeurs entre parenthèses. Si vous omettez le `-vserver` paramètre, le groupe est supprimé au niveau du cluster :

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME>
```

Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local.

Contourner l'authentification Duo pour les utilisateurs

Vous pouvez exclure tous les utilisateurs ou des utilisateurs spécifiques du processus d'authentification Duo SSH.

Exclure tous les utilisateurs Duo

Vous pouvez désactiver l'authentification SSH Cisco Duo pour tous les utilisateurs.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Désactivez l'authentification Cisco Duo pour les utilisateurs SSH en remplaçant le nom du vServer par `<STORAGE_VM_NAME>`:

```
security login duo -vserver <STORAGE_VM_NAME> -is-duo-enabled-false
```

Exclure les utilisateurs du groupe Duo

Vous pouvez exclure certains utilisateurs faisant partie d'un groupe Duo du processus d'authentification Duo SSH.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.

2. Désactivez l'authentification Cisco Duo pour des utilisateurs spécifiques d'un groupe. Remplacez le nom du groupe et la liste des utilisateurs à exclure par les valeurs entre parenthèses :

```
security login group modify -group-name <GROUP_NAME> -exclude-users  
<USER1, USER2>
```

Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local. Utilisateurs que vous spécifiez avec `-exclude-users` Le paramètre ne sera pas inclus dans le processus d'authentification Duo.

Exclure les utilisateurs Duo locaux

Vous pouvez exclure certains utilisateurs locaux de l'authentification Duo à l'aide du panneau d'administration Cisco Duo. Pour obtenir des instructions, reportez-vous au "[Documentation Cisco Duo](#)".

Générer et installer un certificat de serveur signé par une autorité de certification

Sur les systèmes de production, il est recommandé d'installer un certificat numérique signé par une autorité de certification pour l'authentification du cluster ou d'un SVM en tant que serveur SSL. Vous pouvez utiliser le `security certificate generate-csr` Commande pour générer une requête de signature de certificat (CSR) et le `security certificate install` commande permettant d'installer le certificat que vous recevez de l'autorité de certification.

Générer une demande de signature de certificat

Vous pouvez utiliser le `security certificate generate-csr` Commande pour générer une requête de signature de certificat (CSR). Après le traitement de votre demande, l'autorité de certification vous envoie le certificat numérique signé.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Générer une RSC :

```
security certificate generate-csr -common-name FQDN_or_common_name -size  
512|1024|1536|2048 -country country -state state -locality locality  
-organization organization -unit unit -email-addr email_of_contact -hash  
-function SHA1|SHA256|MD5
```

La commande suivante crée une CSR avec une clé privée 2048 bits générée par la fonction de hachage « 'S ra256' » à l'usage du groupe « logiciels » dans le département « IT » d'une entreprise dont le nom commun personnalisé est « `erver1.companyname.com` », situé à Sunnyvale, en Californie, aux États-Unis. L'adresse e-mail de l'administrateur du contact du SVM est « [web@example.com](#) ». Le système affiche la RSC et la clé privée dans la sortie.

Exemple de création d'une RSC

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
```

Certificate Signing Request :

-----BEGIN CERTIFICATE REQUEST-----

```
MIIBGjCBxQIBADBgMRQWEgYDVQQDEwtleGFtcGxlLmNvbTELMakGA1UEBhMCVVMx
CTAHBgNVBAgTADAEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBcWUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Private Key :

-----BEGIN RSA PRIVATE KEY-----

```
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+jlhrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
```

Note: Please keep a copy of your certificate request and private key for future reference.

2. Copiez la demande de certificat à partir de la sortie CSR et envoyez-la sous forme électronique (par exemple un courriel) à une autorité de certification tierce approuvée pour signature.

Après le traitement de votre demande, l'AC vous envoie le certificat numérique signé. Vous devez conserver une copie de la clé privée et du certificat numérique signé par l'autorité de certification.

Installez un certificat de serveur signé par une autorité de certification

Vous pouvez utiliser le `security certificate install` Commande permettant d'installer un certificat de serveur signé par une autorité de certification sur un SVM. ONTAP vous invite à entrer les certificats racine et intermédiaire de l'autorité de certification (CA) qui forment la chaîne de certificats du certificat du serveur.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étape

1. Installer un certificat de serveur signé par une autorité de certification :

```
security certificate install -vserver SVM_name -type certificate_type
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).



ONTAP vous invite à entrer les certificats racine et intermédiaire de l'autorité de certification qui constituent la chaîne de certificats du certificat du serveur. La chaîne commence par le certificat de l'autorité de certification qui a émis le certificat du serveur et peut atteindre le certificat racine de l'autorité de certification. Tout certificat intermédiaire manquant entraîne l'échec de l'installation du certificat du serveur.

La commande suivante installe le certificat de serveur signé par l'autorité de certification et les certificats intermédiaires sur SVM « engData2 ».

Exemple d'installation de certificats intermédiaires de certificat de serveur signés par une autorité de certification

```
cluster1::>security certificate install -vserver engData2 -type
server
```

Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----

```
MIIB8TCCA ZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTAD EJMAcGA1UECXMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTAD EJMAcGA1UECXMAM
Q8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIaKEAyXrK2sry
-----END CERTIFICATE-----
```

Please enter Private Key: Press <Enter> when done

-----BEGIN RSA PRIVATE KEY-----

```
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvF
C6lX2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM70tbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJ
z7UCIQDr8d3gOG7lUyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrFYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAZt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
```

-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----

```
MIIE+zCCBGSGAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwwgbsxJDAiBgNVBACGTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbGlDZXJ0IENsYXNzIDIGUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFOwYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFROZSBHbyBE
YWRkeSBHcm9lcCwgSW5jLjExMC8GA1UECXMOR28gRGFkZkhkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwbgsxJDAiBgNVBACGTG1ZhbG1DZXJ0
IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIgUG9saWN5IFZhbG1kYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDEzhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTE5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBACGTG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENs
YXNzIDIgUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEzhodHRw
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital certificate for future reference.

Gérer les certificats avec System Manager

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour gérer les autorités de certification de confiance, les certificats client/serveur et les autorités de certification locales (intégrées).

Avec System Manager, vous pouvez gérer les certificats reçus d'autres applications afin de pouvoir authentifier les communications de ces applications. Vous pouvez également gérer vos propres certificats qui identifient votre système à d'autres applications.

Afficher les informations sur le certificat

System Manager vous permet d'afficher les autorités de certification approuvées, les certificats client/serveur et les autorités de certification locales stockées sur le cluster.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Faites défiler jusqu'à la zone **sécurité**.
Dans la section **certificats**, les détails suivants sont affichés :
 - Le nombre d'autorités de certification stockées approuvées.
 - Nombre de certificats client/serveur stockés.
 - Le nombre d'autorités de certification locales stockées.
3. Sélectionnez n'importe quel nombre pour afficher les détails d'une catégorie de certificats ou sélectionnez  Pour ouvrir la page **certificats**, qui contient des informations sur toutes les catégories.
La liste affiche les informations relatives à l'ensemble du cluster. Pour afficher les informations relatives à une seule machine virtuelle de stockage spécifique, effectuez les opérations suivantes :
 - a. Sélectionnez **stockage > machines virtuelles de stockage**.

- b. Sélectionnez la VM de stockage.
- c. Passez à l'onglet **Paramètres**.
- d. Sélectionnez un numéro affiché dans la section **certificat**.

Que faire ensuite

- À partir de la page **certificats**, vous pouvez [Générer une demande de signature de certificat](#).
- Les informations de certificat sont séparées en trois onglets, un pour chaque catégorie. Vous pouvez effectuer les tâches suivantes à partir de chaque onglet :

Dans cet onglet...	Vous pouvez effectuer ces procédures...
Autorités de certification approuvées	<ul style="list-style-type: none"> • [install-trusted-cert] • Supprimer une autorité de certification approuvée • Renouvelez une autorité de certification approuvée
Certificats client/serveur	<ul style="list-style-type: none"> • [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
Autorités locales de certification	<ul style="list-style-type: none"> • Créez une autorité de certification locale • Signer un certificat à l'aide d'une autorité de certification locale • Supprimer une autorité de certification locale • Renouvelez une autorité de certification locale

Générer une demande de signature de certificat

Vous pouvez générer une demande de signature de certificat (CSR) avec System Manager à partir de n'importe quel onglet de la page **certificats**. Une clé privée et une RSC correspondante sont générées, qui peuvent être signées à l'aide d'une autorité de certification pour générer un certificat public.

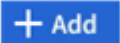
Étapes

1. Consultez la page **certificats**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez **+Generate CSR**.
3. Renseignez les informations relatives au nom du sujet :
 - a. Saisissez un **nom commun**.
 - b. Sélectionnez un **pays**.
 - c. Saisissez une **organisation**.
 - d. Entrez une **unité d'organisation**.
4. Si vous souhaitez remplacer les valeurs par défaut, sélectionnez **plus d'options** et fournissez des informations supplémentaires.

Installez (ajoutez) une autorité de certification approuvée

Vous pouvez installer des autorités de certification approuvées supplémentaires dans System Manager.

Étapes

1. Affichez l'onglet **autorités de certification approuvées**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez .
3. Dans le panneau **Ajouter une autorité de certification approuvée**, effectuez les opérations suivantes :
 - Saisissez un **nom**.
 - Pour le **scope**, sélectionnez une VM de stockage.
 - Saisissez un **nom commun**.
 - Sélectionnez un **type**.
 - Entrez ou importez **détails du certificat**.


Supprimer une autorité de certification approuvée

Avec System Manager, vous pouvez supprimer une autorité de certification approuvée.



Vous ne pouvez pas supprimer les autorités de certification approuvées préinstallées avec ONTAP.

Étapes

1. Affichez l'onglet **autorités de certification approuvées**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom de l'autorité de certification approuvée.
3. Sélectionnez  En regard du nom, puis sélectionnez **Supprimer**.

Renouvelez une autorité de certification approuvée

Avec System Manager, vous pouvez renouveler une autorité de certification de confiance qui a expiré ou est sur le point d'expirer.

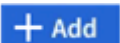
Étapes

1. Affichez l'onglet **autorités de certification approuvées**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom de l'autorité de certification approuvée.
3. Sélectionnez  En regard du nom du certificat, puis **Renew**.

Installez (ajoutez) un certificat client/serveur

System Manager vous permet d'installer des certificats client/serveur supplémentaires.

Étapes

1. Affichez l'onglet **certificats client/serveur**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez .
3. Sur le panneau **Ajouter un certificat client/serveur**, effectuez les opérations suivantes :
 - Saisissez un **nom de certificat**.

- Pour le **scope**, sélectionnez une VM de stockage.
- Saisissez un **nom commun**.
- Sélectionnez un **type**.
- Entrez ou importez **détails du certificat**.
Vous pouvez écrire ou copier et coller les détails du certificat à partir d'un fichier texte ou importer le texte d'un fichier de certificat en cliquant sur **Importer**.
- Entrez la **clé privée**.
Vous pouvez écrire ou copier et coller la clé privée à partir d'un fichier texte ou importer le texte d'un fichier de clé privée en cliquant sur **Importer**.

Générer (ajouter) un certificat client/serveur auto-signé

System Manager vous permet de générer des certificats client/serveur autosignés supplémentaires.


Étapes

1. Afficher l'onglet **certificats client/serveur**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez **+générer un certificat auto-signé**.
3. Dans le panneau **générer un certificat auto-signé**, effectuez les opérations suivantes :
 - Saisissez un **nom de certificat**.
 - Pour le **scope**, sélectionnez une VM de stockage.
 - Saisissez un **nom commun**.
 - Sélectionnez un **type**.
 - Sélectionnez une fonction **hachage**.
 - Sélectionnez un **taille de clé**.
 - Sélectionnez une **VM de stockage**.

Supprimer un certificat client/serveur

Avec System Manager, vous pouvez supprimer les certificats client/serveur.


Étapes

1. Afficher l'onglet **certificats client/serveur**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom du certificat client/serveur.
3. Sélectionnez  En regard du nom, cliquez sur **Supprimer**.

Renouveler un certificat client/serveur

Avec System Manager, vous pouvez renouveler un certificat client/serveur qui a expiré ou est sur le point d'expirer.

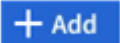
Étapes

1. Afficher l'onglet **certificats client/serveur**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom du certificat client/serveur.
3. Sélectionnez  En regard du nom, cliquez sur **renouveler**.

Créer une autorité de certification locale

Avec System Manager, vous pouvez créer une nouvelle autorité de certification locale.

Étapes

1. Affichez l'onglet **autorités locales de certification**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez  **Add**.
3. Dans le panneau **Ajouter une autorité de certification locale**, effectuez les opérations suivantes :
 - Saisissez un **nom**.
 - Pour le **scope**, sélectionnez une VM de stockage.
 - Saisissez un **nom commun**.
4. Si vous souhaitez remplacer les valeurs par défaut, sélectionnez **plus d'options** et fournissez des informations supplémentaires.

Signer un certificat à l'aide d'une autorité de certification locale

Dans System Manager, vous pouvez signer un certificat à l'aide d'une autorité de certification locale.


Étapes

1. Affichez l'onglet **autorités locales de certification**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom de l'autorité de certification locale.
3. Sélectionnez  En regard du nom, **signer un certificat**.
4. Remplissez le formulaire **signer une demande de signature de certificat**.
 - Vous pouvez coller le contenu de la signature de certificat ou importer un fichier de demande de signature de certificat en cliquant sur **Importer**.
 - Indiquez le nombre de jours pendant lesquels le certificat sera valide.

Supprimer une autorité de certification locale

Avec System Manager, vous pouvez supprimer une autorité de certification locale.


Étapes

1. Affichez l'onglet **local Certificate Authority**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom de l'autorité de certification locale.
3. Sélectionnez  À côté du nom, puis **Supprimer**.

Renouvelez une autorité de certification locale

Avec System Manager, vous pouvez renouveler une autorité de certification locale qui a expiré ou est sur le point d'expirer.

Étapes

1. Affichez l'onglet **local Certificate Authority**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom de l'autorité de certification locale.
3. Sélectionnez  En regard du nom, cliquez sur **renouveler**.

Présentation de la configuration de l'accès au contrôleur de domaine Active Directory

Vous devez configurer l'accès du contrôleur AD domain au cluster ou au SVM avant qu'un compte AD ne puisse accéder au SVM. Si vous avez déjà configuré un serveur SMB pour un SVM de données, vous pouvez configurer le SVM en tant que passerelle, ou *tunnel*, pour l'accès AD au cluster. Si vous n'avez pas configuré de serveur SMB, vous pouvez créer un compte ordinateur pour le SVM sur le domaine AD.

ONTAP prend en charge les services d'authentification de contrôleur de domaine suivants :

- Kerberos
- LDAP
- NETLOGON
- Autorité de sécurité locale (LSA)

ONTAP prend en charge les algorithmes de clé de session suivants pour les connexions Netlogon sécurisées :

Algorithme de clé de session	Disponible à partir de...
HMAC-SHA256, basé sur la norme AES (Advanced Encryption Standard) Si votre cluster exécute ONTAP 9.9.1 ou une version antérieure et que votre contrôleur de domaine applique AES pour des services Netlogon sécurisés, la connexion échoue. Dans ce cas, vous devez reconfigurer votre contrôleur de domaine pour accepter les connexions par clé forte avec ONTAP.	ONTAP 9.10.1
DES et HMAC-MD5 (lorsque la clé est réglée)	Toutes les versions d'ONTAP 9

Si vous souhaitez utiliser les clés de session AES lors de l'établissement d'un canal sécurisé Netlogon, vous devez vérifier que AES est activé sur votre SVM.

- Depuis ONTAP 9.14.1, AES est activé par défaut lorsque vous créez un SVM, et vous n'avez pas besoin de modifier les paramètres de sécurité de votre SVM pour utiliser des clés de session AES lors de l'établissement de canaux sécurisés Netlogon.
- Dans ONTAP 9.10.1 à 9.13.1, AES est désactivé par défaut lors de la création d'un SVM. Vous devez activer AES à l'aide de la commande suivante :

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```



Lorsque vous effectuez une mise à niveau vers ONTAP 9.14.1 ou une version ultérieure, le paramètre AES des SVM existants créés avec les anciennes versions de ONTAP ne changera pas automatiquement. Vous devez toujours mettre à jour la valeur de ce paramètre pour activer les AES sur ces SVM.

Configurer un tunnel d'authentification

Si vous avez déjà configuré un serveur SMB pour un SVM de données, vous pouvez utiliser le `security login domain-tunnel create` Commande permettant de configurer le SVM en tant que passerelle ou *tunnel*, pour l'accès AD au cluster.

Avant de commencer

- Un serveur SMB doit être configuré pour un SVM de données.
- Vous devez avoir activé un compte utilisateur AD domain pour accéder au SVM admin pour le cluster.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.

Depuis ONTAP 9.10.1, si vous disposez d'une passerelle SVM (tunnel du domaine) pour l'accès AD, vous pouvez utiliser Kerberos pour l'authentification admin si vous avez désactivé NTLM dans votre domaine AD. Dans les versions précédentes, Kerberos n'était pas pris en charge par l'authentification admin pour les passerelles SVM. Cette fonctionnalité est disponible par défaut ; aucune configuration n'est requise.



L'authentification Kerberos a toujours été tentée en premier. En cas d'échec, l'authentification NTLM est alors tentée.

Étape

1. Configurer un SVM de données compatible SMB en tant que tunnel d'authentification pour l'accès au contrôleur de domaine AD au cluster :

```
security login domain-tunnel create -vserver svm_name
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).



Le SVM doit être exécuté pour que l'utilisateur puisse être authentifié.

La commande suivante configure le SVM de données SMB « engData » comme un tunnel d'authentification.

```
cluster1::>security login domain-tunnel create -vserver engData
```

Créer un compte SVM Computer sur le domaine

Si vous n'avez pas configuré de serveur SMB pour un SVM de données, vous pouvez utiliser le `vserver active-directory create` Commande pour créer un compte ordinateur pour le SVM sur le domaine.

Description de la tâche

Une fois que vous avez saisi le `vserver active-directory create` Vous êtes invité à fournir les informations d'identification d'un compte utilisateur AD avec suffisamment de privilèges pour ajouter des ordinateurs à l'unité organisationnelle spécifiée dans le domaine. Le mot de passe du compte ne peut pas être vide.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étape

1. Créer un compte ordinateur pour un SVM sur le domaine AD :

```
vserver active-directory create -vserver SVM_name -account-name  
NetBIOS_account_name -domain domain -ou organizational_unit
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

La commande suivante crée un compte ordinateur nommé « ADSERVER1 » sur le domaine « example.com » pour SVM « engData ». Une fois la commande saisie, vous êtes invité à saisir les informations d'identification du compte utilisateur AD.

```
cluster1::>vserver active-directory create -vserver engData -account  
-name ADSERVER1 -domain example.com
```

In order to create an Active Directory machine account, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "example.com" domain.

Enter the user name: Administrator

Enter the password:

Configuration de la présentation de l'accès aux serveurs LDAP ou NIS

Vous devez configurer l'accès des serveurs LDAP ou NIS à un SVM pour que les comptes LDAP ou NIS puissent accéder au SVM. La fonction de commutation vous permet d'utiliser LDAP ou NIS comme sources de service de noms alternatifs.

Configurez l'accès au serveur LDAP

Vous devez configurer l'accès des serveurs LDAP à une SVM avant que les comptes LDAP ne puissent accéder à la SVM. Vous pouvez utiliser le `vserver services name-service ldap client create` Commande permettant de créer une configuration client LDAP sur le SVM. Vous pouvez ensuite utiliser le `vserver services name-service ldap create` Commande permettant d'associer la configuration client LDAP à la SVM.

Description de la tâche

La plupart des serveurs LDAP peuvent utiliser les schémas par défaut fournis par ONTAP :

- MS-AD-BIS (schéma préféré pour la plupart des serveurs AD Windows 2012 et versions ultérieures)
- AD-IDMU (serveurs AD Windows 2008, Windows 2016 et versions ultérieures)
- AD-SFU (serveurs AD Windows 2003 et versions antérieures)
- RFC-2307 (SERVEURS LDAP UNIX)

Il est préférable d'utiliser les schémas par défaut à moins qu'il n'y ait une obligation de faire autrement. Si c'est le cas, vous pouvez créer votre propre schéma en copiant un schéma par défaut et en modifiant la copie. Pour plus d'informations, voir :

- ["Configuration NFS"](#)
- ["Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP"](#)

Avant de commencer

- Vous devez avoir installé un ["Certificat numérique de serveur signé CA"](#) Sur le SVM.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Créer une configuration client LDAP sur un SVM :

```
vserver services name-service ldap client create -vserver SVM_name -client
-config client_configuration -servers LDAP_server_IPs -schema schema -use
-start-tls true|false
```



Le démarrage de TLS est pris en charge uniquement pour l'accès aux SVM de données. Il n'est pas pris en charge pour l'accès aux SVM d'administration.

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

La commande suivante crée une configuration client LDAP nommée « corp » sur le SVM « engData ». Le client établit des liaisons anonymes vers les serveurs LDAP avec les adresses IP 172.160.0.100 et 172.16.0.101. Le client utilise le schéma RFC-2307 pour effectuer des requêtes LDAP. La communication entre le client et le serveur est cryptée à l'aide de Start TLS.

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```



À partir de ONTAP 9.2, le champ `-ldap-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur LDAP.

2. Associer la configuration client LDAP au SVM :

```
vserver services name-service ldap create
-vserver SVM_name -client-config client_configuration -client-enabled
true|false
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

La commande suivante associe la configuration du client LDAP corp Avec la SVM engData, Et active le client LDAP sur la SVM.

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```



À partir de ONTAP 9.2, le `vserver services name-service ldap create` Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP n'est pas en mesure de contacter le serveur de noms.

3. Valider le statut des serveurs name en utilisant la commande `vserver services name-service ldap check`.

La commande suivante valide les serveurs LDAP sur le SVM vs 0.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                     |
| Client Configuration Name: c1                     |
| LDAP Status: up                                   |
| LDAP Status Details: Successfully connected to LDAP server |
| "10.11.12.13".                                   |
```

La commande `name service check` est disponible à partir de ONTAP 9.2.

Configurer l'accès au serveur NIS

Vous devez configurer l'accès du serveur NIS à un SVM pour que les comptes NIS puissent accéder au SVM. Vous pouvez utiliser le `vserver services name-service nis-domain create` Commande permettant de créer une configuration de domaine NIS sur un SVM

Description de la tâche

Vous pouvez créer plusieurs domaines NIS. Un seul domaine NIS peut être défini sur `active` à la fois.

Avant de commencer

- Tous les serveurs configurés doivent être disponibles et accessibles avant de configurer le domaine NIS sur le SVM.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étape

1. Créer une configuration de domaine NIS sur un SVM :

```
vserver services name-service nis-domain create -vserver SVM_name -domain
client_configuration -active true|false -nis-servers NIS_server_IPs
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).



À partir de ONTAP 9.2, le champ `-nis-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur NIS.

La commande suivante crée une configuration de domaine NIS sur SVM « engData ». Domaine NIS `nisdomain` Est actif lors de la création et communique avec un serveur NIS avec l'adresse IP `192.0.2.180`.

```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
```

Créer un commutateur de service de nom

La fonction de changement de service de noms vous permet d'utiliser LDAP ou NIS comme sources de service de noms alternatifs. Vous pouvez utiliser le `vserver services name-service ns-switch modify` commande permettant de spécifier l'ordre de recherche des sources de service de noms.

Avant de commencer

- Vous devez avoir configuré l'accès aux serveurs LDAP et NIS.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou un administrateur SVM.

Étape

1. Spécifiez l'ordre de recherche des sources de service de noms :

```
vserver services name-service ns-switch modify -vserver SVM_name -database  
name_service_switch_database -sources name_service_source_order
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

La commande suivante spécifie l'ordre de recherche des sources de service de noms LDAP et NIS pour la base de données « passwd » sur SVM « engData ».

```
cluster1::>vserver services name-service ns-switch  
modify -vserver engData -database passwd -source files ldap,nis
```

Modifier un mot de passe administrateur

Vous devez modifier votre mot de passe initial immédiatement après la première connexion au système. Si vous êtes un administrateur de SVM, vous pouvez utiliser `security login password` commande permettant de modifier votre propre mot de passe. Si vous êtes administrateur de cluster, vous pouvez utiliser `security login password` pour modifier le mot de passe d'un administrateur.

Description de la tâche

Le nouveau mot de passe doit respecter les règles suivantes :

- Il ne peut pas contenir le nom d'utilisateur
- Elle doit comporter au moins huit caractères
- Il doit contenir au moins une lettre et un chiffre
- Il ne peut pas être le même que les six derniers mots de passe



Vous pouvez utiliser le `security login role config modify` commande permettant de modifier les règles de mot de passe des comptes associés à un rôle donné. Pour plus d'informations, reportez-vous à la section ["référence de commande"](#).

Avant de commencer

- Vous devez être un administrateur de cluster ou de SVM pour modifier votre propre mot de passe.
- Vous devez être un administrateur de cluster pour modifier le mot de passe d'un autre administrateur.

Étape

1. Modifier un mot de passe d'administrateur : `security login password -vserver svm_name -username user_name`

La commande suivante permet de modifier le mot de passe de l'administrateur `admin1` Pour la SVM `vs1.example.com`. Vous êtes invité à saisir le mot de passe actuel, puis à saisir de nouveau le nouveau mot de passe.

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

Verrouiller et déverrouiller un compte administrateur

Vous pouvez utiliser le `security login lock` commande permettant de verrouiller un compte d'administrateur, et le `security login unlock` commande pour déverrouiller le compte.

Avant de commencer

Pour effectuer ces tâches, vous devez être un administrateur de cluster.

Étapes

1. Verrouiller un compte administrateur :

```
security login lock -vserver SVM_name -username user_name
```

La commande suivante verrouille le compte administrateur `admin1` Pour la SVM `vs1.example.com`:

```
cluster1::>security login lock -vserver engData -username admin1
```

2. Déverrouiller un compte administrateur :

```
security login unlock -vserver SVM_name -username user_name
```

La commande suivante déverrouille le compte administrateur `admin1` Pour la SVM `vs1.example.com`:

```
cluster1::>security login unlock -vserver engData -username admin1
```

La gestion des tentatives de connexion a échoué

Les tentatives répétées de connexion échouées indiquent parfois qu'un intrus tente d'accéder au système de stockage. Vous pouvez prendre plusieurs mesures pour vous assurer qu'une intrusion n'a pas lieu.

Comment savoir que les tentatives de connexion ont échoué

Le système de gestion des événements (EMS) vous informe de l'échec des tentatives de connexion toutes les heures. Vous pouvez trouver un enregistrement des tentatives de connexion échouées dans le `audit.log` fichier.

Que faire en cas d'échec des tentatives de connexion répétées

À court terme, vous pouvez prendre plusieurs mesures pour éviter une intrusion :

- Exiger que les mots de passe soient composés d'un nombre minimum de caractères majuscules, de minuscules, de caractères spéciaux et/ou de chiffres
- Imposer un délai après une tentative de connexion échouée
- Limitez le nombre de tentatives de connexion ayant échoué autorisées et verrouillez les utilisateurs après le nombre spécifié de tentatives ayant échoué
- Expire et verrouille les comptes inactifs pendant un nombre de jours spécifié

Vous pouvez utiliser le `security login role config modify` pour effectuer ces tâches.

Sur le long terme, vous pouvez prendre les mesures suivantes :

- Utilisez le `security ssh modify` Commande pour limiter le nombre de tentatives de connexion ayant échoué pour tous les SVM nouvellement créés.
- Migrez les comptes d'algorithme MD5 existants vers l'algorithme SHA-512 plus sécurisé en exigeant des utilisateurs de modifier leurs mots de passe.

Appliquer SHA-2 sur les mots de passe du compte d'administrateur

Les comptes d'administrateur créés avant ONTAP 9.0 continuent d'utiliser des mots de passe MD5 après la mise à niveau, jusqu'à ce que les mots de passe soient changés manuellement. MD5 est moins sécurisé que SHA-2. Par conséquent, après la mise à niveau, vous devez inviter les utilisateurs de comptes MD5 à modifier leurs mots de passe pour utiliser la fonction de hachage SHA-512 par défaut.

Description de la tâche

La fonctionnalité de hachage du mot de passe vous permet d'effectuer les opérations suivantes :

- Affiche les comptes utilisateur correspondant à la fonction de hachage spécifiée.
- Expire les comptes qui utilisent une fonction de hachage spécifiée (par exemple MD5), forçant les utilisateurs à modifier leurs mots de passe lors de leur prochaine connexion.
- Verrouiller les comptes dont les mots de passe utilisent la fonction de hachage spécifiée.
- Pour revenir à une version antérieure à ONTAP 9, réinitialisez le mot de passe de l'administrateur du cluster afin qu'il soit compatible avec la fonction de hachage (MD5) prise en charge par la version précédente.

ONTAP n'accepte que les mots de passe SHA-2 pré-hachés à l'aide du SDK de gestion NetApp (`security-login-create` et `security-login-modify-password`).

Étapes

1. Migrez les comptes administrateur MD5 vers la fonction de hachage SHA-512 :

- a. Expire tous les comptes administrateur MD5 : `security login expire-password -vserver * -username * -hash-function md5`

Cela oblige les utilisateurs de compte MD5 à changer leurs mots de passe lors de la prochaine connexion.

- b. Demandez aux utilisateurs de comptes MD5 de se connecter par le biais d'une console ou d'une session SSH.

Le système détecte que les comptes ont expiré et invite les utilisateurs à modifier leur mot de passe. SHA-512 est utilisé par défaut pour les mots de passe modifiés.

2. Pour les comptes MD5 dont les utilisateurs ne se connectent pas pour modifier leurs mots de passe dans un délai donné, forcez la migration du compte :

- a. Verrouiller les comptes qui utilisent toujours la fonction de hachage MD5 (niveau de privilège avancé) :
`security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`


Après le nombre de jours spécifié par `-lock-after`, Les utilisateurs ne peuvent pas accéder à leurs comptes MD5.

- b. Déverrouillez les comptes lorsque les utilisateurs sont prêts à modifier leur mot de passe : `security login unlock -vserver svm_name -username user_name`


- c. Demandez aux utilisateurs de se connecter à leurs comptes via une console ou une session SSH et de modifier leur mot de passe lorsque le système les invite à le faire.

Diagnostiquer et corriger les problèmes d'accès aux fichiers

Étapes

1. Dans System Manager, sélectionnez **stockage > machines virtuelles de stockage**.
2. Sélectionnez la VM de stockage sur laquelle vous souhaitez effectuer un suivi.
3. Cliquez sur  **Plus**.
4. Cliquez sur **Trace File Access**.
5. Indiquez le nom d'utilisateur et l'adresse IP du client, puis cliquez sur **Start Tracing**.

Les résultats de la trace s'affichent dans un tableau. La colonne **motifs** indique la raison pour laquelle un fichier n'a pas pu être accédé.

6. Cliquez sur  dans la colonne de gauche du tableau de résultats pour afficher les autorisations d'accès aux fichiers.

Gestion de la vérification multi-administrateurs

Présentation de la vérification multi-administrateur

Depuis ONTAP 9.11.1, vous pouvez utiliser la vérification multi-administration (MAV) pour vous assurer que certaines opérations, telles que la suppression de volumes ou de copies Snapshot, ne peuvent être exécutées qu'après approbation d'administrateurs désignés. Cela empêche les administrateurs compromis, malveillants ou peu expérimentés d'effectuer des modifications ou de supprimer des données indésirables.

La configuration de la vérification multi-administrateurs comprend :

- ["Création d'un ou plusieurs groupes d'approbation administrateur."](#)
- ["Activation de la fonctionnalité de vérification multi-administrateurs."](#)
- ["Ajout ou modification de règles."](#)

Après la configuration initiale, ces éléments ne peuvent être modifiés que par les administrateurs d'un groupe d'approbation MAV (administrateurs MAV).

Lorsque la vérification multi-administrateur est activée, chaque opération protégée nécessite trois étapes :

- Lorsqu'un utilisateur lance l'opération, un ["la demande a été générée."](#)
- Avant de pouvoir être exécuté, au moins un ["L'administrateur MAV doit approuver."](#)
- Après approbation, l'utilisateur termine l'opération.

La vérification multi-administrateurs n'est pas destinée aux volumes ou aux flux de travail nécessitant une automatisation élevée, car chaque tâche automatisée nécessite une approbation avant que l'opération ne puisse être terminée. Si vous souhaitez utiliser l'automatisation et le MAV ensemble, il est recommandé d'utiliser des requêtes pour des opérations MAV spécifiques. Vous pouvez, par exemple, appliquer `volume delete MAV` ne règle que les volumes où l'automatisation n'est pas impliquée et vous pouvez désigner ces volumes avec un schéma de nommage particulier.



Si vous avez besoin de désactiver la fonctionnalité de vérification multi-administrateurs sans l'approbation de l'administrateur MAV, contactez le support NetApp et mentionnez l'article suivant de la base de connaissances : ["Comment désactiver la vérification multi-administrateur si MAV admin n'est pas disponible"](#).

Fonctionnement de la vérification multi-administration

La vérification multi-administrateurs comprend les éléments suivants :

- Groupe d'un ou plusieurs administrateurs ayant des pouvoirs d'approbation et de veto.
- Un ensemble d'opérations ou de commandes protégées dans une table *rules*.
- Un *moteur de règles* pour identifier et contrôler l'exécution des opérations protégées.

Les règles MAV sont évaluées après les règles de contrôle d'accès basé sur des rôles (RBAC). Par conséquent, les administrateurs qui exécutent ou approuvent les opérations protégées doivent déjà posséder le minimum de privilèges RBAC pour ces opérations. ["En savoir plus sur le RBAC."](#)

Règles définies par le système

Lorsque la vérification multi-admin est activée, les règles définies par le système (également appelées règles *Guard-rail*) établissent un ensemble d'opérations MAV pour contenir le risque de contournement du processus MAV lui-même. Ces opérations ne peuvent pas être supprimées de la table des règles. Une fois MAV activé, les opérations désignées par un astérisque (*) nécessitent l'approbation d'un ou de plusieurs administrateurs avant l'exécution, à l'exception des commandes * show*.

- `security multi-admin-verify modify fonctionnement*`

Contrôle la configuration de la fonctionnalité de vérification multi-administrateur.

- `security multi-admin-verify approval-group` **opérations***

Contrôlez l'appartenance à un ensemble d'administrateurs avec des informations d'identification de vérification multi-administrateur.

- `security multi-admin-verify rule` **opérations***

Contrôler le jeu de commandes qui nécessitent une vérification multi-administrateur.

- `security multi-admin-verify request` **exploitation**

Contrôler le processus d'approbation.

Commandes protégées par des règles

Outre les commandes définies par le système, les commandes suivantes sont protégées par défaut lorsque la vérification multi-admin est activée, mais vous pouvez modifier les règles afin de supprimer la protection de ces commandes.

- `security login password`
- `security login unlock`
- `set`

Les commandes suivantes peuvent être protégées dans ONTAP 9.11.1 et versions ultérieures.

<code>cluster peer delete</code>	<code>volume snapshot autodelete modify</code>
<code>event config modify</code>	<code>volume snapshot delete</code>
<code>security login create</code>	<code>volume snapshot policy add-schedule</code>
<code>security login delete</code>	<code>volume snapshot policy create</code>
<code>security login modify</code>	<code>volume snapshot policy delete</code>
<code>system node run</code>	<code>volume snapshot policy modify</code>
<code>system node systemshell</code>	<code>volume snapshot policy modify-schedule</code>
<code>volume delete</code>	<code>volume snapshot policy remove-schedule</code>
<code>volume flexcache delete</code>	<code>volume snapshot restore</code>
	<code>vserver peer delete</code>

Les commandes suivantes peuvent être protégées à partir de ONTAP 9.13.1 :

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`

- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

Les commandes suivantes peuvent être protégées à partir de ONTAP 9.14.1 :

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

Fonctionnement de l'approbation multi-admin

Chaque fois qu'une opération protégée est saisie sur un cluster protégé par MAV, une demande d'exécution d'opération est envoyée au groupe d'administrateurs MAV désigné.

Vous pouvez configurer :

- Les noms, les coordonnées et le nombre d'administrateurs du groupe MAV.

Un administrateur MAV doit avoir un rôle RBAC avec des privilèges d'administrateur de cluster.

- Nombre de groupes d'administrateurs MAV.
 - Un groupe MAV est attribué pour chaque règle d'opération protégée.
 - Pour plusieurs groupes MAV, vous pouvez configurer quel groupe MAV approuve une règle donnée.
- Nombre d'approbations MAV nécessaires à l'exécution d'une opération protégée.
- Période_d'expiration_ de l'approbation au cours de laquelle un administrateur MAV doit répondre à une demande d'approbation.
- Période_d'expiration_ de l'exécution pendant laquelle l'administrateur demandeur doit effectuer l'opération.

Une fois ces paramètres configurés, l'approbation MAV est requise pour les modifier.

Les administrateurs MAV ne peuvent pas approuver leurs propres demandes d'exécution d'opérations protégées. Par conséquent :

- MAV ne doit pas être activé sur les clusters avec un seul administrateur.
- S'il n'y a qu'une seule personne dans le groupe MAV, cet administrateur MAV ne peut pas entrer d'opérations protégées ; les administrateurs réguliers doivent les entrer et l'administrateur MAV ne peut approuver que.
- Si vous souhaitez que les administrateurs MAV puissent exécuter des opérations protégées, le nombre d'administrateurs MAV doit être supérieur d'un au nombre d'approbations requises.
Par exemple, si deux approbations sont requises pour une opération protégée et que vous voulez que les administrateurs MAV les exécutent, il doit y avoir trois personnes dans le groupe administrateurs MAV.

Les administrateurs MAV peuvent recevoir des demandes d'approbation dans des alertes par e-mail (à l'aide d'EMS) ou interroger la file d'attente des requêtes. Lorsqu'ils reçoivent une demande, ils peuvent effectuer l'une des trois actions suivantes :

- Approuver

- Rejet (veto)
- Ignorer (aucune action)

Les notifications par e-mail sont envoyées à tous les approbateurs associés à une règle MAV lorsque :

- Une demande est créée.
- Une demande est approuvée ou vetotée.
- Une requête approuvée est exécutée.

Si le demandeur se trouve dans le même groupe d'approbation pour l'opération, il recevra un e-mail lorsque sa demande est approuvée.

Remarque : Un demandeur ne peut approuver ses propres demandes, même si elles font partie du groupe d'approbation. Mais ils peuvent obtenir les notifications par e-mail. Les demandeurs qui ne sont pas dans les groupes d'approbation (c'est-à-dire qui ne sont pas des administrateurs MAV) ne reçoivent pas de notifications par e-mail.

Fonctionnement de l'exécution des opérations protégées

Si l'exécution est approuvée pour une opération protégée, l'utilisateur demandeur continue avec l'opération à l'invite. Si l'opération est mise au veto, l'utilisateur requérant doit supprimer la demande avant de continuer.

Les règles MAV sont évaluées après les autorisations RBAC. Par conséquent, un utilisateur sans autorisations RBAC suffisantes pour l'exécution de l'opération ne peut pas lancer le processus de requête MAV.

Gérer les groupes d'approbation des administrateurs

Avant d'activer la vérification multi-administrateur (MAV), vous devez créer un groupe d'approbation administrateur contenant un ou plusieurs administrateurs à accorder ou à accorder une autorité d'approbation ou de veto. Une fois que vous avez activé la vérification multi-administrateur, toute modification de l'appartenance au groupe d'approbation nécessite l'approbation de l'un des administrateurs qualifiés existants.

Description de la tâche

Vous pouvez ajouter des administrateurs existants à un groupe MAV ou créer de nouveaux administrateurs.



La fonctionnalité MAV permet de définir les paramètres existants de contrôle d'accès basé sur des rôles (RBAC). Les administrateurs MAV potentiels doivent disposer de privilèges suffisants pour exécuter des opérations protégées avant d'être ajoutés aux groupes d'administrateurs MAV. ["En savoir plus sur le RBAC."](#)

Vous pouvez configurer MAV pour avertir les administrateurs MAV que les demandes d'approbation sont en attente. Pour ce faire, vous devez configurer les notifications par e-mail, en particulier, le Mail From et Mail Server paramètres—ou vous pouvez effacer ces paramètres pour désactiver la notification. Sans alertes par e-mail, les administrateurs MAV doivent vérifier manuellement la file d'attente d'approbation.



Procédure de System Manager

Si vous souhaitez créer un groupe d'approbation MAV pour la première fois, reportez-vous à la procédure System Manager à ["activation de la vérification multi-administrateurs"](#)

Pour modifier un groupe d'approbation existant ou créer un groupe d'approbation supplémentaire :

1. Identifiez les administrateurs pour qu'ils reçoivent une vérification multi-administrateur.
 - a. Cliquez sur **Cluster > Paramètres**.
 - b. Cliquez sur  À côté de **utilisateurs et rôles**.
 - c. Cliquez sur  **Add** Sous **utilisateurs**.
 - d. Modifiez la liste si nécessaire.

Pour plus d'informations, voir "[Contrôlez l'accès administrateur](#)."

2. Créer ou modifier le groupe d'approbation MAV :
 - a. Cliquez sur **Cluster > Paramètres**.
 - b. Cliquez sur  En regard de **Multi-Admin Approval** dans la section **Security**.
(Vous verrez le  Si MAV n'est pas encore configuré.)
 - Nom : entrez un nom de groupe.
 - Approbateurs : sélectionnez des approbateurs dans une liste d'utilisateurs.
 - Adresse e-mail : saisissez une ou plusieurs adresses e-mail.
 - Groupe par défaut : sélectionnez un groupe.

Une approbation MAV est requise pour modifier une configuration existante une fois que MAV est activé.

Procédure CLI

1. Vérifier que les valeurs ont été définies pour le Mail From et Mail Server paramètres. Entrez :

```
event config show
```

L'affichage doit être similaire à ce qui suit :

```
cluster01::> event config show
                        Mail From:  admin@localhost
                        Mail Server: localhost
                        Proxy URL:   -
                        Proxy User:  -
                        Publish/Subscribe Messaging Enabled: true
```

Pour configurer ces paramètres, entrez :

```
event config modify -mail-from email_address -mail-server server_name
```

2. Identifiez les administrateurs pour qu'ils reçoivent une vérification multi-administrateur

Si vous voulez...	Saisissez cette commande
Afficher les administrateurs actuels	<code>security login show</code>
Modifier les informations d'identification des administrateurs actuels	<code>security login modify <parameters></code>

Si vous voulez...	Saisissez cette commande
Créer de nouveaux comptes d'administrateur	<code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code>

3. Créer le groupe d'approbation MAV :

```
security multi-admin-verify approval-group create [ -vserver svm_name] -name group_name -approvers approver1[,approver2...] [[-email address1], address1...]
```

- `-vserver` - Seul le SVM d'admin est pris en charge dans cette version.
- `-name` - Le nom du groupe MAV, jusqu'à 64 caractères.
- `-approvers` - La liste d'un ou plusieurs approbateurs.
- `-email` - Une ou plusieurs adresses e-mail qui sont notifiées lors de la création, de l'approbation, du veto ou de l'exécution d'une demande.

Exemple : la commande suivante crée un groupe MAV avec deux membres et des adresses e-mail associées.

```
cluster-1::> security multi-admin-verify approval-group create -name mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. Vérifier la création et l'appartenance de groupe :

```
security multi-admin-verify approval-group show
```

Exemple:

```
cluster-1::> security multi-admin-verify approval-group show
Vserver   Name           Approvers      Email
-----
svm-1     mav-grp1      pavan,julia    email
pavan@myfirm.com,julia@myfirm.com
```

Utilisez ces commandes pour modifier votre configuration initiale du groupe MAV.

Remarque : tous exigent l'approbation de l'administrateur MAV avant l'exécution.

Si vous voulez...	Saisissez cette commande
Modifier les caractéristiques du groupe ou modifier les informations du membre existant	<code>security multi-admin-verify approval-group modify [<i>parameters</i>]</code>

Si vous voulez...	Saisissez cette commande
Ajouter ou supprimer des membres	<code>security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[, approver2...]] [-approvers-to-remove approver1[, approver2...]]</code>
Supprimer un groupe	<code>security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name</code>

Activez et désactivez la vérification multi-administration

La vérification multi-administrateur (MAV) doit être activée explicitement. Une fois que vous avez activé la vérification multi-administrateur, l'approbation par les administrateurs d'un groupe d'approbation MAV (administrateurs MAV) est requise pour la supprimer.

Description de la tâche

Une fois MAV activé, la modification ou la désactivation de MAV nécessite l'approbation de l'administrateur MAV.



Si vous avez besoin de désactiver la fonctionnalité de vérification multi-administrateurs sans l'approbation de l'administrateur MAV, contactez le support NetApp et mentionnez l'article suivant de la base de connaissances : ["Comment désactiver la vérification multi-administrateur si MAV admin n'est pas disponible"](#).

Lorsque vous activez MAV, vous pouvez spécifier globalement les paramètres suivants.

Groupes d'approbation

Une liste de groupes d'approbation globaux. Au moins un groupe est requis pour activer la fonctionnalité MAV.



Si vous utilisez MAV avec la protection anti-ransomware autonome (ARP), définissez un nouveau groupe d'approbation ou un groupe d'approbation existant chargé d'approuver la pause ARP, de désactiver et d'effacer les demandes suspectes.

Approbateurs requis

Nombre d'approbateurs requis pour exécuter une opération protégée. La valeur par défaut et le nombre minimum sont 1.



Le nombre requis d'approbateurs doit être inférieur au nombre total d'approbateurs uniques dans les groupes d'approbation par défaut.

Expiration de l'approbation (heures, minutes, secondes)

Période pendant laquelle un administrateur MAV doit répondre à une demande d'approbation. La valeur par défaut est une heure (1h), la valeur minimale prise en charge est une seconde (1s) et la valeur maximale prise en charge est de 14 jours (14d).



Expiration de l'exécution (heures, minutes, secondes)

Période pendant laquelle l'administrateur requérant doit effectuer l'opération :: La valeur par défaut est une heure (1h), la valeur minimale prise en charge est une seconde (1s) et la valeur maximale prise en charge est de 14 jours (14d).

Vous pouvez également remplacer n'importe lequel de ces paramètres pour un particulier "[règles de fonctionnement](#)."



Procédure de System Manager

1. Identifiez les administrateurs pour qu'ils reçoivent une vérification multi-administrateur.

- a. Cliquez sur **Cluster > Paramètres**.
- b. Cliquez sur  À côté de **utilisateurs et rôles**.
- c. Cliquez sur  **Add** Sous **utilisateurs**.
- d. Modifiez la liste si nécessaire.

Pour plus d'informations, voir "[Contrôlez l'accès administrateur](#)."

2. Activez la vérification multi-administration en créant au moins un groupe d'approbation et en ajoutant au moins une règle.

- a. Cliquez sur **Cluster > Paramètres**.
- b. Cliquez sur  En regard de **Multi-Admin Approval** dans la section **Security**.
- c. Cliquez sur  **Add** pour ajouter au moins un groupe d'approbation.
 - Nom – Entrez un nom de groupe.
 - Approbateurs : sélectionnez des approbateurs dans une liste d'utilisateurs.
 - Adresse e-mail – Entrez une ou plusieurs adresses e-mail.
 - Groupe par défaut : sélectionnez un groupe.
- d. Ajoutez au moins une règle.
 - Opération – sélectionnez une commande prise en charge dans la liste.
 - Requête – saisissez les options et les valeurs de commande souhaitées.
 - Paramètres facultatifs ; laissez vide pour appliquer des paramètres globaux ou attribuez une valeur différente pour des règles spécifiques afin de remplacer les paramètres globaux.
 - Nombre requis d'approbateurs
 - Groupes d'approbation
- e. Cliquez sur **Paramètres avancés** pour afficher ou modifier les valeurs par défaut.
 - Nombre d'approbateurs requis (par défaut : 1)
 - Expiration de la demande d'exécution (par défaut : 1 heure)
 - Expiration de la demande d'approbation (par défaut : 1 heure)
 - Serveur de messagerie*
 - De l'adresse e-mail*

*Ces paramètres mettent à jour les paramètres de messagerie gérés sous "gestion des notifications". Vous êtes invité à les définir si elles n'ont pas encore été configurées.


f. Cliquez sur **Activer** pour terminer la configuration initiale du MAV.

Après la configuration initiale, l'état actuel du MAV est affiché dans la mosaïque **Multi-Admin Approval**.

- État (activé ou non)
- Opérations actives pour lesquelles des approbations sont requises
- Nombre de demandes ouvertes à l'état en attente

Vous pouvez afficher une configuration existante en cliquant sur ➔. L'approbation MAV est requise pour modifier une configuration existante.

Pour désactiver la vérification multi-administrateur :

1. Cliquez sur **Cluster > Paramètres**.
2. Cliquez sur  En regard de **Multi-Admin Approval** dans la section **Security**.
3. Cliquez sur le bouton bascule activé.

L'approbation MAV est requise pour effectuer cette opération.

Procédure CLI

Avant d'activer la fonctionnalité MAV au niveau de la CLI, au moins une "Groupe administrateur MAV" doit avoir été créé.

Si vous voulez...	Saisissez cette commande
Activer la fonctionnalité MAV	<pre>security multi-admin-verify modify -approval-groups group1[,group2...] [- required-approvers nn] -enabled true [-execution-expiry [nnh][nmm][nns]] [-approval-expiry [nnh][nmm][nns]]</pre> <p>Exemple : la commande suivante active MAV avec 1 groupe d'approbation, 2 approbateurs requis et périodes d'expiration par défaut.</p> <pre>cluster-1::> security multi-admin- verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre> <p>Terminez la configuration initiale en ajoutant au moins une configuration "règle de fonctionnement."</p>

Si vous voulez...	Saisissez cette commande
Modifier une configuration MAV (nécessite l'approbation MAV)	<code>security multi-admin-verify approval-group modify [-approval-groups <i>group1</i> [,<i>group2</i>...]] [-required-approvers <i>nn</i>] [-execution-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]] [-approval-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]]</code>
Vérifier la fonctionnalité MAV	<code>security multi-admin-verify show</code> Exemple: <pre> cluster-1::> security multi-admin-verify show Is Required Execution Approval Approval Enabled Approvers Expiry Expiry Groups ----- true 2 1h 1h mav-grp1 </pre>
Désactiver la fonctionnalité MAV (nécessite l'approbation MAV)	<code>security multi-admin-verify modify -enabled false</code>

Gérer les règles d'opération protégées

Vous créez des règles de vérification multi-administration (MAV) pour désigner des opérations nécessitant une approbation. Chaque fois qu'une opération est lancée, des opérations protégées sont interceptées et une demande d'approbation est générée.

Les règles peuvent être créées avant d'activer MAV par tout administrateur disposant des fonctionnalités RBAC appropriées, mais une fois MAV activé, toute modification de l'ensemble de règles nécessite l'approbation MAV.

Une seule règle MAV peut être créée par opération ; par exemple, vous ne pouvez pas en créer plusieurs `volume-snapshot-delete` règles. Toutes les contraintes de règle souhaitées doivent être contenues dans une règle.

Commandes protégées par des règles

Vous pouvez créer des règles pour protéger les commandes suivantes à partir de ONTAP 9.11.1.

<code>cluster peer delete</code>	<code>volume snapshot autodelete modify</code>
<code>event config modify</code>	<code>volume snapshot delete</code>
<code>security login create</code>	<code>volume snapshot policy add-schedule</code>
<code>security login delete</code>	<code>volume snapshot policy create</code>
<code>security login modify</code>	<code>volume snapshot policy delete</code>
<code>system node run</code>	<code>volume snapshot policy modify</code>
<code>system node systemshell</code>	<code>volume snapshot policy modify-schedule</code>
<code>volume delete</code>	<code>volume snapshot policy remove-schedule</code>
<code>volume flexcache delete</code>	<code>volume snapshot restore</code>
	<code>vserver peer delete</code>

Vous pouvez créer des règles pour protéger les commandes suivantes à partir de ONTAP 9.13.1 :

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

Vous pouvez créer des règles pour protéger les commandes suivantes à partir de ONTAP 9.14.1 :

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

Les règles pour les commandes par défaut du système MAV, le `security multi-admin-verify` "[commandes](#)", ne peut pas être modifié.

Outre les commandes définies par le système, les commandes suivantes sont protégées par défaut lorsque la vérification multi-admin est activée, mais vous pouvez modifier les règles afin de supprimer la protection de ces commandes.

- `security login password`
- `security login unlock`
- `set`

Contraintes de règle

Lorsque vous créez une règle, vous pouvez éventuellement spécifier le `-query` option permettant de limiter la demande à un sous-ensemble de la fonctionnalité de la commande. Le `-query` Option peut également être utilisée pour limiter les éléments de configuration tels que la SVM, le volume et les noms des snapshots.

Par exemple, dans le `volume snapshot delete` commande `-query` peut être défini sur `-snapshot !hourly*,!daily*,!weekly*`, Ce qui signifie que les instantanés de volume préfixés avec des attributs horaires, quotidiens ou hebdomadaires sont exclus des protections MAV.

```
smci-vsimg20::> security multi-admin-verify rule show
```

Vserver	Operation	Required Approvers	Approval Groups
vs01	volume snapshot delete Query: -snapshot !hourly*,!daily*,!weekly*	-	-



Tous les éléments de configuration exclus ne seraient pas protégés par MAV, et tout administrateur pourrait les supprimer ou les renommer.

Par défaut, les règles spécifient qu'un correspondant `security multi-admin-verify request create "protected_operation"` la commande est générée automatiquement lorsqu'une opération protégée est saisie. Vous pouvez modifier cette valeur par défaut pour exiger que la `request create` la commande doit être saisie séparément.



Par défaut, les règles héritent des paramètres généraux MAV suivants, bien que vous puissiez spécifier des exceptions spécifiques aux règles :

- Nombre requis d'approbateurs
- Groupes d'approbation
- Période d'expiration de l'approbation
- Période d'expiration de l'exécution

Procédure de System Manager

Pour ajouter une règle d'opération protégée pour la première fois, reportez-vous à la procédure de System Manager à ["activation de la vérification multi-administrateurs"](#)

Pour modifier le jeu de règles existant :

1. Sélectionnez **Cluster > Paramètres**.
2. Sélectionnez  En regard de **Multi-Admin Approval** dans la section **Security**.
3. Sélectionnez  **Add** pour ajouter au moins une règle, vous pouvez également modifier ou supprimer des règles existantes.
 - Opération – sélectionnez une commande prise en charge dans la liste.
 - Requête – saisissez les options et les valeurs de commande souhaitées.
 - Paramètres facultatifs – laissez vide pour appliquer des paramètres globaux ou attribuez une valeur différente pour des règles spécifiques afin de remplacer les paramètres globaux.

- Nombre requis d'approbateurs
- Groupes d'approbation

Procédure CLI



Tout `security multi-admin-verify rule` Les commandes exigent l'approbation de l'administrateur MAV avant leur exécution, sauf `security multi-admin-verify rule show`.

Si vous voulez...	Saisissez cette commande
Créer une règle	<code>security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]</code>
Modifier les informations d'identification des administrateurs actuels	<code>security login modify <parameters></code> Exemple : la règle suivante nécessite l'approbation pour supprimer le volume racine. <code>security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"</code>
Modifier une règle	<code>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</code>
Supprimer une règle	<code>security multi-admin-verify rule delete -operation "protected_operation"</code>
Afficher les règles	<code>security multi-admin-verify rule show</code>

Pour plus d'informations sur la syntaxe de commande, reportez-vous à la section `security multi-admin-verify rule` pages de manuel.

Demander l'exécution d'opérations protégées

Lorsque vous lancez une opération ou une commande protégée sur un cluster activé pour la vérification multi-administrateur (MAV), ONTAP intercepte automatiquement l'opération et demande de générer une requête qui doit être approuvée par un ou plusieurs administrateurs d'un groupe d'approbation MAV (administrateurs MAV). Vous pouvez également créer une requête MAV sans la boîte de dialogue.

Si elle est approuvée, vous devez alors répondre à la requête pour terminer l'opération dans le délai d'expiration de la requête. Si vous vous êtes opposé ou si les périodes de demande ou d'expiration sont dépassées, vous devez supprimer la demande et la renvoyer.

La fonctionnalité MAV permet de définir les paramètres RBAC existants. C'est-à-dire que votre rôle d'administrateur doit disposer de privilèges suffisants pour exécuter une opération protégée sans tenir compte des paramètres MAV. ["En savoir plus sur le RBAC"](#).

Si vous êtes administrateur MAV, vos demandes d'exécution d'opérations protégées doivent également être approuvées par un administrateur MAV.

Procédure de System Manager

Lorsqu'un utilisateur clique sur un élément de menu pour lancer une opération et que l'opération est protégée, une demande d'approbation est générée et l'utilisateur reçoit une notification semblable à ce qui suit :

```
Approval request to delete the volume was sent.  
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

La fenêtre **Multi-Admin Requests** est disponible lorsque MAV est activé, affichant les demandes en attente basées sur l'ID de connexion et le rôle MAV de l'utilisateur (approbateur ou non). Pour chaque demande en attente, les champs suivants sont affichés :

- Fonctionnement
- Index (nombre)
- État (en attente, approuvé, rejeté, exécuté ou expiré)

Si une demande est rejetée par un approbateur, aucune autre action n'est possible.

- Requête (tous les paramètres ou valeurs de l'opération demandée)
- Utilisateur demandeur
- La demande expire le
- (Nombre de) approbateurs en attente
- (Nombre de) approbateurs potentiels

Lorsque la demande est approuvée, l'utilisateur demandeur peut relancer l'opération dans la période d'expiration.

Si l'utilisateur tente de nouveau l'opération sans approbation, une notification s'affiche comme suit :

```
Request to perform delete operation is pending approval.  
Retry the operation after request is approved.
```

Procédure CLI

1. Entrez directement l'opération protégée ou à l'aide de la commande MAV request.

Exemples – pour supprimer un volume, entrez l'une des commandes suivantes :

```
° volume delete
```



```
cluster-1::*> volume delete -volume voll -vserver vs0
```

```
Warning: This operation requires multi-admin verification. To create  
a
```

```
    verification request use "security multi-admin-verify  
request  
    create".
```

```
    Would you like to create a request for this operation?  
    {y|n}: y
```

```
Error: command failed: The security multi-admin-verify request (index  
3) is  
    auto-generated and requires approval.
```

```
° security multi-admin-verify request create "volume delete"
```

```
Error: command failed: The security multi-admin-verify request (index  
3)  
    requires approval.
```

2. Vérifier l'état de la demande et répondre à l'avis MAV.

- a. Si la requête est approuvée, répondez au message de l'interface de ligne de commande pour terminer l'opération.

Exemple:

```
cluster-1::> security multi-admin-verify request show 3
```

```
    Request Index: 3
      Operation: volume delete
        Query: -vserver vs0 -volume voll1
        State: approved
Required Approvers: 1
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
    Approvals: admin2
    User Vetoed: -
      Vserver: cluster-1
  User Requested: admin
    Time Created: 2/25/2022 13:32:03
    Time Approved: 2/25/2022 13:35:36
      Comment: -
  Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll1 -vserver vs0
```

Info: Volume "voll1" in Vserver "vs0" will be marked as deleted and placed in the volume recovery queue. The space used by the volume will be recovered only after the retention period of 12 hours has completed. To recover the space immediately, get the volume name using (privilege:advanced) "volume recovery-queue show voll_*" and then "volume recovery-queue purge -vserver vs0 -volume <volume_name>" command. To recover the volume use the (privilege:advanced) "volume recovery-queue recover -vserver vs0 -volume <volume_name>" command.

Warning: Are you sure you want to delete volume "voll1" in Vserver "vs0" ?
{y|n}: y

- b. Si la demande est voetotée ou si la période d'expiration est passée, supprimez la demande et relancez ou contactez l'administrateur MAV.

Exemple:

```
cluster-1::> security multi-admin-verify request show 3
```

```
Request Index: 3
  Operation: volume delete
    Query: -vserver vs0 -volume voll1
    State: vetoed
Required Approvers: 1
Pending Approvers: 1
  Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
    Approvals: -
    User Vetoed: admin2
    Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:38:47
  Time Approved: -
    Comment: -
Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll1 -vserver vs0
```

```
Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

Gérer les demandes d'opérations protégées

Lorsque les administrateurs d'un groupe d'approbation MAV (administrateurs MAV) sont avertis d'une demande d'exécution d'opération en attente, ils doivent répondre par un message d'approbation ou de veto dans un délai fixe (expiration de l'approbation). Si un nombre suffisant d'approbations n'est pas reçu, le demandeur doit supprimer la demande et en faire une autre.

Description de la tâche

Les demandes d'approbation sont identifiées par des numéros d'index, qui sont inclus dans les e-mails et sont affichées dans la file d'attente des demandes.

Les informations suivantes de la file d'attente de demandes peuvent être affichées :

Fonctionnement

Opération protégée pour laquelle la demande est créée.

Requête

Objet (ou objets) sur lequel l'utilisateur souhaite appliquer l'opération.

État

État actuel de la demande ; en attente, approuvé, rejeté, expiré, exécuté. Si une demande est rejetée par un approbateur, aucune autre action n'est possible.

Approbateurs requis

Nombre d'administrateurs MAV requis pour approuver la demande. Un utilisateur peut définir le paramètre approbateurs requis pour la règle d'opération. Si un utilisateur ne définit pas les approbateurs requis sur la règle, les approbateurs requis du paramètre global sont appliqués.

Approbateurs en attente

Nombre d'administrateurs MAV toujours requis pour approuver la demande pour que la demande soit marquée comme approuvée.

Expiration de l'approbation

Période pendant laquelle un administrateur MAV doit répondre à une demande d'approbation. Tout utilisateur autorisé peut définir la règle d'approbation-expiration d'une opération. Si l'approbation-expiration n'est pas définie pour la règle, l'approbation-expiration du paramètre global est appliquée.

Expiration de l'exécution

Période pendant laquelle l'administrateur requérant doit terminer l'opération. Tout utilisateur autorisé peut définir une règle d'exécution-expiration pour une opération. Si exécution-expiration n'est pas définie pour la règle, l'exécution-expiration du paramètre global est appliquée.

Utilisateurs approuvés

Les administrateurs MAV qui ont approuvé la demande.

L'utilisateur a refusé son droit d'veto

Les administrateurs MAV qui ont opposé leur veto à la demande.

VM de stockage (vServer)

SVM avec lequel la requête est associée. Seule le SVM d'administration est pris en charge dans cette version.

Utilisateur demandé

Nom d'utilisateur de l'utilisateur qui a créé la demande.

Heure de création

Heure de création de la demande.

Heure d'approbation

Heure à laquelle l'état de la demande passe à approuvé.

Commentaire

Tout commentaire associé à la demande.

Utilisateurs autorisés

Liste des utilisateurs autorisés à effectuer l'opération protégée pour laquelle la demande est approuvée. Si `users-permitted` est vide, alors tout utilisateur disposant des autorisations appropriées peut effectuer l'opération.

Toutes les demandes expirées ou exécutées sont supprimées lorsqu'une limite de 1000 demandes est atteinte ou lorsque la durée d'expiration est supérieure à 8 heures pour les demandes expirées. Les demandes de veto

sont supprimées dès qu'elles sont marquées comme expirées.

Procédure de System Manager

Les administrateurs MAV reçoivent des e-mails contenant les détails de la demande d'approbation, la période d'expiration de la demande et un lien pour approuver ou rejeter la demande. Ils peuvent accéder à une boîte de dialogue d'approbation en cliquant sur le lien dans l'e-mail ou accédez à **Events & Jobs> requêtes** dans System Manager.

La fenêtre **requêtes** est disponible lorsque la vérification multi-administrateur est activée, affichant les demandes en attente basées sur l'ID de connexion de l'utilisateur et le rôle MAV (approbateur ou non).

- Fonctionnement
- Index (nombre)
- État (en attente, approuvé, rejeté, exécuté ou expiré)

Si une demande est rejetée par un approbateur, aucune autre action n'est possible.

- Requête (tous les paramètres ou valeurs de l'opération demandée)
- Utilisateur demandeur
- La demande expire le
- (Nombre de) approbateurs en attente
- (Nombre de) approbateurs potentiels

Les administrateurs MAV disposent de contrôles supplémentaires dans cette fenêtre ; ils peuvent approuver, rejeter ou supprimer des opérations individuelles ou des groupes d'opérations sélectionnés. Toutefois, si l'administrateur MAV est l'utilisateur qui demande, il ne peut approuver, rejeter ou supprimer ses propres demandes.

Procédure CLI

1. Lorsqu'une demande est signalée par courrier électronique en attente, notez le numéro d'index de la demande et la période d'expiration de l'approbation. Le numéro d'index peut également être affiché à l'aide des options **show** ou **show-Pending** mentionnées ci-dessous.
2. Approuver ou opposer un veto à la demande.

Si vous voulez...	Saisissez cette commande
Approuver une demande	<code>security multi-admin-verify request approve nn</code>
Veto sur une demande	<code>security multi-admin-verify request veto nn</code>
Affiche toutes les demandes, les demandes en attente ou une seule demande	<code>`security multi-admin-verify request { show</code>

Si vous voulez...	Saisissez cette commande
<pre>show-pending } [nn] { -fields field1[,field2...]</pre>	<pre>[-instance] }</pre> <p>Vous pouvez afficher toutes les demandes dans la file d'attente ou uniquement les demandes en attente. Si vous saisissez le numéro d'index, seules les informations pour ce numéro sont affichées. Vous pouvez afficher des informations sur des champs spécifiques (en utilisant le <code>-fields</code> paramètre) ou à propos de tous les champs (en utilisant le <code>-instance</code> paramètre).</p>
Supprimer une demande	<pre>security multi-admin-verify request delete nn</pre>

Exemple :

La séquence suivante approuve une demande après que l'administrateur MAV ait reçu l'e-mail de demande avec l'index numéro 3, qui a déjà une approbation.

```

cluster1::> security multi-admin-verify request show-pending
                                Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete -    pending 1      julia

```

```
cluster-1::> security multi-admin-verify request approve 3
```

```
cluster-1::> security multi-admin-verify request show 3
```

```

Request Index: 3
  Operation: volume delete
    Query: -
    State: approved
Required Approvers: 2
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
    Approvals: mav-admin2
    User Vetoed: -
      Vserver: cluster-1
User Requested: julia
  Time Created: 2/25/2022 13:32:03
  Time Approved: 2/25/2022 13:35:36
    Comment: -
Users Permitted: -

```

Exemple :

La séquence suivante affiche une demande après que l'administrateur MAV ait reçu l'e-mail de demande avec l'index numéro 3, qui a déjà une approbation.

```

cluster1::> security multi-admin-verify request show-pending
                                Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete -    pending 1      pavan

cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
  Operation: volume delete
    Query: -
    State: vetoed
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
  Approvals: mav-admin1
  User Vetoed: mav-admin2
    Vserver: cluster-1
User Requested: pavan
  Time Created: 2/25/2022 13:32:03
  Time Approved: 2/25/2022 13:35:36
    Comment: -
Users Permitted: -

```

Authentification et autorisation via OAuth 2.0

Présentation de la mise en œuvre de ONTAP OAuth 2.0

Depuis ONTAP 9.14, vous avez la possibilité de contrôler l'accès à vos clusters ONTAP à l'aide de l'infrastructure d'autorisation ouverte (OAuth 2.0). Vous pouvez configurer cette fonctionnalité à l'aide de n'importe quelle interface d'administration ONTAP, notamment l'interface de ligne de commandes ONTAP, System Manager et l'API REST. Cependant, les décisions d'autorisation et de contrôle d'accès OAuth 2.0 ne peuvent être appliquées que lorsqu'un client accède à ONTAP à l'aide de l'API REST.



La prise en charge d'OAuth 2.0 a été introduite pour la première fois avec ONTAP 9.14.0. Sa disponibilité dépend donc de la version ONTAP que vous utilisez. Voir la ["Notes de version de ONTAP"](#) pour en savoir plus.

Caractéristiques et avantages

Les principales caractéristiques et avantages de l'utilisation d'OAuth 2.0 avec ONTAP sont décrits ci-dessous.

Prise en charge de la norme OAuth 2.0

OAuth 2.0 est le cadre d'autorisation standard de l'industrie. Il permet de restreindre et de contrôler l'accès aux ressources protégées à l'aide de jetons d'accès signés. L'utilisation d'OAuth 2.0 présente plusieurs avantages :

- De nombreuses options pour la configuration de l'autorisation
- Ne jamais révéler les informations d'identification du client, y compris les mots de passe
- Les tokens peuvent être définis pour expirer en fonction de votre configuration
- La solution est idéale pour une utilisation avec les API REST

Testé avec plusieurs serveurs d'autorisation courants

L'implémentation ONTAP est conçue pour être compatible avec tout serveur d'autorisation compatible OAuth 2.0. Il a été testé avec les serveurs ou services populaires suivants, notamment :

- Auth0
- ADFS (Active Directory Federation Service)
- Porte-clés

Prise en charge de plusieurs serveurs d'autorisation simultanés

Vous pouvez définir jusqu'à huit serveurs d'autorisation pour un seul cluster ONTAP. Vous disposez ainsi de la flexibilité nécessaire pour répondre aux besoins de votre environnement de sécurité diversifié.

Intégration avec les rôles REST

Les décisions d'autorisation ONTAP sont finalement basées sur les rôles REST attribués aux utilisateurs ou aux groupes. Ces rôles sont soit portés dans le jeton d'accès en tant que étendues autonomes, soit basés sur des définitions ONTAP locales avec Active Directory ou des groupes LDAP.

Option permettant d'utiliser des jetons d'accès limités par l'expéditeur

Vous pouvez configurer ONTAP et les serveurs d'autorisation pour utiliser MTLS (Mutual transport Layer Security) qui renforce l'authentification des clients. Il garantit que les jetons d'accès OAuth 2.0 ne sont utilisés que par les clients auxquels ils ont été émis à l'origine. Cette fonction prend en charge et s'aligne sur plusieurs recommandations de sécurité courantes, y compris celles établies par FAPI et MITRE.

Implémentation et configuration

À un niveau élevé, il existe plusieurs aspects de la mise en œuvre et de la configuration d'OAuth 2.0 que vous devez prendre en compte lors de la mise en route.

OAuth 2.0 entités au sein de ONTAP

Le cadre d'autorisation OAuth 2.0 définit plusieurs entités qui peuvent être mappées à des éléments réels ou virtuels au sein de votre centre de données ou de votre réseau. Les entités OAuth 2.0 et leur adaptation à ONTAP sont présentées dans le tableau ci-dessous.

OAuth 2.0 entité	Description
Ressource	Les terminaux d'API REST qui fournissent l'accès aux ressources ONTAP via des commandes ONTAP internes.

OAuth 2.0 entité	Description
Propriétaire de la ressource	Utilisateur du cluster ONTAP qui a créé ou possède la ressource protégée par défaut.
Serveur de ressources	Hôte des ressources protégées qui correspond au cluster ONTAP.
Client	Application demandant l'accès à un point de terminaison d'API REST pour le compte ou avec l'autorisation du propriétaire de la ressource.
Serveur d'autorisation	Généralement un serveur dédié responsable de l'émission des jetons d'accès et de l'application de la stratégie administrative.

Configuration ONTAP principale

Vous devez configurer le cluster ONTAP pour activer et utiliser OAuth 2.0. Cela inclut l'établissement d'une connexion au serveur d'autorisation et la définition de la configuration d'autorisation ONTAP requise. Vous pouvez effectuer cette configuration à l'aide de n'importe quelle interface d'administration, notamment :

- Interface de ligne de commande ONTAP
- System Manager
- L'API REST DE ONTAP

Environnement et services de soutien

Outre les définitions ONTAP, vous devez également configurer les serveurs d'autorisation. Si vous utilisez le mappage groupe-rôle, vous devez également configurer les groupes Active Directory ou l'équivalent LDAP.

Clients ONTAP pris en charge

À partir de ONTAP 9.14, un client d'API REST peut accéder à ONTAP à l'aide d'OAuth 2.0. Avant d'émettre un appel API REST, vous devez obtenir un jeton d'accès auprès du serveur d'autorisation. Le client transmet ensuite ce token au cluster ONTAP en tant que *bearer token* à l'aide de l'en-tête de requête d'autorisation HTTP. Selon le niveau de sécurité requis, vous pouvez également créer et installer un certificat au niveau du client pour utiliser des jetons limités par l'expéditeur basés sur MTLS.

Terminologie sélectionnée

Lorsque vous commencez à explorer un déploiement OAuth 2.0 avec ONTAP, il est utile de vous familiariser avec une partie de la terminologie. Voir "[Ressources supplémentaires](#)" Pour obtenir des liens vers des informations supplémentaires sur OAuth 2.0.

Jeton d'accès

Jeton émis par un serveur d'autorisation et utilisé par une application client OAuth 2.0 pour faire des demandes d'accès aux ressources protégées.

Jeton Web JSON

Norme utilisée pour formater les jetons d'accès. JSON est utilisé pour représenter les réclamations OAuth 2.0 dans un format compact avec les réclamations disposées en trois sections principales.

Jeton d'accès contraint par l'expéditeur

Fonctionnalité facultative basée sur le protocole MTLS (Mutual transport Layer Security). En utilisant une demande de confirmation supplémentaire dans le jeton, cela garantit que le jeton d'accès n'est utilisé que par le client auquel il a été émis à l'origine.

Jeu de clés Web JSON

Un JWKS est un ensemble de clés publiques utilisées par ONTAP pour vérifier les jetons JWT présentés par les clients. Les jeux de clés sont généralement disponibles au niveau du serveur d'autorisation via un URI dédié.

Portée

Les étendues permettent de limiter ou de contrôler l'accès d'une application à des ressources protégées telles que l'API REST ONTAP. Ils sont représentés sous forme de chaînes dans le jeton d'accès.

Rôle REST ONTAP

Les rôles REST ont été introduits avec ONTAP 9.6 et constituent une partie centrale du framework ONTAP RBAC. Ces rôles sont différents des rôles traditionnels antérieurs qui sont encore pris en charge par ONTAP. L'implémentation OAuth 2.0 dans ONTAP ne prend en charge que les rôles REST.

En-tête d'autorisation HTTP

En-tête inclus dans la requête HTTP pour identifier le client et les autorisations associées dans le cadre d'un appel d'API REST. Plusieurs versions ou implémentations sont disponibles selon la manière dont l'authentification et l'autorisation sont effectuées. Lors de la présentation d'un jeton d'accès OAuth 2.0 à ONTAP, le jeton est identifié comme un *jeton porteur*.

Authentification de base HTTP

Une technique d'authentification HTTP précoce encore prise en charge par ONTAP. Les informations d'identification en texte clair (nom d'utilisateur et mot de passe) sont concaténées avec un deux-points et codées en base64. La chaîne est placée dans l'en-tête de la demande d'autorisation et envoyée au serveur.

FAPI

Un groupe de travail de la Fondation OpenID qui fournit des protocoles, des schémas de données et des recommandations de sécurité pour le secteur financier. L'API était à l'origine connue sous le nom d'API de qualité financière.

ONGLET

Une société privée à but non lucratif fournissant des conseils techniques et de sécurité à l'armée de l'air américaine et au gouvernement américain.

Ressources supplémentaires

Plusieurs ressources supplémentaires sont fournies ci-dessous. Vous devriez consulter ces sites pour obtenir plus d'informations sur OAuth 2.0 et les normes connexes.

Protocoles et normes

- ["RFC 6749 : cadre d'autorisation OAuth 2.0"](#)
- ["RFC 7519 : tokens Web JSON \(JWT\)"](#)
- ["RFC 7523 : profil JSON Web Token \(JWT\) pour les autorisations et l'authentification des clients OAuth 2.0"](#)
- ["RFC 7662 : introspection de tokens OAuth 2.0"](#)
- ["RFC 7800 : clé de preuve de possession pour JWT"](#)
- ["RFC 8705 : authentification du client mutuelle OAuth 2.0 et jetons d'accès liés au certificat"](#)

Organisations

- ["Fondation OpenID"](#)
- ["Groupe de travail de l'IAI"](#)
- ["ONGLET"](#)
- ["IANA - JWT"](#)

Produits et services

- ["Auth0"](#)
- ["Présentation de l'ADFS"](#)
- ["Porte-clés"](#)

Outils et utilitaires supplémentaires

- ["JWT par Auth0"](#)
- ["OpenSSL"](#)

Documentation et ressources de NetApp

- ["Automatisation ONTAP"](#) documentation

Concepts

Serveurs d'autorisation et jetons d'accès

Les serveurs d'autorisation effectuent plusieurs fonctions importantes en tant que composant central dans le cadre d'autorisation OAuth 2.0.

Serveurs d'autorisation OAuth 2.0

Les serveurs d'autorisation sont principalement responsables de la création et de la signature des jetons d'accès. Ces tokens contiennent des informations d'identité et d'autorisation permettant à une application client d'accéder de manière sélective aux ressources protégées. Les serveurs sont généralement isolés les uns des autres et peuvent être mis en œuvre de différentes manières, notamment en tant que serveur dédié autonome ou dans le cadre d'un produit de gestion des identités et des accès plus large.



Une terminologie différente peut parfois être utilisée pour un serveur d'autorisation, en particulier lorsque la fonctionnalité OAuth 2.0 est intégrée dans un produit ou une solution de gestion des identités et des accès plus large. Par exemple, le terme **Identity Provider (IDP)** est fréquemment utilisé de manière interchangeable avec **Authorization Server**.

L'administration

Outre l'émission de jetons d'accès, les serveurs d'autorisation fournissent également des services administratifs connexes, généralement via une interface utilisateur Web. Par exemple, vous pouvez définir et administrer :

- Authentification des utilisateurs et des utilisateurs
- Étendues
- Ségrégation administrative par les locataires et les royaumes
- Application des règles
- Connexion à divers services externes

- Prise en charge d'autres protocoles d'identité (tels que SAML)

ONTAP est compatible avec les serveurs d'autorisation conformes à la norme OAuth 2.0.

Définition de ONTAP

Vous devez définir un ou plusieurs serveurs d'autorisation sur ONTAP. ONTAP communique en toute sécurité avec chaque serveur pour vérifier les tokens et effectuer d'autres tâches connexes pour la prise en charge des applications client.

Les principaux aspects de la configuration ONTAP sont présentés ci-dessous. Voir aussi "[Scénarios de déploiement OAuth 2.0](#)" pour en savoir plus.

Comment et où les jetons d'accès sont validés

Il existe deux options pour valider les jetons d'accès.

- Validation locale

ONTAP peut valider les jetons d'accès localement en fonction des informations fournies par le serveur d'autorisation qui a émis le token. Les informations extraites du serveur d'autorisation sont mises en cache par ONTAP et actualisées à intervalles réguliers.

- Introspection à distance

Vous pouvez également utiliser l'introspection à distance pour valider les tokens sur le serveur d'autorisation. L'introspection est un protocole permettant aux parties autorisées d'interroger un serveur d'autorisation sur un jeton d'accès. Il permet à ONTAP d'extraire certaines métadonnées d'un jeton d'accès et de valider le jeton. ONTAP met en cache une partie des données pour des raisons de performances.

Emplacement réseau

ONTAP peut se trouver derrière un pare-feu. Dans ce cas, vous devez identifier un proxy comme faisant partie de la configuration.

Définition des serveurs d'autorisation

Vous pouvez définir un serveur d'autorisation pour ONTAP à l'aide de n'importe quelle interface d'administration, notamment l'interface de ligne de commandes, System Manager ou l'API REST. Par exemple, avec l'interface de ligne de commandes, vous utilisez la commande `security oauth2 client create`.

Nombre de serveurs d'autorisation

Vous pouvez définir jusqu'à huit serveurs d'autorisation sur un seul cluster ONTAP. Le même serveur d'autorisation peut être défini plusieurs fois sur le même cluster ONTAP tant que les demandes d'émetteur ou d'émetteur/d'audience sont uniques. Par exemple, avec Keycloak, ce sera toujours le cas lorsque vous utilisez des domaines différents.

Utilisation des jetons d'accès OAuth 2.0

Les jetons d'accès OAuth 2.0 émis par les serveurs d'autorisation sont vérifiés par ONTAP et utilisés pour prendre des décisions d'accès basées sur les rôles pour les requêtes client de l'API REST.

Acquisition d'un jeton d'accès

Vous devez acquérir un jeton d'accès à partir d'un serveur d'autorisation défini sur le cluster ONTAP où vous

utilisez l'API REST. Pour acquérir un jeton, vous devez contacter directement le serveur d'autorisation.



ONTAP n'émet pas de tokens d'accès ni ne redirige pas les requêtes des clients vers les serveurs d'autorisation.

La façon dont vous demandez un jeton dépend de plusieurs facteurs, notamment :

- Serveur d'autorisation et ses options de configuration
- Type de subvention OAuth 2.0
- Client ou outil logiciel utilisé pour émettre la demande

Types de subventions

Un *Grant* est un processus bien défini, comprenant un ensemble de flux réseau, utilisé pour demander et recevoir un jeton d'accès OAuth 2.0. Plusieurs types d'octroi différents peuvent être utilisés en fonction du client, de l'environnement et des exigences de sécurité. Une liste des types de subventions les plus populaires est présentée dans le tableau ci-dessous.

Type de subvention	Description
Informations d'identification du client	Type de subvention populaire basé sur l'utilisation de références uniquement (par exemple, un ID et un secret partagé). Le client est supposé avoir une relation de confiance étroite avec le propriétaire de la ressource.
Mot de passe	Le type d'octroi d'autorisations de mot de passe du propriétaire de ressource peut être utilisé lorsque le propriétaire de la ressource a une relation de confiance établie avec le client. Elle peut également être utile lors de la migration de clients HTTP hérités vers OAuth 2.0.
Code d'autorisation	Il s'agit d'un type d'octroi idéal pour les clients confidentiels et basé sur un flux basé sur la redirection. Il peut être utilisé pour obtenir à la fois un jeton d'accès et un jeton d'actualisation.

Contenu JWT

Un jeton d'accès OAuth 2.0 est formaté en JWT. Le contenu est créé par le serveur d'autorisation en fonction de votre configuration. Cependant, les tokens sont opaques pour les applications client. Un client n'a aucune raison d'inspecter un jeton ou d'être au courant du contenu.

Chaque jeton d'accès JWT contient un ensemble de réclamations. Les réclamations décrivent les caractéristiques de l'émetteur et l'autorisation en fonction des définitions administratives du serveur d'autorisation. Certaines des réclamations enregistrées avec la norme sont décrites dans le tableau ci-dessous. Toutes les chaînes sont sensibles à la casse.

Réclamation	Mot-clé	Description
Émetteur	iss	Identifie le principal qui a émis le token. Le traitement de la demande est spécifique à l'application.
Objet	sous	L'objet ou l'utilisateur du jeton. Le nom est défini comme unique au niveau global ou local.
Public	aud	Destinataires pour lequel le token est destiné. Implémenté en tant que tableau de chaînes.

Réclamation	Mot-clé	Description
Expiration	date	Heure après laquelle le jeton expire et doit être rejeté.

Voir ["RFC 7519 : tokens Web JSON"](#) pour en savoir plus.

Options pour l'autorisation client ONTAP

Plusieurs options sont disponibles pour personnaliser votre autorisation client ONTAP. Les décisions d'autorisation sont finalement basées sur les rôles REST ONTAP contenus dans ou dérivés des jetons d'accès.



Vous pouvez uniquement utiliser ["Rôles REST ONTAP"](#) Lors de la configuration de l'autorisation pour OAuth 2.0. Les anciens rôles ONTAP traditionnels ne sont pas pris en charge.

Introduction

La mise en œuvre OAuth 2.0 au sein de ONTAP est conçue pour être flexible et robuste, offrant les options dont vous avez besoin pour sécuriser l'environnement ONTAP. À un niveau élevé, il existe trois principales catégories de configuration permettant de définir l'autorisation du client ONTAP. Ces options de configuration s'excluent mutuellement.

ONTAP applique l'option la plus appropriée en fonction de votre configuration. Voir ["Comment ONTAP détermine l'accès"](#) Pour en savoir plus sur la façon dont ONTAP traite vos définitions de configuration pour prendre des décisions d'accès.

Oscilloscopes autonomes OAuth 2.0

Ces étendues contiennent un ou plusieurs rôles REST personnalisés, chacun encapsulé dans une seule chaîne. Ils sont indépendants des définitions de rôles ONTAP. Vous devez définir ces chaînes de portée sur votre serveur d'autorisation.

Utilisateurs et rôles REST spécifiques à ONTAP en local

En fonction de votre configuration, les définitions d'identité ONTAP locales peuvent être utilisées pour prendre des décisions d'accès. Les options sont les suivantes :

- Rôle REST nommé unique
- Correspondance du nom d'utilisateur avec un utilisateur ONTAP local

La syntaxe de portée d'un rôle nommé est **ontap-role-`<URL-encoded-ONTAP-role-name>`**. Par exemple, si le rôle est « admin », la chaîne de portée sera « ontap-role-admin ».

Groupes Active Directory ou LDAP

Si les définitions ONTAP locales sont examinées mais qu'aucune décision d'accès ne peut être prise, les groupes Active Directory (« domaine ») ou LDAP (« nsswitch ») sont utilisés. Les informations de groupe peuvent être spécifiées de deux manières :

- Chaîne de portée OAuth 2.0

Prend en charge les applications confidentielles en utilisant le flux d'informations d'identification du client lorsqu'aucun utilisateur n'est membre d'un groupe. Le périmètre doit être nommé **ontap-group-`<URL-encoded-ONTAP-group-name>`**. Par exemple, si le groupe est « développement », la chaîne de portée sera « ontap-groupe-développement ».

- Dans la réclamation « Groupe »

Ceci est destiné aux jetons d'accès émis par ADFS à l'aide du flux propriétaire de la ressource (mot de passe Grant).

Oscilloscopes OAuth 2.0 autonomes

Les étendues autonomes sont des chaînes portées dans le jeton d'accès. Chacune d'entre elles constitue une définition de rôle personnalisée complète et comprend tout ce dont ONTAP a besoin pour prendre une décision d'accès. Le périmètre est distinct et celui de tous les rôles REST définis au sein de ONTAP lui-même.

Format de la chaîne de portée

Au niveau de la base, la portée est représentée sous la forme d'une chaîne contiguë et composée de six valeurs séparées par deux points. Les paramètres utilisés dans la chaîne de portée sont décrits ci-dessous.

Littéral ONTAP

La portée doit commencer par la valeur littérale `ontap` en minuscules. Cette opération identifie la portée en tant que spécifique à ONTAP.

Cluster

Il définit le cluster ONTAP auquel la portée s'applique. Les valeurs peuvent inclure :

- UUID de cluster

Identifie un seul cluster.

- Astérisque (*)

Indique que la portée s'applique à tous les clusters.

Vous pouvez utiliser la commande CLI de ONTAP `cluster identity show` Pour afficher l'UUID de votre cluster. Si elle n'est pas spécifiée, la portée s'applique à tous les clusters.

Rôle

Nom du rôle REST contenu dans le périmètre autonome. Cette valeur n'est pas examinée par ONTAP ou associée à tout rôle REST existant défini sur ONTAP. Le nom est utilisé pour la journalisation.

Niveau d'accès

Cette valeur indique le niveau d'accès appliqué à l'application client lors de l'utilisation du noeud final de l'API dans le périmètre. Il existe six valeurs possibles, comme décrit dans le tableau ci-dessous.

Niveau d'accès	Description
Aucune	Refuse tout accès au noeud final spécifié.
lecture seule	Autorise uniquement l'accès en lecture à l'aide de GET.
read_create	Permet l'accès en lecture ainsi que la création de nouvelles instances de ressources à l'aide de POST.

Niveau d'accès	Description
lire_modifier	Permet l'accès en lecture ainsi que la mise à jour des ressources existantes à l'aide d'un CORRECTIF.
read_create_modify	Permet tous les accès sauf supprimer. Les opérations autorisées comprennent OBTENIR (lire), POST (créer) et PATCH (mettre à jour).
tous	Permet un accès complet.

SVM

Nom du SVM au sein du cluster auquel la portée s'applique. Utilisez la valeur * (astérisque) pour indiquer tous les SVM.



Cette fonctionnalité n'est pas entièrement prise en charge par ONTAP 9.14.1. Vous pouvez ignorer le paramètre du SVM et utiliser un astérisque comme emplacement réservé. Vérifiez le ["Notes de version de ONTAP"](#) Pour vérifier la prise en charge future des SVM.

URI DE L'API REST

Chemin complet ou partiel d'une ressource ou d'un ensemble de ressources associées. La chaîne doit commencer par `/api`. Si vous ne spécifiez pas de valeur, la portée s'applique à tous les terminaux d'API du cluster ONTAP.

Exemples de portée

Quelques exemples de portées autonomes sont présentés ci-dessous.

ontap*:joes-role:read_create_modify:*/api/cluster

Permet à l'utilisateur affecté à ce rôle d'accéder en lecture, création et modification à `/cluster` point final.

Outil d'administration CLI

Pour faciliter l'administration des étendues autonomes et réduire le risque d'erreur, ONTAP fournit la commande CLI `security oauth2 scope` pour générer des chaînes de portée basées sur vos paramètres d'entrée.

La commande `security oauth2 scope` propose deux cas d'utilisation basés sur vos commentaires :

- Paramètres de l'interface de ligne de commande pour la chaîne de périmètre

Vous pouvez utiliser cette version de la commande pour générer une chaîne de portée basée sur les paramètres d'entrée.

- Chaîne d'étendue aux paramètres CLI

Vous pouvez utiliser cette version de la commande pour générer les paramètres de la commande en fonction de la chaîne de périmètre d'entrée.

Exemple

L'exemple suivant génère une chaîne de périmètre avec le résultat inclus après l'exemple de commande ci-dessous. La définition s'applique à tous les clusters.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api  
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

Comment ONTAP détermine l'accès

Pour bien concevoir et mettre en œuvre OAuth 2.0, vous devez comprendre comment ONTAP utilise votre configuration d'autorisation pour prendre des décisions d'accès pour les clients.

Étape 1 : oscilloscopes autonomes

Si le jeton d'accès contient des périmètres autonomes, ONTAP examine d'abord ces périmètres. S'il n'y a pas de portées autonomes, passez à l'étape 2.

Avec une ou plusieurs portées autonomes présentes, ONTAP applique chaque portée jusqu'à ce qu'une décision explicite **ALLOW** ou **DENY** puisse être prise. Si une décision explicite est prise, le traitement prend fin.

Si ONTAP ne peut pas prendre de décision explicite en matière d'accès, passez à l'étape 2.

Étape 2 : vérifiez l'indicateur de rôles locaux

ONTAP examine la valeur de l'indicateur `use-local-roles-if-present`. La valeur de cet indicateur est définie séparément pour chaque serveur d'autorisation défini sur ONTAP.

- Si la valeur est de `true` passez à l'étape 3.
- Si la valeur est de `false` le traitement se termine et l'accès est refusé.

Étape 3 : rôle REST ONTAP nommé

Si le jeton d'accès contient un rôle REST nommé, ONTAP utilise ce rôle pour prendre la décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

S'il n'y a pas de rôle REST nommé ou si le rôle est introuvable, passez à l'étape 4.

Étape 4 : utilisateurs ONTAP locaux

Extrayez le nom d'utilisateur du jeton d'accès et essayez de le faire correspondre à un utilisateur ONTAP local.

Si un utilisateur ONTAP local est associé, ONTAP utilise le rôle défini pour que l'utilisateur puisse prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

Si un utilisateur ONTAP local ne correspond pas ou s'il n'y a pas de nom d'utilisateur dans le jeton d'accès, passez à l'étape 5.

Étape 5 : mappage groupe-rôle

Extrayez le groupe du jeton d'accès et essayez de le faire correspondre à un groupe. Les groupes sont définis à l'aide d'Active Directory ou d'un serveur LDAP équivalent.

S'il existe une correspondance de groupe, ONTAP utilise le rôle défini pour le groupe pour prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

S'il n'y a pas de correspondance de groupe ou s'il n'y a pas de groupe dans le jeton d'accès, l'accès est refusé et le traitement se termine.

Scénarios de déploiement OAuth 2.0

Plusieurs options de configuration sont disponibles lors de la définition d'un serveur d'autorisation dans ONTAP. En fonction de ces options, vous pouvez créer un serveur d'autorisation adapté à votre environnement de déploiement.

Résumé des paramètres de configuration

Plusieurs paramètres de configuration sont disponibles lors de la définition d'un serveur d'autorisation dans ONTAP. Ces paramètres sont généralement pris en charge dans toutes les interfaces administratives.

Les noms des paramètres peuvent varier légèrement en fonction de l'interface d'administration de ONTAP. Par exemple, lors de la configuration de l'introspection à distance, le noeud final est identifié à l'aide du paramètre de commande CLI `-introspection-endpoint`. Mais avec System Manager, le champ équivalent est *URI* d'introspection de jeton de serveur d'autorisation. Pour prendre en charge toutes les interfaces administratives ONTAP, une description générale des paramètres est fournie. Le paramètre ou le champ exact doit être évident en fonction du contexte.

Paramètre	Description
Nom	Nom du serveur d'autorisation tel qu'il est connu de ONTAP.
Client supplémentaire	Application interne ONTAP à laquelle s'applique la définition. Ce doit être http .
URI de l'émetteur	Nom de domaine complet avec chemin identifiant le site ou l'organisation qui émet les jetons.
URI du fournisseur JWKS	Nom de domaine complet avec chemin et nom de fichier où ONTAP obtient les jeux de clés Web JSON utilisés pour valider les jetons d'accès.
Intervalle de rafraîchissement JWKS	Intervalle de temps déterminant la fréquence à laquelle ONTAP actualise les informations de certificat à partir de l'URI JWKS du fournisseur. La valeur est spécifiée au format ISO-8601.
Point d'extrémité d'introspection	Nom de domaine complet avec chemin utilisé par ONTAP pour effectuer la validation de jeton à distance via l'introspection.
ID client	Nom du client tel que défini sur le serveur d'autorisation. Lorsque cette valeur est incluse, vous devez également fournir le secret client associé en fonction de l'interface.
Proxy sortant	Cela permet d'accéder au serveur d'autorisation lorsque ONTAP se trouve derrière un pare-feu. L'URI doit être au format curl.
Utilisez des rôles locaux, le cas échéant	Indicateur booléen déterminant si les définitions ONTAP locales sont utilisées, y compris un rôle REST nommé et des utilisateurs locaux.
Supprimer la réclamation utilisateur	Autre nom utilisé par ONTAP pour correspondre aux utilisateurs locaux. Utilisez le <code>sub</code> champ du jeton d'accès correspondant au nom d'utilisateur local.

Scénarios de déploiement

Vous trouverez ci-dessous plusieurs scénarios de déploiement courants. Ils sont organisés selon que la validation des tokens est effectuée localement par ONTAP ou à distance par le serveur d'autorisation. Chaque scénario inclut une liste des options de configuration requises. Voir "[Déployer OAuth 2.0 dans ONTAP](#)" pour des exemples de commandes de configuration.



Après avoir défini un serveur d'autorisation, vous pouvez afficher sa configuration via l'interface d'administration ONTAP. Par exemple, utilisez la commande `security oauth2 client show` Via l'interface de ligne de commandes ONTAP.

Validation locale

Les scénarios de déploiement suivants sont basés sur l'exécution locale de la validation des jetons par ONTAP.

Utilisez des oscilloscopes autonomes sans proxy

Il s'agit du déploiement le plus simple utilisant uniquement des oscilloscopes autonomes OAuth 2.0. Aucune définition d'identité ONTAP locale n'est utilisée. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- URI du fournisseur JWKS
- URI de l'émetteur

Vous devez également ajouter les étendues au niveau du serveur d'autorisation.

Utiliser des portées autonomes avec un proxy

Ce scénario de déploiement utilise les étendues autonomes OAuth 2.0. Aucune définition d'identité ONTAP locale n'est utilisée. Mais le serveur d'autorisation est derrière un pare-feu et vous devez donc configurer un proxy. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- URI du fournisseur JWKS
- Proxy sortant
- URI de l'émetteur
- Public

Vous devez également ajouter les étendues au niveau du serveur d'autorisation.

Utilisez les rôles d'utilisateur local et le mappage de nom d'utilisateur par défaut avec un proxy

Ce scénario de déploiement utilise des rôles d'utilisateur local avec un mappage de noms par défaut. Le sinistre utilisateur distant utilise la valeur par défaut de `sub` ce champ du jeton d'accès est donc utilisé pour correspondre au nom d'utilisateur local. Le nom d'utilisateur doit comporter au maximum 40 caractères. Le serveur d'autorisation se trouve derrière un pare-feu, vous devez donc également configurer un proxy. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- URI du fournisseur JWKS
- Utilisez des rôles locaux, le cas échéant (`true`)
- Proxy sortant
- Émetteur

Vous devez vous assurer que l'utilisateur local est défini sur ONTAP.

Utilisez des rôles d'utilisateur locaux et un mappage de nom d'utilisateur alternatif avec un proxy

Ce scénario de déploiement utilise des rôles d'utilisateur local avec un autre nom d'utilisateur qui est utilisé pour correspondre à un utilisateur ONTAP local. Le serveur d'autorisation est derrière un pare-feu, vous devez donc configurer un proxy. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- URI du fournisseur JWKS
- Utilisez des rôles locaux, le cas échéant (`true`)
- Demande d'utilisateur à distance
- Proxy sortant
- URI de l'émetteur
- Public

Vous devez vous assurer que l'utilisateur local est défini sur ONTAP.

Introspection à distance

Les configurations de déploiement suivantes sont basées sur ONTAP qui effectue la validation des jetons à distance via l'introspection.

Utilisez des oscilloscopes autonomes sans proxy

Il s'agit d'un déploiement simple basé sur l'utilisation des oscilloscopes autonomes OAuth 2.0. Aucune définition d'identité ONTAP n'est utilisée. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- Point d'extrémité d'introspection
- ID client
- URI de l'émetteur

Vous devez définir les étendues ainsi que le secret client et client sur le serveur d'autorisation.

Authentification du client à l'aide d'un protocole TLS mutuel

Selon vos besoins en matière de sécurité, vous pouvez éventuellement configurer le protocole MTLS (Mutual TLS) pour mettre en œuvre une authentification client forte. Lorsqu'il est utilisé avec ONTAP dans le cadre d'un déploiement OAuth 2.0, MTLS garantit que les jetons d'accès ne sont utilisés que par les clients auxquels ils ont été initialement émis.

Protocole commun avec OAuth 2.0

TLS (transport Layer Security) est utilisé pour établir un canal de communication sécurisé entre deux applications, généralement un navigateur client et un serveur Web. Le protocole mutuel TLS étend cette fonction en fournissant une identification forte du client par le biais d'un certificat client. Lorsqu'elle est utilisée

dans un cluster ONTAP avec OAuth 2.0, la fonctionnalité MTLS de base est étendue en créant et en utilisant des jetons d'accès limités par l'expéditeur.

Un jeton d'accès limité par l'expéditeur ne peut être utilisé que par le client auquel il a été émis à l'origine. Pour prendre en charge cette fonction, une nouvelle demande de confirmation (`cnf`) est inséré dans le jeton. Le champ contient la propriété `x5t#S256` qui contient un résumé du certificat client utilisé lors de la demande du jeton d'accès. Cette valeur est vérifiée par ONTAP dans le cadre de la validation du jeton. Les jetons d'accès émis par les serveurs d'autorisation qui ne sont pas soumis à des contraintes d'expéditeur n'incluent pas la demande de confirmation supplémentaire.

Vous devez configurer ONTAP pour qu'il utilise MTLS séparément pour chaque serveur d'autorisation. Par exemple, la commande CLI `security oauth2 client` inclut le paramètre `use-mutual-tls` Contrôler le traitement MTLS en fonction de trois valeurs, comme indiqué dans le tableau ci-dessous.



Dans chaque configuration, le résultat et l'action de ONTAP dépendent de la valeur du paramètre de configuration, ainsi que du contenu du jeton d'accès et du certificat client. Les paramètres du tableau sont organisés du moins au plus restrictif.

Paramètre	Description
Aucune	L'authentification mutuelle TLS OAuth 2.0 est complètement désactivée pour le serveur d'autorisation. ONTAP n'effectuera pas l'authentification du certificat du client MTLS même si la demande de confirmation est présente dans le jeton ou si un certificat client est fourni avec la connexion TLS.
demande	L'authentification mutuelle TLS OAuth 2.0 est appliquée si un jeton d'accès limité par l'expéditeur est présenté par le client. C'est-à-dire que MTLS est appliqué uniquement si la demande de confirmation (avec la propriété <code>x5t#S256</code>) est présent dans le jeton d'accès. Il s'agit du paramètre par défaut.
obligatoire	L'authentification mutuelle TLS OAuth 2.0 est appliquée pour tous les jetons d'accès émis par le serveur d'autorisation. Par conséquent, tous les tokens d'accès doivent être soumis à des contraintes d'expéditeur. L'authentification et la demande de l'API REST échouent si la demande de confirmation n'est pas présente dans le jeton d'accès ou si un certificat client n'est pas valide.

Flux de mise en œuvre de haut niveau

Les étapes typiques de l'utilisation de MTLS avec OAuth 2.0 dans un environnement ONTAP sont présentées ci-dessous. Voir "[RFC 8705 : authentification du client mutuelle OAuth 2.0 et jetons d'accès liés au certificat](#)" pour en savoir plus.

Étape 1 : création et installation d'un certificat client

L'établissement de l'identité du client repose sur la preuve de la connaissance d'une clé privée du client. La clé publique correspondante est placée dans un certificat X.509 signé présenté par le client. À un niveau élevé, les étapes impliquées dans la création du certificat client comprennent :

1. Générez une paire de clés publique et privée
2. Créez une demande de signature de certificat
3. Envoyez le fichier CSR à une autorité de certification connue
4. CA vérifie la demande et émet le certificat signé

Vous pouvez normalement installer le certificat client dans votre système d'exploitation local ou l'utiliser

directement avec un utilitaire commun tel que curl.

Étape 2 : configurer ONTAP pour utiliser MTLS

Vous devez configurer ONTAP pour utiliser MTLS. Cette configuration est effectuée séparément pour chaque serveur d'autorisation. Par exemple, avec l'interface de ligne de commandes, la commande `security oauth2 client` est utilisé avec le paramètre facultatif `use-mutual-tls`. Voir "[Déployer OAuth 2.0 dans ONTAP](#)" pour en savoir plus.

Étape 3 : le client demande un jeton d'accès

Le client doit demander un jeton d'accès au serveur d'autorisation configuré sur ONTAP. L'application client doit utiliser MTLS avec le certificat créé et installé à l'étape 1.

Étape 4 : le serveur d'autorisation génère le jeton d'accès

Le serveur d'autorisation vérifie la demande du client et génère un jeton d'accès. Dans ce cadre, il crée un résumé de message du certificat client qui est inclus dans le jeton en tant que demande de confirmation (champ `cnf`).

Étape 5 : l'application client présente le jeton d'accès à ONTAP

L'application client effectue un appel d'API REST vers le cluster ONTAP et inclut le jeton d'accès dans l'en-tête de la demande d'autorisation en tant que **jeton porteur**. Le client doit utiliser MTLS avec le même certificat que celui utilisé pour demander le jeton d'accès.

Étape 6 : ONTAP vérifie le client et le jeton.

ONTAP reçoit le jeton d'accès dans une requête HTTP ainsi que le certificat client utilisé dans le cadre du traitement MTLS. ONTAP valide d'abord la signature dans le jeton d'accès. En fonction de la configuration, ONTAP génère un résumé de message du certificat client et le compare à la demande de confirmation `cnf` du jeton. Si les deux valeurs correspondent, ONTAP a confirmé que le client faisant la demande d'API est le même client auquel le jeton d'accès a été émis à l'origine.

Configuration et déploiement

Préparez-vous à déployer OAuth 2.0 avec ONTAP

Avant de configurer OAuth 2.0 dans un environnement ONTAP, vous devez préparer le déploiement. Un résumé des principales tâches et décisions est inclus ci-dessous. L'agencement des sections est généralement aligné sur l'ordre que vous devez suivre. Toutefois, même si cette solution est applicable à la plupart des déploiements, vous devez l'adapter à votre environnement selon les besoins. Vous devez également envisager de créer un plan de déploiement formel.



En fonction de votre environnement, vous pouvez sélectionner la configuration des serveurs d'autorisation définis pour ONTAP. Cela inclut les valeurs de paramètre que vous devez spécifier pour chaque type de déploiement. Voir "[Scénarios de déploiement OAuth 2.0](#)" pour en savoir plus.

Ressources protégées et applications client

OAuth 2.0 est un cadre d'autorisation permettant de contrôler l'accès aux ressources protégées. Dans un premier temps, il est donc important de déterminer quelles sont les ressources disponibles et quels clients ont besoin d'y accéder.

Identifiez les applications client

Vous devez décider quels clients utiliseront OAuth 2.0 lors de l'émission d'appels API REST et à quels terminaux API ils ont besoin d'accéder.

Passez en revue les rôles REST ONTAP et les utilisateurs locaux existants

Vous devez examiner les définitions d'identité ONTAP existantes, y compris les rôles REST et les utilisateurs locaux. Selon la configuration d'OAuth 2.0, ces définitions peuvent être utilisées pour prendre des décisions d'accès.

Transition globale vers OAuth 2.0

Bien que vous puissiez implémenter l'autorisation OAuth 2.0 progressivement, vous pouvez également déplacer tous les clients API REST vers OAuth 2.0 immédiatement en définissant un indicateur global pour chaque serveur d'autorisation. Vous pouvez ainsi prendre des décisions d'accès en fonction de votre configuration ONTAP existante sans avoir à créer de étendues autonomes.

Serveurs d'autorisation

Les serveurs d'autorisation jouent un rôle important dans votre déploiement OAuth 2.0 en émettant des jetons d'accès et en appliquant une stratégie administrative.

Sélectionnez et installez le serveur d'autorisation

Vous devez sélectionner et installer un ou plusieurs serveurs d'autorisation. Il est important de se familiariser avec les options de configuration et les procédures de vos fournisseurs d'identité, y compris la définition des périmètres.

Déterminez si le certificat d'autorité de certification racine d'autorisation doit être installé

ONTAP utilise le certificat du serveur d'autorisation pour valider les jetons d'accès signés présentés par les clients. Pour ce faire, ONTAP a besoin du certificat de l'autorité de certification racine et de tous les certificats intermédiaires. Ils peuvent être pré-installés avec ONTAP. Si ce n'est pas le cas, vous devez les installer.

Évaluez l'emplacement et la configuration du réseau

Si le serveur d'autorisation est derrière un pare-feu, ONTAP doit être configuré pour utiliser un serveur proxy.

Authentification et autorisation du client

Il existe plusieurs aspects de l'authentification et de l'autorisation des clients que vous devez prendre en compte.

Étendues autonomes ou définitions d'identité ONTAP locales

À un niveau élevé, vous pouvez définir des étendues autonomes définies sur le serveur d'autorisation ou vous appuyer sur les définitions d'identité ONTAP locales existantes, y compris les rôles et les utilisateurs.

Options avec traitement ONTAP local

Si vous utilisez les définitions d'identité ONTAP, vous devez choisir celles qui doivent être appliquées, notamment :

- Rôle REST nommé
- Faire correspondre les utilisateurs locaux
- Groupes Active Directory ou LDAP

Validation locale ou introspection à distance

Vous devez décider si les jetons d'accès seront validés localement par ONTAP ou au niveau du serveur

d'autorisation par introspection. Plusieurs valeurs connexes sont également à prendre en compte, telles que l'intervalle d'actualisation.

Jetons d'accès limités par l'expéditeur

Pour les environnements nécessitant un niveau de sécurité élevé, vous pouvez utiliser des jetons d'accès avec limite d'envoi basés sur MTLS. Cela nécessite un certificat pour chaque client.

Interface d'administration

Vous pouvez administrer OAuth 2.0 via n'importe quelle interface ONTAP, notamment :

- Interface de ligne de commandes
- System Manager
- API REST

Comment les clients demandent des jetons d'accès

Les applications client doivent demander des jetons d'accès directement à partir du serveur d'autorisation. Vous devez décider de la façon dont cela sera fait, y compris le type de subvention.

Configurer ONTAP

Vous devez effectuer plusieurs tâches de configuration ONTAP.

Définissez les rôles REST et les utilisateurs locaux

En fonction de votre configuration d'autorisation, le traitement local ONTAP Identify peut être utilisé. Dans ce cas, vous devez revoir et définir les rôles REST et les définitions d'utilisateur.

Configuration centrale

Trois étapes principales sont nécessaires pour effectuer la configuration principale de ONTAP, notamment :

- Vous pouvez également installer le certificat racine (ainsi que tous les certificats intermédiaires) de l'autorité de certification qui a signé le certificat du serveur d'autorisation.
- Définissez le serveur d'autorisation.
- Activez le traitement OAuth 2.0 pour le cluster.

Déployer OAuth 2.0 dans ONTAP

Le déploiement de la fonctionnalité principale OAuth 2.0 implique trois étapes principales.

Avant de commencer

Vous devez préparer le déploiement OAuth 2.0 avant de configurer ONTAP. Par exemple, vous devez évaluer le serveur d'autorisation, y compris la façon dont son certificat a été signé et s'il est derrière un pare-feu. Voir ["Préparez-vous à déployer OAuth 2.0 avec ONTAP"](#) pour en savoir plus.

Étape 1 : installez le certificat du serveur d'authentification

ONTAP inclut un grand nombre de certificats d'autorité de certification racine pré-installés. Ainsi, dans de nombreux cas, le certificat de votre serveur d'autorisation sera immédiatement reconnu par ONTAP sans configuration supplémentaire. Mais selon la façon dont le certificat du serveur d'autorisation a été signé, vous devrez peut-être installer un certificat d'autorité de certification racine et tous les certificats intermédiaires.

Suivez les instructions ci-dessous pour installer le certificat si nécessaire. Vous devez installer tous les

certificats requis au niveau du cluster.

Choisissez la procédure appropriée en fonction de votre accès à ONTAP.

Exemple 1. Étapes

System Manager

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Faites défiler jusqu'à la section **sécurité**.
3. Cliquez sur → en regard de **certificats**.
4. Sous l'onglet **autorités de certification approuvées**, cliquez sur **Ajouter**.
5. Cliquez sur **Importer** et sélectionnez le fichier de certificat.
6. Renseignez les paramètres de configuration de votre environnement.
7. Cliquez sur **Ajouter**.

CLI

1. Commencez l'installation :

```
security certificate install -type server-ca
```

2. Recherchez le message de console suivant :

```
Please enter Certificate: Press <Enter> when done
```

3. Ouvrez le fichier de certificat à l'aide d'un éditeur de texte.
4. Copiez l'intégralité du certificat, y compris les lignes suivantes :

```
-----BEGIN CERTIFICATE-----
```

```
-----END CERTIFICATE-----
```

5. Collez le certificat dans le terminal après l'invite de commande.
6. Appuyez sur **entrée** pour terminer l'installation.
7. Vérifiez que le certificat est installé à l'aide de l'une des méthodes suivantes :

```
security certificate show-user-installed
```

```
security certificate show
```

Étape 2 : configurer le serveur d'autorisation

Vous devez définir au moins un serveur d'autorisation sur ONTAP. Vous devez choisir les valeurs de paramètre en fonction de votre configuration et de votre plan de déploiement. Révision "[Scénarios de déploiement OAuth2](#)" pour déterminer les paramètres exacts nécessaires à votre configuration.



Pour modifier une définition de serveur d'autorisation, vous pouvez supprimer la définition existante et en créer une nouvelle.

L'exemple ci-dessous est basé sur le premier scénario de déploiement simple à l'adresse "[Validation locale](#)". Les oscilloscopes autonomes sont utilisés sans proxy.

Choisissez la procédure appropriée en fonction de votre accès à ONTAP. La procédure CLI utilise des variables symboliques que vous devez remplacer avant d'exécuter la commande.

Exemple 2. Étapes

System Manager

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Faites défiler jusqu'à la section **sécurité**.
3. Cliquez sur **+** en regard de **OAuth 2.0 autorisation**.
4. Sélectionnez **plus d'options**.
5. Indiquez les valeurs requises pour votre déploiement, notamment :
 - Nom
 - Application (http)
 - URI du fournisseur JWKS
 - URI de l'émetteur
6. Cliquez sur **Ajouter**.

CLI

1. Créez à nouveau la définition :

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri  
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

Par exemple :

```
security oauth2 client create \  
-config-name auth0 \  
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-  
realm/protocol/openid-connect/certs \  
-application http \  
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

Étape 3 : activez OAuth 2.0

La dernière étape consiste à activer OAuth 2.0. Il s'agit d'un paramètre global pour le cluster ONTAP.



N'activez pas le traitement OAuth 2.0 tant que vous n'avez pas confirmé que ONTAP, les serveurs d'autorisation et les services de support ont tous été correctement configurés.

Choisissez la procédure appropriée en fonction de votre accès à ONTAP.

Exemple 3. Étapes

System Manager

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Faites défiler jusqu'à la section **sécurité**.
3. Cliquez sur → en regard de **OAuth 2.0 autorisation**.
4. Activer **OAuth 2.0 autorisation**.

CLI

1. Activer OAuth 2.0 :

```
security oauth2 modify -enabled true
```

2. Confirmer que OAuth 2.0 est activé :

```
security oauth2 show  
Is OAuth 2.0 Enabled: true
```

Émettre un appel API REST à l'aide d'OAuth 2.0

L'implémentation OAuth 2.0 dans ONTAP prend en charge les applications clientes de l'API REST. Vous pouvez émettre un appel d'API REST simple en utilisant curl pour commencer à utiliser OAuth 2.0. L'exemple présenté ci-dessous récupère la version du cluster ONTAP.

Avant de commencer

Vous devez configurer et activer la fonction OAuth 2.0 pour votre cluster ONTAP. Cela inclut la définition d'un serveur d'autorisation.

Étape 1 : acquérir un jeton d'accès

Vous devez acquérir un jeton d'accès à utiliser avec l'appel de l'API REST. La requête de jeton est effectuée en dehors de ONTAP et la procédure exacte dépend du serveur d'autorisation et de sa configuration. Vous pouvez demander le token via un navigateur Web, une commande curl ou un langage de programmation.

À des fins d'illustration, un exemple de la façon dont un jeton d'accès peut être demandé à Keycloak à l'aide de curl est présenté ci-dessous.

Exemple de Keycloak

```
curl --request POST \  
--location  
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-  
connect/token' \  
--header 'Content-Type: application/x-www-form-urlencoded' \  
--data-urlencode 'client_id=dp-client-1' \  
--data-urlencode 'grant_type=client_credentials' \  
--data-urlencode 'client_secret=5iTUf9QKLGxAoYaliR33v1D5A2xq09V7'
```

Vous devez copier et enregistrer le jeton renvoyé.

Étape 2 : lancez l'appel de l'API REST

Après avoir un jeton d'accès valide, vous pouvez utiliser une commande curl avec le jeton d'accès pour émettre un appel d'API REST.

Paramètres et variables

Les deux variables de l'exemple curl sont décrites dans le tableau ci-dessous.

Variable	Description
\$FQDN_IP	Nom de domaine complet ou adresse IP du LIF de gestion ONTAP.
\$ACCESS_TOKEN	Jeton d'accès OAuth 2.0 émis par le serveur d'autorisation.

Vous devez d'abord définir ces variables dans l'environnement de shell Bash avant de lancer l'exemple de bouclage. Par exemple, dans l'interface de ligne de commande Linux, tapez la commande suivante pour définir et afficher la variable FQDN :

```
FQDN_IP=172.14.31.224  
echo $FQDN_IP  
172.14.31.224
```

Une fois les deux variables définies dans votre shell Bash local, vous pouvez copier la commande curl et la coller dans l'interface de ligne de commande. Appuyez sur **entrée** pour remplacer les variables et émettre la commande.

Exemple de boucle

```
curl --request GET \  
--location "https://$FQDN_IP/api/cluster?fields=version" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Bearer $ACCESS_TOKEN"
```

Configurez l'authentification SAML

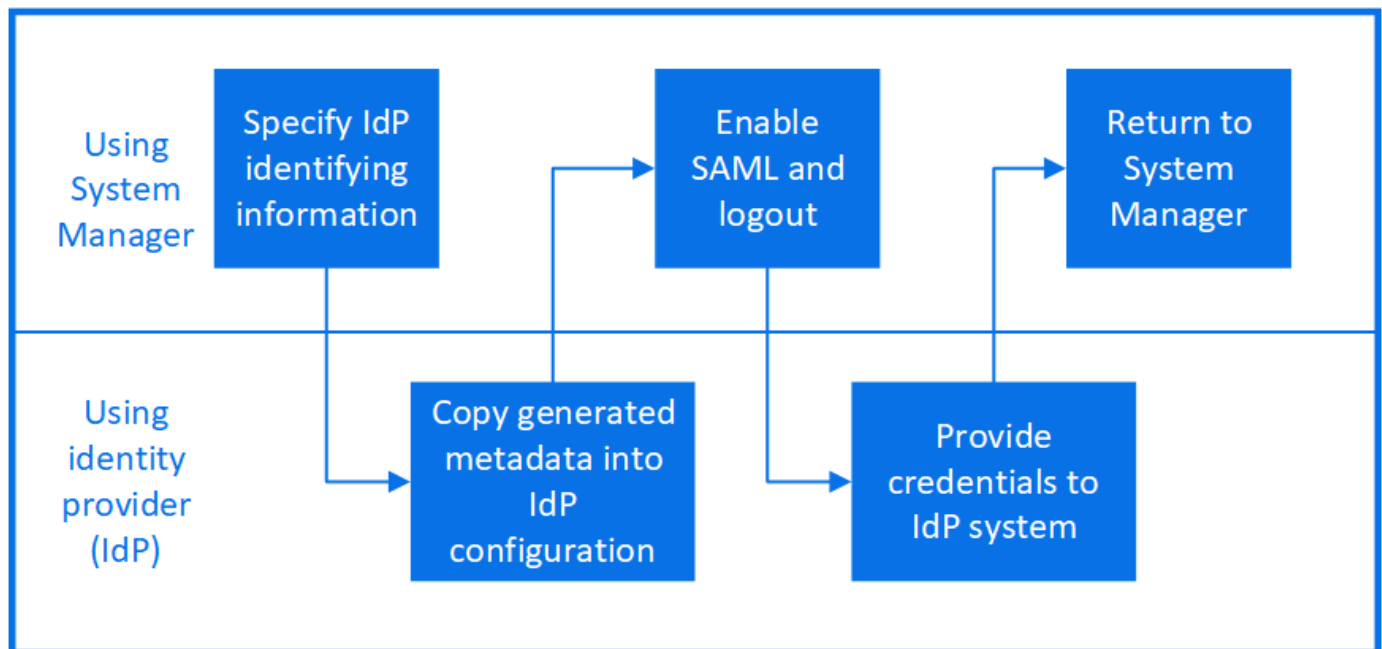
Depuis ONTAP 9.3, vous pouvez configurer l'authentification SAML pour les services Web. Lorsque l'authentification SAML est configurée et activée, les utilisateurs sont authentifiés par un fournisseur d'identité externe (IDP) au lieu des fournisseurs de services d'annuaire tels qu'Active Directory et LDAP.

Activez l'authentification SAML

Pour activer l'authentification SAML avec System Manager ou l'interface de ligne de commandes, effectuez les opérations suivantes. Si votre cluster exécute ONTAP 9.7 ou une version antérieure, les étapes à suivre dans System Manager sont différentes. Consultez l'aide en ligne de System Manager disponible sur votre système.



Après avoir activé l'authentification SAML, seuls les utilisateurs distants peuvent accéder à l'interface graphique de System Manager. Les utilisateurs locaux ne peuvent pas accéder à l'interface graphique de System Manager après l'authentification SAML.



Avant de commencer

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



Consultez la documentation fournie par le PDI que vous avez configuré.

- Vous devez avoir l'URI du IDP.

Description de la tâche

- L'authentification SAML s'applique uniquement au `http` et `ontapi` en termes de latence.

Le `http` et `ontapi` Les applications sont utilisées par les services web suivants : infrastructure processeur de service, API ONTAP ou System Manager.

- L'authentification SAML est applicable uniquement pour l'accès au SVM d'administration.


Les PDI suivants ont été validés avec System Manager :

- Services de fédération Active Directory
- Cisco DUO (validé avec les versions ONTAP suivantes :)
 - 9.7P21 et versions ultérieures 9.7 (voir ["Documentation de System Manager Classic"](#))
 - 9.8P17 et versions ultérieures 9.8
 - 9.9.1P13 et versions ultérieures 9.9
 - 9.10.1P9 et versions ultérieures 9.10
 - 9.11.1P4 et versions ultérieures 9.11
 - versions 9.12.1 et ultérieures
- Hurlent

Effectuez les opérations suivantes en fonction de votre environnement :

Exemple 4. Étapes

System Manager

1. Cliquez sur **Cluster > Paramètres**.
2. En regard de **authentification SAML**, cliquez sur .
3. Vérifiez que la case **Activer l'authentification SAML** est cochée.
4. Entrez l'URL de l'URI IDP (y compris "https://").
5. Modifiez l'adresse du système hôte, si nécessaire.
6. Assurez-vous que le bon certificat est utilisé :
 - Si votre système a été mappé avec un seul certificat de type « serveur », ce certificat est considéré comme le certificat par défaut et il n'est pas affiché.
 - Si votre système a été mappé avec plusieurs certificats comme type « serveur », l'un des certificats s'affiche. Pour sélectionner un autre certificat, cliquez sur **Modifier**.
7. Cliquez sur **Enregistrer**. Une fenêtre de confirmation affiche les informations sur les métadonnées, qui ont été automatiquement copiées dans le presse-papiers.
8. Accédez au système IDP que vous avez spécifié et copiez les métadonnées de votre presse-papiers pour mettre à jour les métadonnées système.
9. Revenez à la fenêtre de confirmation (dans System Manager) et cochez la case **J'ai configuré le IDP avec l'URI hôte ou les métadonnées**.
10. Cliquez sur **Déconnexion** pour activer l'authentification SAML. Le système IDP affiche un écran d'authentification.
11. Dans le système IDP, saisissez vos identifiants SAML. Une fois vos identifiants vérifiés, vous accédez à la page d'accueil de System Manager.

CLI

1. Créez une configuration SAML pour que ONTAP puisse accéder aux métadonnées IDP :

```
security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name
```

`idp_uri` Est l'adresse FTP ou HTTP de l'hôte IDP à partir de laquelle les métadonnées IDP peuvent être téléchargées.

`ontap_host_name` Est le nom d'hôte ou l'adresse IP de l'hôte du fournisseur de services SAML, qui, dans le cas présent, correspond au système ONTAP. Par défaut, l'adresse IP de la LIF de cluster-management est utilisée.

Vous pouvez éventuellement fournir les informations de certificat de serveur ONTAP. Par défaut, les informations de certificat de serveur Web ONTAP sont utilisées.


```
cluster_12::> security saml-sp create -idp-uri  
https://example.url.net/idp/shibboleth
```

Warning: This restarts the web server. Any HTTP/S connections that are active

will be disrupted.

Do you want to continue? {y|n}: y

[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server domain to ensure that users are the same for different authentication methods. See the "security login show" command for the Data ONTAP user configuration.

L'URL permettant d'accéder aux métadonnées de l'hôte ONTAP s'affiche.

2. À partir de l'hôte IDP, configurez le IDP avec les métadonnées de l'hôte ONTAP.

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

3. Activer la configuration SAML :

```
security saml-sp modify -is-enabled true
```

Tout utilisateur existant qui accède à l' http ou ontapi L'application est automatiquement configurée pour l'authentification SAML.

4. Si vous souhaitez créer des utilisateurs pour le http ou ontapi Application après la configuration de SAML, spécifiez SAML comme méthode d'authentification pour les nouveaux utilisateurs.

- a. Créez une méthode de connexion pour les nouveaux utilisateurs avec l'authentification SAML :

```
security login create -user-or-group-name user_name -application [http |  
ontapi] -authentication-method saml -vserver svm_name
```

```
cluster_12::> security login create -user-or-group-name admin1  
-application http -authentication-method saml -vserver  
cluster_12
```

- b. Vérifiez que l'entrée utilisateur est créée :

```
security login show
```

```
cluster_12::> security login show
```

```
Vserver: cluster_12
```

```
Second
```

User/Group	Authentication	Acct
Name	Application Method	Role Name
Method		Locked
admin	console	password
none		admin
admin	http	password
none		admin
admin	http	saml
none		admin
admin	ontapi	password
none		admin
admin	ontapi	saml
none		admin
admin	service-processor	password
none		admin
admin	ssh	password
none		admin
admin1	http	password
none		backup
**admin1	http	saml
none**		backup


Désactivez l'authentification SAML

Vous pouvez désactiver l'authentification SAML lorsque vous souhaitez arrêter l'authentification des utilisateurs Web à l'aide d'un fournisseur d'identité externe (IDP). Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés tels qu'Active Directory et LDAP sont utilisés pour l'authentification.

Effectuez les opérations suivantes en fonction de votre environnement :

Exemple 5. Étapes

System Manager

1. Cliquez sur **Cluster > Paramètres**.
2. Sous **authentification SAML**, cliquez sur le bouton bascule **activé**.
3. *Facultatif* : vous pouvez également cliquer sur  En regard de **SAML Authentication**, puis décochez la case **Activer l'authentification SAML**.

CLI

1. Désactiver l'authentification SAML :

```
security saml-sp modify -is-enabled false
```

2. Si vous ne souhaitez plus utiliser l'authentification SAML ou si vous souhaitez modifier l'IDP, supprimez la configuration SAML :

```
security saml-sp delete
```

Résolution des problèmes liés à la configuration SAML

Si la configuration de l'authentification SAML échoue, vous pouvez réparer manuellement chaque nœud sur lequel la configuration SAML a échoué et effectuer une restauration suite à la défaillance. Au cours du processus de réparation, le serveur Web est redémarré et toutes les connexions HTTP ou HTTPS actives sont interrompues.

Description de la tâche

Lorsque vous configurez l'authentification SAML, ONTAP applique la configuration SAML par nœud. Lorsque vous activez l'authentification SAML, ONTAP tente automatiquement de réparer chaque nœud en cas de problèmes de configuration. Si la configuration SAML est problématique sur n'importe quel nœud, vous pouvez désactiver l'authentification SAML, puis réactiver l'authentification SAML. Lorsque la configuration SAML ne s'applique pas à un ou plusieurs nœuds, même après la réactivation de l'authentification SAML, cela peut se présenter. Vous pouvez identifier le nœud sur lequel la configuration SAML a échoué, puis réparer manuellement ce nœud.

Étapes

1. Connectez-vous au niveau de privilège avancé :

```
set -privilege advanced
```

2. Identifiez le nœud sur lequel la configuration SAML a échoué :

```
security saml-sp status show -instance
```

```
cluster_12::*> security saml-sp status show -instance

Node: node1
Update Status: config-success
Database Epoch: 9
Database Transaction Count: 997
Error Text:
SAML Service Provider Enabled: false
ID of SAML Config Job: 179

Node: node2
Update Status: config-failed
Database Epoch: 9
Database Transaction Count: 997
Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
ID of SAML Config Job: 180
2 entries were displayed.
```

3. Corrigez la configuration SAML sur le nœud défaillant :

security saml-sp repair -node *node_name*

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

Le serveur Web est redémarré et toutes les connexions HTTP ou HTTPS actives sont interrompues.

4. Vérifiez que le langage SAML est configuré sur tous les nœuds :

security saml-sp status show -instance

```
cluster_12::*> security saml-sp status show -instance
```

```

                Node: node1
            Update Status: config-success
        Database Epoch: 9
    Database Transaction Count: 997
        Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                Node: node2
            Update Status: **config-success**
        Database Epoch: 9
    Database Transaction Count: 997
        Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

Informations associées

["Commandes de ONTAP 9"](#)

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

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 « core dump » d'un nœud, la `spi` le service web crée automatiquement un point de montage d'un nœud vers le volume racine d'un autre nœud où les fichiers résident. 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

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.
- 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 TLSv1.2 et TLSv1.3 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 ou TLSv1.3 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.

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 de 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 : <ul style="list-style-type: none"> • 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) 	<code>system services web modify</code>
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	<code>system services web show</code>
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	<code>system services web node show</code>
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	<code>system services firewall policy create</code> Réglage du <code>-service</code> paramètre à <code>http</code> ou <code>https</code> permet aux demandes d'accès web de passer par le pare-feu.

Les fonctions que vous recherchez...	Utilisez cette commande...
Associer une politique de pare-feu à une LIF	<pre>network interface modify</pre> <p>Vous pouvez utiliser le <code>-firewall-policy</code> Paramètre pour modifier la politique de pare-feu d'une LIF.</p>

Configurer l'accès aux services Web

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.

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

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.
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.

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.



Vous utilisez le `security login create` commande permettant d'ajouter une méthode d'accès pour un utilisateur.

Commandes 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 : <ul style="list-style-type: none">• Activer ou désactiver un service Web• Spécifiez si seul HTTPS peut être utilisé pour accéder à un service Web	<code>vserver services web modify</code>
Afficher la configuration et la disponibilité des services web pour le cluster ou anSVM	<code>vserver services web show</code>
Autoriser un rôle à accéder à un service web sur le cluster ou anSVM	<code>vserver services web access create</code>
Afficher les rôles autorisés pour accéder aux services web sur le cluster ou anSVM	<code>vserver services web access show</code>
Empêcher un rôle d'accéder à un service Web sur le cluster ou anSVM	<code>vserver services web access delete</code>

Informations associées

["Commandes de ONTAP 9"](#)

Commandes permettant de gérer les points de montage sur les nœuds

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	<code>system node root-mount create</code> Un seul point de montage peut exister d'un nœud à un autre.
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	<code>system node root-mount show</code>
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	<code>system node root-mount delete</code>

Informations associées

["Commandes de ONTAP 9"](#)

Gérer SSL

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 la machine virtuelle de stockage (SVM) du cluster ora.



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



Résoudre les problèmes d'accès au service Web


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 <code>unable to connect</code> ou <code>failure to establish a connection</code> 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. <div>  <p>Vous utilisez le <code>network ping</code> Commande ping d'une LIF. Pour plus d'informations sur la configuration du réseau, reportez-vous au <i>Network Management Guide</i>.</p> </div>
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. <div>  <p>Vous utilisez le <code>system services firewall policy</code> commandes permettant de gérer les politiques de pare-feu. Vous utilisez le <code>network interface modify</code> commande avec <code>-firewall -policy</code> Paramètre pour associer une policy à une LIF.</p> </div>	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...
<p>Assurez-vous que le moteur de protocole Web est activé pour que les services Web soient accessibles.</p> <div data-bbox="167 464 220 516">  </div> <div data-bbox="277 373 535 609"> <p>Vous utilisez le <code>system services web</code> commandes permettant de gérer le moteur de protocole web pour le cluster.</p> </div>	<p>Votre navigateur Web renvoie un <code>not found</code> erreur lorsque vous essayez d'accéder à un service web.</p>	<p>Le service Web est peut-être désactivé.</p>
<p>Assurez-vous que chaque service Web auquel vous souhaitez autoriser l'accès est activé individuellement.</p> <div data-bbox="167 947 220 999">  </div> <div data-bbox="277 852 535 1087"> <p>Vous utilisez le <code>vserver services web modify</code> commande permettant d'activer un service web pour l'accès.</p> </div>	<p>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.</p>	<p>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.</p>

Ce problème d'accès...	Se produit en raison de cette erreur de configuration...	Pour résoudre l'erreur...
<p>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.</p> <div data-bbox="167 926 220 982">  </div> <p>Vous utilisez le <code>security login</code> 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 <code>ontapi</code> méthode d'accès. L'accès à tous les autres services Web nécessite le <code>http</code> méthode d'accès. Vous utilisez le <code>vserver</code> <code>services web</code> <code>access</code> commandes permettant de gérer l'accès d'un rôle à un service web.</p>	<p>Vous vous connectez à votre service Web via HTTPS et votre navigateur Web indique que votre connexion est interrompue.</p>	<p>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.</p>

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

Vérifiez l'identité des serveurs distants à l'aide de certificats

Vérifiez l'identité des serveurs distants à l'aide de la présentation des certificats

ONTAP prend en charge les fonctions de certificat de sécurité pour vérifier l'identité des serveurs distants.

Le logiciel ONTAP permet des connexions sécurisées à l'aide des fonctionnalités et protocoles de certificat numérique suivants :

- 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). Cette fonction est désactivée par défaut.
- Un ensemble par défaut de certificats racine de confiance est inclus avec le logiciel ONTAP.
- Les certificats KMIP (Key Management Interoperability Protocol) permettent d'effectuer une authentification mutuelle d'un cluster et d'un serveur KMIP.

Vérifiez que les certificats numériques sont valides à l'aide du protocole OCSP

Depuis ONTAP 9.2, le protocole OCSP (Online Certificate Status Protocol) permet aux applications ONTAP qui utilisent les communications TLS (transport Layer Security) de recevoir le statut du certificat numérique lorsque le protocole OCSP est activé. Vous pouvez à tout moment activer ou désactiver les vérifications d'état des certificats OCSP pour des applications spécifiques. Par défaut, la vérification du statut du certificat OCSP est désactivée.

Ce dont vous avez besoin

Vous avez besoin d'un accès de niveau de privilège avancé pour effectuer cette tâche.

Description de la tâche

OCSP prend en charge les applications suivantes :

- AutoSupport
- Système de gestion des événements (EMS)
- LDAP sur TLS
- Protocole KMIP (Key Management Interoperability Protocol)
- Consignation d'audits
- FabricPool
- SSH (à partir de ONTAP 9.13.1)

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`.
2. Pour activer ou désactiver les vérifications du statut des certificats OCSP pour des applications ONTAP spécifiques, utilisez la commande appropriée.

Si vous souhaitez que l'état du certificat OCSP soit vérifié pour certaines applications...	Utilisez la commande...
Activé	<code>security config ocsp enable -app app name</code>
Désactivé	<code>security config ocsp disable -app app name</code>

La commande suivante active la prise en charge OCSP pour AutoSupport et EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

Lorsque OCSP est activé, l'application reçoit l'une des réponses suivantes :

- Bon - le certificat est valide et la communication continue.
 - Révoqué - le certificat est considéré comme non digne de confiance par son autorité de certification émettrice et la communication ne peut pas se poursuivre.
 - Inconnu - le serveur n'a pas d'informations d'état sur le certificat et la communication ne peut pas se poursuivre.
 - Il manque des informations de serveur OCSP dans le certificat. Le serveur agit comme si OCSP est désactivé et continue avec la communication TLS, mais aucune vérification d'état n'a lieu.
 - Aucune réponse du serveur OCSP - l'application ne peut pas continuer.
3. Pour activer ou désactiver les vérifications d'état des certificats OCSP pour toutes les applications utilisant les communications TLS, utilisez la commande appropriée.

Si vous souhaitez que l'état du certificat OCSP soit vérifié pour toutes les applications...	Utilisez la commande...
Activé	<pre>security config ocsd enable</pre> <pre>-app all</pre>
Désactivé	<pre>security config ocsd disable</pre> <pre>-app all</pre>

Lorsque cette option est activée, toutes les applications reçoivent une réponse signée indiquant le statut du certificat spécifié : bon, révoqué ou inconnu. Dans le cas d'un certificat révoqué, l'application ne pourra pas continuer. Si l'application ne parvient pas à recevoir de réponse du serveur OCSP ou si le serveur est inaccessible, l'application ne pourra pas continuer.

4. Utilisez le `security config ocsd show` Commande pour afficher toutes les applications qui prennent en charge OCSP et leur état de support.

```
cluster::*> security config ocsd show
Application                                OCSP Enabled?
-----
autosupport                                false
audit_log                                  false
fabricpool                                 false
ems                                         false
kmip                                        false
ldap_ad                                    true
ldap_nis_namemap                           true
ssh                                         true

8 entries were displayed.
```

Afficher les certificats par défaut pour les applications basées sur TLS

Depuis ONTAP 9.2, ONTAP fournit un ensemble par défaut de certificats racine de confiance pour les applications ONTAP utilisant TLS (transport Layer Security).

Ce dont vous avez besoin

Les certificats par défaut ne sont installés que sur le SVM d'admin pendant sa création ou lors d'une mise à niveau vers ONTAP 9.2.

Description de la tâche

Les applications actuelles qui agissent en tant que client et qui nécessitent une validation de certificat sont AutoSupport, EMS, LDAP, Audit Logging, FabricPool, Et KMIP.

Lorsque les certificats expirent, un message EMS est appelé pour demander à l'utilisateur de supprimer les

certificats. Les certificats par défaut ne peuvent être supprimés qu'au niveau de privilège avancé.



La suppression des certificats par défaut peut entraîner l'absence de fonctionnement de certaines applications ONTAP (par exemple, AutoSupport et Audit Logging).

Étape

1. Vous pouvez afficher les certificats par défaut qui sont installés sur le SVM d'admin en utilisant la commande `Security Certificate show` :

`security certificate show -vserver -type server-ca`

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver      Serial Number  Common Name                                     Type
-----
fas2552-2n-abc-3
              01              AAACertificateServices
server-ca
Certificate Authority: AAA Certificate Services
Expiration Date: Sun Dec 31 18:59:59 2028
```

Authentifier mutuellement le cluster et un serveur KMIP

Authentification mutuelle du cluster et présentation d'un serveur KMIP

L'authentification mutuelle du cluster et d'un gestionnaire de clés externe, tel qu'un serveur KMIP (Key Management Interoperability Protocol), permettent au gestionnaire de clés de communiquer avec le cluster via KMIP sur SSL. Dans ce cas, une application ou certaines fonctionnalités (par exemple, la fonctionnalité Storage Encryption) nécessitent des clés sécurisées pour assurer un accès sécurisé aux données.

Générer une demande de signature de certificat pour le cluster

Vous pouvez utiliser le certificat de sécurité `generate-csr` Commande pour générer une requête de signature de certificat (CSR). Après le traitement de votre demande, l'autorité de certification vous envoie le certificat numérique signé.

Ce dont vous avez besoin

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou un administrateur SVM.

Étapes

1. Générer une RSC :

`security certificate generate-csr -common-name FQDN_or_common_name -size 512|1024|1536|2048 -country country -state state -locality locality`

```
-organization organization -unit unit -email-addr email_of_contact -hash  
-function SHA1|SHA256|MD5
```

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

La commande suivante crée une RSC avec une clé privée de 2,048 bits générée par la fonction de hachage SHA256, utilisée par le groupe Software dans LE département IT d'une société dont le nom commun personnalisé est server1.companyname.com, située à Sunnyvale (Californie), aux États-Unis. L'adresse e-mail de l'administrateur du contact SVM est web@example.com. Le système affiche la RSC et la clé privée dans la sortie.

```
cluster1::>security certificate generate-csr -common-name  
server1.companyname.com -size 2048 -country US -state California -  
locality Sunnyvale -organization IT -unit Software -email-addr  
web@example.com -hash-function SHA256  
Certificate Signing Request :  
-----BEGIN CERTIFICATE REQUEST-----  
MIIBGjCBxQIBADBgMRQWEgYDVQQDEwtleGFtcGxlLmNvbTELMakGA1UEBhMCVVMx  
CTAHBgNVBAgTADAEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G  
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApt1nzS  
xOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJbmXuj6U3alwoUsb13wfEvQnHVFNCi  
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBcWUAA0EA6EagLfso5+4g+ejiRKKTUPQO  
UqOUEoKuvxhOvPC2w7b//fNSFsFHVxloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==  
-----END CERTIFICATE REQUEST-----  
Private Key :  
24 | Administrator Authentication and RBAC  
-----BEGIN RSA PRIVATE KEY-----  
MIIBOwIBAAJBAPXFanNoJApt1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJb  
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu  
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM  
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu  
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NctEYxd0Q5  
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA  
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==  
-----END RSA PRIVATE KEY-----  
Note: Please keep a copy of your certificate request and private key  
for future reference.
```

2. Copiez la demande de certificat à partir de la sortie CSR, puis envoyez-la sous forme électronique (par exemple, un courriel) à une autorité de certification tierce approuvée pour signature.

Après le traitement de votre demande, l'AC vous envoie le certificat numérique signé. Vous devez conserver une copie de la clé privée et du certificat numérique signé par l'autorité de certification.

Installez un certificat de serveur signé par l'autorité de certification pour le cluster

Pour permettre à un serveur SSL d'authentifier le cluster ou la machine virtuelle de stockage (SVM) en tant que client SSL, vous installez un certificat numérique avec le type client sur le cluster ou le SVM. Ensuite, vous fournissez le certificat client-CA à l'administrateur du serveur SSL pour l'installation sur le serveur.

Ce dont vous avez besoin

Vous devez déjà avoir installé le certificat root du serveur SSL sur le cluster ou SVM avec le `server-ca` type de certificat.

Étapes

1. Pour utiliser un certificat numérique auto-signé pour l'authentification client, utilisez le `security certificate create` commande avec `type client` paramètre.
2. Pour utiliser un certificat numérique signé par une autorité de certification pour l'authentification client, procédez comme suit :
 - a. Générez une demande de signature de certificat numérique (RSC) à l'aide du certificat de sécurité `generate-csr` commande.

ONTAP affiche la sortie CSR, qui comprend une demande de certificat et une clé privée, et vous rappelle de copier la sortie dans un fichier pour référence ultérieure.
 - b. Envoyez la demande de certificat de la sortie CSR sous forme électronique (par exemple, un courriel) à une autorité de certification approuvée pour signature.

Vous devez conserver une copie de la clé privée et du certificat signé par l'AC pour référence ultérieure.

Après le traitement de votre demande, l'AC vous envoie le certificat numérique signé.

- a. Installez le certificat signé par l'autorité de certification à l'aide du `security certificate install` commande avec `-type client` paramètre.
- b. Entrez le certificat et la clé privée lorsque vous y êtes invité, puis appuyez sur **entrée**.
- c. Entrez tout certificat racine ou intermédiaire supplémentaire lorsque vous y êtes invité, puis appuyez sur **entrée**.

Vous installez un certificat intermédiaire sur le cluster ou le SVM si une chaîne de certificats qui commence à l'autorité de certification racine de confiance et se termine par le certificat SSL qui vous est délivré, manque les certificats intermédiaires. Un certificat intermédiaire est un certificat subordonné délivré par la racine de confiance spécifiquement pour délivrer des certificats de serveur d'entité finale. Le résultat est une chaîne de certificats qui commence au niveau de l'autorité de certification racine de confiance, passe par le certificat intermédiaire et se termine par le certificat SSL qui vous a été délivré.

3. Fournir le `client-ca` Certificat du cluster ou SVM à l'administrateur du serveur SSL pour installation sur le serveur.

Commande du certificat de sécurité `show` avec `-instance` et `-type client-ca` paramètres affiche le `client-ca` informations sur le certificat.

Installez un certificat client signé par une autorité de certification pour le serveur KMIP

Le sous-type de certificat du protocole KMIP (Key Management Interoperability Protocol) (paramètre `-subtype kmip-cert`), ainsi que les types `client` et `serveur-ca`, spécifie que le certificat est utilisé pour authentifier mutuellement le cluster et un gestionnaire de clés externe, comme un serveur KMIP.

Description de la tâche

Installez un certificat KMIP pour authentifier un serveur KMIP en tant que serveur SSL sur le cluster.

Étapes

1. Utilisez le `security certificate install` commande avec `-type server-ca` et `-subtype kmip-cert` Paramètres pour installer un certificat KMIP pour le serveur KMIP.
2. Lorsque vous y êtes invité, entrez le certificat, puis appuyez sur entrée.

ONTAP vous rappelle de conserver une copie du certificat à des fins de référence ultérieure.

```
cluster1::> security certificate install -type server-ca -subtype kmip-  
cert  
-vserver cluster1
```

```
Please enter Certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
```

```
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG  
2JhucwNhkcV8sEVAbkSdjbCxlRhLQ2pRdKkkirWmnWXbj9T/UWZyB2oK0z5XqcJ  
2HUw19JlYDln1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
```

```
...
```

```
-----END CERTIFICATE-----
```

```
You should keep a copy of the CA-signed digital certificate for future  
reference.
```

```
cluster1::>
```

Informations sur le copyright

Copyright © 2024 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 DÉLICTELLE (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.