Authentification et contrôle d'accès

ONTAP 9

NetApp
February 13, 2026

Sommaire

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 le Gestionnaire système classique (disponible uniquement dans ONTAP 9.7 et versions antérieures), reportez-vous à la section "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

En savoir plus sur l’authentification administrateur et le contrôle d’accès basé sur des rôles dans ONTAP

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 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"

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

- "LDAP ou NIS"

  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.

Authentification d'administrateur ONTAP 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.

Fiche de configuration complète

Avant de créer des comptes de connexion et de configurer le contrôle d'accès basé sur les rôles (RBAC), vous devez recueillir des informations pour chaque élément de la "feuilles de calcul de configuration".

Déterminez si le compte administrateur est local ou distant

- **Si local:** Activer "mot de passe", , "SSH", "AUTHENTIFICATION SSH"ou "SSL" accès.
- **Si distant:** déterminer le type d'accès distant. Selon le type d'accès, "Activez l'accès à Active Directory", "Activez l'accès LDAP ou NIS"ou "Configuration de l'authentification SAML (uniquement pour le SVM d'administration)".

Configurez l'accès basé sur les rôles

Le rôle attribué à un administrateur détermine les commandes auxquelles l'administrateur a accès. Le rôle est attribué lors de la création du compte administrateur et peut être "modifié" ultérieurement. Vous pouvez utiliser des rôles prédéfinis pour "cluster" et "SVM" les administrateurs, ou "définir des rôles personnalisés" selon les besoins.

Gestion des comptes d'administrateur

Selon la manière dont vous avez activé l'accès au compte, vous devrez peut-être associer un "clé publique avec un compte local" , gérer "Clés publiques et certificats X.509" , configurer "Cisco Duo 2FA pour les connexions SSH" , installer un "Certificat numérique de serveur signé CA" , ou configurer "Active Directory" , "LDAP ou NIS" accès. Vous pouvez effectuer l'une de ces tâches avant ou après l'activation de l'accès au compte.

Configurer des fonctions de sécurité supplémentaires

- "Gestion de la vérification multi-administrateurs" si vous souhaitez vous assurer que certaines opérations nécessitent l'approbation des administrateurs désignés.
- "Gérer l'autorisation dynamique" si vous souhaitez appliquer dynamiquement des contrôles d'autorisation supplémentaires basés sur le niveau de confiance d'un utilisateur.
- "Configurer l'élévation des privilèges juste-à-temps (JIT)" si vous souhaitez autoriser les utilisateurs à accéder temporairement à des privilèges élevés pour effectuer certaines tâches.

Feuilles de calcul pour l'authentification de l'administrateur ONTAP 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.

Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Créer ou modifier des comptes de connexion

Vous fournissez ces valeurs avec la `security login create` commande lorsque vous activez l'accès des comptes de connexion à une VM de stockage. Pour en savoir plus, `security login create` consultez le "Référence de commande ONTAP".

Vous fournissez les mêmes valeurs avec la `security login modify` commande lorsque vous modifiez la façon dont un compte accède à une VM de stockage. Pour en savoir plus, `security login modify` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	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.	
`-user-or-group-name`	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.	
`-application`	L'application utilisée pour accéder à la VM de stockage : • `http` • `ontapi` • `snmp` • `ssh`	

`-authmethod`	Méthode utilisée pour authentifier le compte : • `cert` Pour l'authentification par certificat SSL • `domain` Pour l'authentification Active Directory • `nsswitch` Pour l'authentification LDAP ou NIS • `password` pour l'authentification par mot de passe utilisateur • `publickey` pour l'authentification par clé publique • `community` Pour les chaînes de communauté SNMP • `usm` Pour le modèle de sécurité utilisateur SNMP • `saml` Pour l'authentification SAML (Security assertion Markup Language)	
`-remote-switch-ipaddress`	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 `snmp` et la méthode d'authentification est `usm`.	
`-role`	Rôle de contrôle d'accès attribué au compte : • Pour le cluster (la VM de stockage admin), la valeur par défaut est `admin`. • Pour une VM de stockage de données, la valeur par défaut est `vsadmin`.	

`-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`	Deuxième méthode d'authentification en cas d'authentification multifacteur : • `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 L'ordre d'authentification est toujours la clé publique suivie du mot de passe.	
`-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 la liaison rapide LDAP, la `-authentication-method` valeur doit être définie sur `nsswitch`. "Utiliser la liaison rapide LDAP pour l'authentification nsswitch pour les SVM NFS ONTAP".	

Configurer les informations de sécurité Cisco Duo

Vous fournissez ces valeurs avec la `security login duo create` commande lorsque vous activez l'authentification à deux facteurs Cisco Duo avec des connexions SSH pour une VM de stockage. Pour en savoir plus, `security login duo create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	La VM de stockage (appelée vServer dans l'interface de ligne de commandes ONTAP) à laquelle s'appliquent les paramètres d'authentification Duo.	
`-integration-key`	Votre clé d'intégration, obtenue lors de l'enregistrement de votre application SSH auprès de Duo.	
`-secret-key`	Votre clé secrète, obtenue lors de l'enregistrement de votre application SSH auprès de Duo.	
`-api-host`	Le nom d'hôte de l'API, obtenu lors de l'enregistrement de votre application SSH auprès de Duo. Par exemple : `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	En cas d'erreurs de service ou de configuration qui empêchent l'authentification Duo, l'échec `safe` (autoriser l'accès) ou `secure` (refuser l'accès). La valeur par défaut est `safe`, 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`	Utilisez le proxy HTTP spécifié. Si le proxy HTTP nécessite une authentification, incluez les informations d'identification dans l'URL du proxy. Par exemple : `http-proxy=http://username:password@proxy.example.org:8080`	
`-autopush`	Soit `true` ou `false`. La valeur par défaut est `false`. Si `true`, 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 `false`, l'utilisateur est invité à choisir une méthode d'authentification. Lorsqu'il est configuré avec `autopush = true`, nous recommandons le réglage `max-prompts = 1`.	

`-max-prompts`	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`. Par exemple, quand `max-prompts = 1`, l'utilisateur doit s'authentifier avec succès à la première invite, tandis que si `max-prompts = 2`, si l'utilisateur saisit des informations incorrectes à l'invite initiale, il sera invité à s'authentifier à nouveau. Lorsqu'il est configuré avec `autopush = true`, nous recommandons le réglage `max-prompts = 1`. Pour la meilleure expérience, un utilisateur avec seulement l'authentification de clé publique aura toujours `max-prompts` réglez sur `1`.	
`-enabled`	Activez l'authentification Duo à deux facteurs. Réglez sur `true` 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 `false`), l'authentification Duo est ignorée.	
`-pushinfo`	Cette option fournit des informations supplémentaires dans la notification Push, telles que le nom de l'application ou du service auquel vous accédez. Cela permet aux utilisateurs de vérifier qu'ils se connectent au service approprié et fournit une couche de sécurité supplémentaire.	

Définissez des rôles personnalisés

Vous fournissez ces valeurs avec `security login role create` la commande lorsque vous définissez un rôle personnalisé. Pour en savoir plus, `security login role create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	(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`	(Facultatif) le niveau d'accès du rôle. Pour les répertoires de commandes : • `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 Pour *commandes non intrinsèques* (commandes qui ne se terminent pas dans `create`, `modify`, `delete`, ou `show`) : • `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 Pour accorder ou refuser l'accès aux commandes intrinsèques, vous devez spécifier le répertoire de commande.	
`-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 `volume`, l'objet requête `"-aggr aggr0"` activation de l'accès pour le système `aggr0` agrégat uniquement.	

Associer une clé publique à un compte d'utilisateur

Vous fournissez ces valeurs avec `security login publickey create` la commande lorsque vous associez une clé publique SSH à un compte utilisateur. Pour en savoir plus, `security login publickey create` consultez le "Référence de commande ONTAP".

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, `admin`, 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`	(Facultatif) à partir de ONTAP 9.13.1, vous permet de gérer l'association de certificats X.509 avec la clé publique SSH. 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 : • `install`: 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. • `modify`: 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. • `delete`: Supprimez l'association de certificat X.509 existante avec la clé publique SSH.	

Configurer les paramètres globaux d'autorisation dynamique

Depuis ONTAP 9.15.1, vous fournissez ces valeurs avec la `security dynamic-authorization modify` commande. Pour en savoir plus, `security dynamic-authorization modify` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	Nom de la machine virtuelle de stockage pour laquelle le paramètre de score de confiance doit être modifié. Si vous omettez ce paramètre, le paramètre de niveau du cluster est utilisé.	

`-state`	Le mode d'autorisation dynamique. Valeurs possibles : • `disabled`: (Par défaut) l'autorisation dynamique est désactivée. • `visibility`: Ce mode est utile pour tester l'autorisation dynamique. Dans ce mode, le score de confiance est vérifié avec chaque activité restreinte, mais pas appliqué. Cependant, toute activité qui aurait été refusée ou qui aurait fait l'objet de défis d'authentification supplémentaires est consignée. • `enforced`: Destiné à être utilisé après avoir terminé les tests avec `visibility` mode. Dans ce mode, le score de confiance est vérifié pour chaque activité restreinte et les restrictions d'activité sont appliquées si les conditions de restriction sont remplies. L'intervalle de suppression est également appliqué, ce qui évite des problèmes d'authentification supplémentaires dans l'intervalle spécifié.	
`-suppression-interval`	Empêche des problèmes d'authentification supplémentaires dans l'intervalle spécifié. L'intervalle est au format ISO-8601 et accepte des valeurs comprises entre 1 minute et 1 heure. Si la valeur est définie sur 0, l'intervalle de suppression est désactivé et l'utilisateur est toujours invité à effectuer une vérification d'authentification si nécessaire.	
`-lower-challenge-boundary`	Limite inférieure de pourcentage de défi pour l'authentification multifacteur (MFA). La plage valide est comprise entre 0 et 99. La valeur 100 n'est pas valide, car toutes les demandes sont refusées. La valeur par défaut est 0.	

`-upper-challenge-boundary`	Limite supérieure de pourcentage de défi MFA. La plage valide est comprise entre 0 et 100. Cette valeur doit être égale ou supérieure à la valeur de la limite inférieure. Une valeur de 100 signifie que chaque demande sera refusée ou soumise à un défi d'authentification supplémentaire ; aucune demande n'est autorisée sans défi. La valeur par défaut est 90.	

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

Vous fournissez ces valeurs avec `security certificate generate-csr` la commande 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. Pour en savoir plus, `security certificate generate-csr` consultez le "Référence de commande ONTAP".

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`.	
`-country`	Pays de la machine virtuelle de stockage, sous un code à deux lettres. La valeur par défaut est `US`. Pour obtenir une liste des codes, reportez-vous à la "Référence de commande ONTAP".	
`-state`	État ou province de la machine virtuelle de stockage.	
`-locality`	Localité de la VM de stockage.	
`-organization`	Organisation de la machine virtuelle de stockage.	
`-unit`	Unité dans l'organisation de la machine virtuelle de stockage.	

`-email-addr`	Adresse e-mail de l'administrateur du contact pour la machine virtuelle de stockage.	
`-hash-function`	Fonction de hachage cryptographique pour la signature du certificat. La valeur par défaut est `SHA256`. Les valeurs possibles sont `SHA1`, `SHA256`, et `MD5`.	

Vous fournissez ces valeurs avec `security certificate install` la commande 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. Pour en savoir plus, `security certificate install` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	Nom de la machine virtuelle de stockage sur laquelle le certificat doit être installé.	
`-type`	Le type de certificat : • `server` pour les certificats de serveur et les certificats intermédiaires • `client-ca` Pour le certificat de clé publique de l'autorité de certification racine du client SSL • `server-ca` Pour le certificat de clé publique de l'autorité de certification racine du serveur SSL dont ONTAP est un client • `client` 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 la `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. Pour en savoir plus, `security login domain-tunnel create` consultez le "Référence de commande ONTAP".

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

Vous fournissez ces valeurs avec la `vserver active-directory create` commande 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. Pour en savoir plus, `vserver active-directory create` consultez le "Référence de commande ONTAP".

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 la `vserver services name-service ldap client create` commande lorsque vous créez une configuration client LDAP pour la machine virtuelle de stockage. Pour en savoir plus, `vserver services name-service ldap client create` consultez le "Référence de commande ONTAP".

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`	Si le client utilise Start TLS pour chiffrer la communication avec le serveur LDAP (`true` ou `false`). 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.	

Vous fournissez ces valeurs avec la `vserver services name-service ldap create` commande lorsque vous associez une configuration client LDAP à la machine virtuelle de stockage. Pour en savoir plus, `vserver services name-service ldap create` consultez le "Référence de commande ONTAP".

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

Vous fournissez ces valeurs avec la `vserver services name-service nis-domain create` commande lorsque vous créez une configuration de domaine NIS sur une machine virtuelle de stockage. Pour en savoir plus, `vserver services name-service nis-domain create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur

`-vserver`	Nom de la machine virtuelle de stockage sur laquelle la configuration de domaine doit être créée.	
`-domain`	Le nom du domaine.	
`-nis-servers`	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 la `vserver services name-service ns-switch create` commande lorsque vous spécifiez l'ordre de recherche des sources de service de noms. Pour en savoir plus, `vserver services name-service ns-switch create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	Nom de la machine virtuelle de stockage sur laquelle l'ordre de recherche de service de noms doit être configuré.	
`-database`	La base de données du service de noms : • `hosts` Pour les services de noms DNS et de fichiers • `group` Pour les fichiers, LDAP et services de noms NIS • `passwd` Pour les fichiers, LDAP et services de noms NIS • `netgroup` Pour les fichiers, LDAP et services de noms NIS • `namemap` Pour les fichiers et les services de noms LDAP	
`-sources`	Ordre dans lequel rechercher les sources de service de noms (dans une liste séparée par des virgules) : • `files` • `dns` • `ldap` • `nis`	

Configurez l'accès SAML

Depuis ONTAP 9.3, vous fournissez ces valeurs avec la `security saml-sp create` commande pour configurer l'authentification SAML. Pour en savoir plus, `security saml-sp create` consultez le "Référence de commande ONTAP".

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.	
`-cert-ca` et `-cert-serial`, ou `-cert-common-name`	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.	
`-verify-metadata-server`	Indique si l'identité du serveur de métadonnées IDP doit être validée `true` ou `false`). Il est recommandé de toujours définir cette valeur sur `true`.	

Créer des comptes de connexion

En savoir plus sur la création de comptes de connexion ONTAP

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

En savoir plus sur l'activation de l'accès à un compte ONTAP 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 `security login create` la commande pour permettre aux comptes locaux d'accéder à un SVM d'administrateur ou de données.

Informations associées

- "création d'une connexion de sécurité"

Activez l'accès par mot de passe du compte ONTAP

Vous pouvez utiliser `security login create` la commande pour permettre aux comptes d'administrateur d'accéder à un SVM d'admin ou 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 sûr du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser `security login modify` la commande pour ajouter le rôle ultérieurement.

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

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`*

   La commande suivante active le compte d'administrateur du cluster `admin1` avec le prédéfini `backup` Rôle d'accès à la SVM d'admin`engCluster` 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
   ```

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

Activez l'accès à la clé publique SSH du compte ONTAP

Vous pouvez utiliser `security login create` la commande pour permettre aux comptes d'administrateur d'accéder à un SVM d'administration ou de données 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 sûr du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser `security login modify` la commande pour ajouter le rôle ultérieurement.

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

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
   ```

   La commande suivante active le compte d'administrateur du SVM `svmadmin1` avec le prédéfini `vsadmin-`

`volume` Rôle d'accès à la SVM`engData1` Utilisation d'une clé publique SSH :

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

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

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)

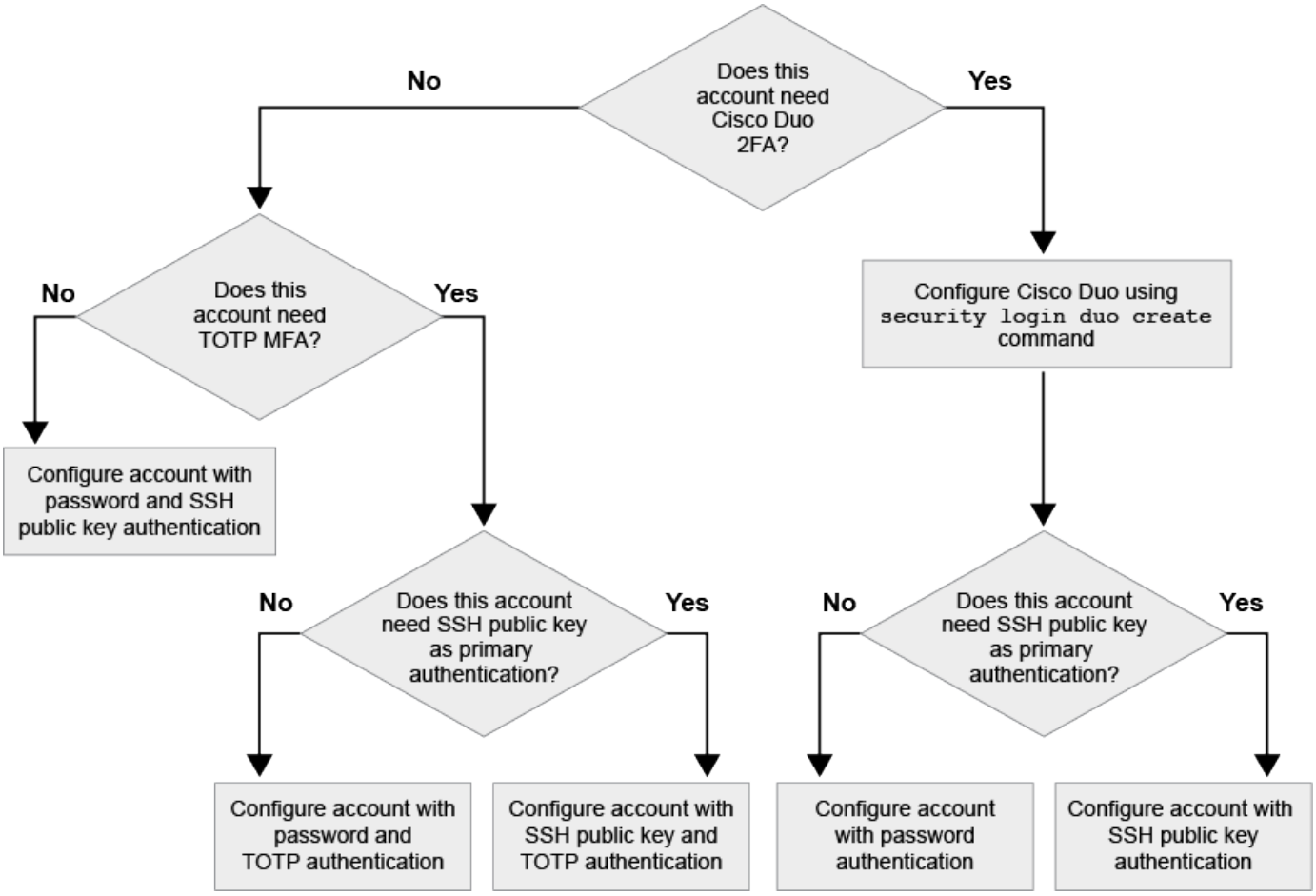
En savoir plus sur l'authentification multifacteur ONTAP

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 ONTAP avec SSH et TOTP

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 sûr du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser `security login modify` la commande pour ajouter le rôle ultérieurement.

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

  "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".
```

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

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>
   ```

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

2. Vérifier que MFA avec TOTP est activé :

```
security login show
```

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

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

- "Authentification multifactorielle dans ONTAP 9 (TR-4647)"
- "Référence de commande ONTAP"

Configurez les comptes utilisateur ONTAP locaux pour MFA avec TOTP

À partir de la version 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.

  Microsoft Authenticator, Google Authenticator, Authy et tout autre authentificateur compatible TOTP sont pris en charge.

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>"
```

Informations associées

- "connexion de sécurité totp créer"
- "connexion de sécurité totp show"

Réinitialisez la clé secrète TOTP pour un compte d'utilisateur ONTAP

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>
```

Informations associées

- "connexion de sécurité totp créer"
- "connexion de sécurité totp supprimer"
- "connexion de sécurité totp show"

Désactivez la clé secrète TOTP pour un compte d'utilisateur ONTAP

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 modify -vserver <svm_name> -username
<account_username> -enabled false
```

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

Activez l'accès au compte ONTAP du certificat SSL

Vous pouvez utiliser `security login create` la commande pour permettre aux comptes d'administrateur d'accéder à un SVM d'administrateur 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
   ```

   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
   ```

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

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

Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Activez l'accès au compte ONTAP Active Directory

Vous pouvez utiliser `security login create` la commande pour permettre aux comptes d'utilisateur ou de groupe Active Directory d'accéder à un SVM d'administrateur 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.

- A partir de ONTAP 9.11.1, vous pouvez utiliser "Utiliser la liaison rapide LDAP pour l'authentification nsswitch pour les SVM NFS ONTAP" si le serveur LDAP AD le prend en charge.
- Si vous n'êtes pas sûr du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser `security login modify` la commande pour ajouter le rôle ultérieurement.

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

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

Version ONTAP	Authentification principale	Authentification secondaire	Commande

9.13.1 et versions ultérieures	Domaine	Clé publique	**Pour un nouvel utilisateur**
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			Pour un utilisateur existant
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

9.0 et versions ultérieures	Domaine	Aucune	`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]`

Pour les groupes AD :

Version ONTAP	Authentification principale	Authentification secondaire	Commande
9.0 et versions ultérieures	Domaine	Aucune	`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]`

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

Informations associées

- "création d'une connexion de sécurité"

Activez l'accès au compte ONTAP LDAP ou NIS

Vous pouvez utiliser `security login create` la commande pour permettre aux comptes utilisateur LDAP ou NIS d'accéder à un SVM d'administration ou de données. 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 sûr du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser `security login modify` la commande pour ajouter le rôle ultérieurement.

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

  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.
- A partir de ONTAP 9.11.1, vous pouvez utiliser "Utiliser la liaison rapide LDAP pour l'authentification nsswitch pour les SVM NFS ONTAP" si le serveur LDAP le prend en charge.
- 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]
   ```

   "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'admin`engCluster`.

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

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

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

Informations associées

- "connexion de sécurité"

Gestion des rôles de contrôle d'accès

En savoir plus sur la gestion des rôles de contrôle d'accès ONTAP

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.

Modifier le rôle attribué à un administrateur ONTAP

Vous pouvez utiliser `security login modify` la commande pour modifier le rôle d'un compte d'administrateur de cluster ou 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
   ```

   "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
   ```

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

Définissez des rôles personnalisés pour les administrateurs ONTAP

Vous pouvez utiliser `security login role create` la 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
   ```

   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
   ```

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

Informations associées

- "création d'un rôle de connexion de sécurité"
- "plex hors ligne de l'agrégat de stockage"
- "chiffrement du stockage"

Rôles prédéfinis pour les administrateurs du cluster ONTAP

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	• Tous les répertoires de commandes (`DEFAULT`) • `security login rest-role` • `security login role`
Lecture seule	• `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
• `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
• `security login password` Pour la gestion du mot de passe local et des informations clés du compte utilisateur • `set`	• À partir de ONTAP 9.8, lecture seule • Avant ONTAP 9.8, aucune	`security`
lecture seule	Tous les autres répertoires de commandes (`DEFAULT`)	SnapLock
tous	• `set` • `volume create` • `volume modify` • `volume move` • `volume show`	Aucune
• `volume move governor` • `volume move recommend`	Aucune	Tous les autres répertoires de commandes (`DEFAULT`)
Aucune	Aucune	Tous les répertoires de commandes (`DEFAULT`)

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.

Informations associées

- "connexion de sécurité"

- "jeu"
- "volumétrie"
- "services vserver ndmp"

Rôles prédéfinis pour les administrateurs des SVM ONTAP

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	• 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 snapshots 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	• 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 snapshots 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	• 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	• 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 snapshots • Affichage des volumes et des informations réseau
vsadmin-snaplock	• 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 snapshots 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	• 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

Gérez l'accès de l'administrateur ONTAP avec System Manager

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 → en regard 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 ⋮ qui s'affiche en regard du nom d'utilisateur.
3. Cliquez sur **Modifier**.
4. Sélectionnez un rôle dans le menu déroulant pour **role**.

Élévation des privilèges d'accès JIT dans ONTAP

À partir d' ONTAP 9.17.1, les administrateurs de cluster peuvent "configurer l'élévation des privilèges juste-à-temps (JIT)" Pour permettre aux utilisateurs ONTAP d'élever temporairement leurs privilèges afin d'effectuer certaines tâches. Lorsque JIT est configuré pour un utilisateur, celui-ci peut temporairement élever ses privilèges à un rôle disposant des autorisations nécessaires pour effectuer une tâche. Après l'expiration de la session, l'utilisateur retrouve son niveau d'accès initial.

Les administrateurs de cluster peuvent configurer la durée d'accès d'un utilisateur à l'élévation JIT. Par exemple, ils peuvent configurer l'accès utilisateur à l'élévation JIT avec une limite de 30 minutes par session (période de validité de session) pendant une période de 30 jours (période de validité JIT). Pendant cette

période, l'utilisateur peut élever ses privilèges autant de fois que nécessaire, mais chaque session est limitée à 30 minutes.

Description de la tâche

- L'élévation des privilèges JIT est réservée aux utilisateurs accédant à ONTAP via SSH. L'élévation des privilèges n'est disponible que dans la session SSH en cours, mais vous pouvez élever les privilèges dans autant de sessions SSH simultanées que nécessaire.
- L'élévation des privilèges JIT n'est prise en charge que pour les utilisateurs utilisant un mot de passe, un commutateur NSSwitch ou une authentification de domaine pour se connecter. L'authentification multifacteur (MFA) n'est pas prise en charge pour l'élévation des privilèges JIT.
- La session JIT d'un utilisateur sera terminée si la session configurée ou la période de validité JIT expire, ou si un administrateur de cluster révoque l'accès JIT pour l'utilisateur.

Avant de commencer

- Pour accéder à l'élévation des privilèges JIT, un administrateur de cluster doit configurer l'accès JIT pour votre compte. Il détermine le rôle auquel vous pouvez élever vos privilèges et la durée pendant laquelle vous pouvez y accéder.

Étapes

1. Élevez temporairement vos privilèges au rôle configuré :

   ```
   security jit-privilege elevate
   ```

   Après avoir saisi cette commande, vous êtes invité à saisir votre mot de passe de connexion. Si l'accès JIT est configuré pour votre compte, vous bénéficierez d'un accès élevé pour la durée de session configurée. Une fois la session expirée, vous retrouverez votre niveau d'accès initial. Vous pouvez élever vos privilèges autant de fois que nécessaire pendant la période de validité JIT configurée.

2. Afficher le temps restant dans votre session JIT :

   ```
   security jit-privilege show-remaining-time
   ```

   Si vous êtes actuellement dans une session JIT, cette commande affiche le temps restant.

3. Si nécessaire, terminez votre session JIT plus tôt que prévu :

   ```
   security jit-privilege reset
   ```

   Si vous êtes actuellement dans une session JIT, cette commande met fin à la session JIT et restaure votre niveau d'accès d'origine.

Configurer l'élévation des privilèges JIT dans ONTAP

Depuis ONTAP 9.17.1, les administrateurs de cluster peuvent configurer l'élévation des privilèges juste-à-temps (JIT) pour permettre aux utilisateurs ONTAP d'élever temporairement leurs privilèges afin d'effectuer certaines tâches. Lorsque JIT est configuré pour un utilisateur, celui-ci peut temporairement "élever leurs privilèges" à un

rôle disposant des autorisations nécessaires pour effectuer une tâche. Une fois la session terminée, l'utilisateur retrouve son niveau d'accès initial.

Les administrateurs de cluster peuvent configurer la durée d'accès d'un utilisateur à l'élévation JIT. Par exemple, vous pouvez configurer l'accès utilisateur à l'élévation JIT avec une limite de 30 minutes par session (période de validité de session) pendant une période de 30 jours (période de validité JIT). Pendant cette période, l'utilisateur peut élever ses privilèges autant de fois que nécessaire, mais chaque session est limitée à 30 minutes.

L'élévation des privilèges JIT respecte le principe du moindre privilège, permettant aux utilisateurs d'effectuer des tâches nécessitant des privilèges élevés sans que ces privilèges leur soient accordés de manière permanente. Cela réduit le risque d'accès non autorisé ou de modifications accidentelles du système. Les exemples suivants décrivent quelques cas d'utilisation courants de l'élévation des privilèges JIT :

- Autoriser l'accès temporaire au `security login create` et `security login delete` commandes permettant l'intégration et la désintégration des utilisateurs.
- Autoriser l'accès temporaire à `system node image update` et `system node upgrade-revert` pendant une fenêtre de mise à jour. Une fois la mise à jour terminée, l'accès aux commandes est révoqué.
- Autoriser l'accès temporaire à `cluster add-node` , `cluster remove-node` , et `cluster modify` pour permettre l'extension ou la reconfiguration du cluster. Une fois les modifications du cluster terminées, l'accès aux commandes est révoqué.
- Autoriser l'accès temporaire à `volume snapshot restore` pour activer les opérations de restauration et la gestion des cibles de sauvegarde. Une fois la restauration ou la configuration terminée, l'accès aux commandes est révoqué.
- Autoriser l'accès temporaire à `security audit log show` pour permettre la révision et l'exportation du journal d'audit lors d'un contrôle de conformité.

Pour une liste plus complète des cas d'utilisation JIT courants, consultez la section « Utilisation JIT ». Cas d'utilisation JIT courants .

Les administrateurs de cluster peuvent configurer l'accès JIT pour les utilisateurs ONTAP et configurer les périodes de validité JIT par défaut soit globalement sur l'ensemble du cluster, soit pour des SVM spécifiques.

Description de la tâche

- L'élévation des privilèges JIT est réservée aux utilisateurs accédant à ONTAP via SSH. Les privilèges élevés ne sont disponibles que dans la session SSH actuelle de l'utilisateur, mais ils peuvent être élevés dans autant de sessions SSH simultanées que nécessaire.
- L'élévation des privilèges JIT n'est prise en charge que pour les utilisateurs utilisant un mot de passe, un commutateur NSSwitch ou une authentification de domaine pour se connecter. L'authentification multifacteur (MFA) n'est pas prise en charge pour l'élévation des privilèges JIT.

Avant de commencer

- Vous devez être un administrateur de cluster ONTAP au `admin` niveau de privilège pour effectuer les tâches suivantes.

Modifier les paramètres JIT globaux

Vous pouvez modifier les paramètres JIT par défaut pour l'ensemble du cluster ONTAP ou pour une SVM spécifique. Ces paramètres déterminent la durée de validité de session par défaut et la durée de validité JIT maximale pour les utilisateurs configurés pour un accès JIT.

Description de la tâche

- La valeur par défaut `default-session-validity-period` La valeur est d'une heure. Ce paramètre détermine la durée pendant laquelle un utilisateur peut accéder à des privilèges élevés dans une session JIT avant de devoir les réélever.
- La valeur par défaut `max-jit-validity-period` La valeur est de 90 jours. Ce paramètre détermine la période maximale pendant laquelle un utilisateur peut accéder à l'élévation JIT après la date de début configurée. Vous pouvez configurer la période de validité JIT pour chaque utilisateur, mais elle ne peut pas dépasser la période de validité JIT maximale.

Étapes

1. Vérifiez les paramètres JIT actuels :

   ```
   security jit-privilege show -vserver <svm_name>
   ```

   `-vserver` est facultatif. Si vous ne spécifiez pas de SVM, la commande affiche les paramètres JIT globaux.

2. Modifier les paramètres JIT globalement ou pour un SVM :

   ```
   security jit-privilege modify -vserver <svm_name> -default-session
   -validity-period <period> -max-jit-validity-period <period>
   ```

   Si vous ne spécifiez pas de SVM, la commande modifie les paramètres JIT globaux. L'exemple suivant définit la durée de session JIT par défaut à 45 minutes et la durée JIT maximale à 30 jours pour SVM. `svm1` :
   `security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

   Dans cet exemple, les utilisateurs pourront accéder à l'élévation JIT pendant 45 minutes à la fois et pourront lancer des sessions JIT pendant un maximum de 30 jours après leur date de début configurée.

Configurer l'accès par élévation de privilèges JIT pour un utilisateur

Vous pouvez attribuer un accès d'élévation de privilèges JIT aux utilisateurs ONTAP .

Étapes

1. Vérifiez l'accès JIT actuel pour un utilisateur :

   ```
   security jit-privilege user show -username <username>
   ```

   `-username` est facultatif. Si vous ne spécifiez pas de nom d'utilisateur, la commande affiche l'accès JIT pour tous les utilisateurs.

2. Attribuer un nouvel accès JIT à un utilisateur :

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

- Si `-vserver` n'est pas spécifié, l'accès JIT est attribué au niveau du cluster.
- `-role` est le rôle RBAC auquel l'utilisateur sera élevé. S'il n'est pas spécifié, `-role` par défaut `admin` .
- `-session-validity-period` Indique la durée pendant laquelle l'utilisateur peut accéder au rôle élevé avant de devoir démarrer une nouvelle session JIT. Si elle n'est pas spécifiée, le rôle global ou SVM `default-session-validity-period` est utilisé.
- `-jit-validity-period` est la durée maximale pendant laquelle un utilisateur peut lancer des sessions JIT après la date de début configurée. Si elle n'est pas spécifiée, `session-validity-period` est utilisé. Ce paramètre ne peut pas dépasser la valeur globale ou SVM `max-jit-validity-period` .
- `-start-time` correspond à la date et à l'heure après lesquelles l'utilisateur peut lancer des sessions JIT. Si elles ne sont pas spécifiées, la date et l'heure actuelles sont utilisées.

  L'exemple suivant permettra `ontap_user` pour accéder au `admin` rôle pendant 1 heure avant de devoir démarrer une nouvelle session JIT. `ontap_user` pourra lancer des sessions JIT pour une période de 60 jours à compter de 13h le 1er juillet 2025 :
  `security jit-privilege user create -username ontap_user -role admin -session -validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"`

3. Si nécessaire, révoquez l'accès JIT d'un utilisateur :

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

Cette commande révoquera l'accès JIT d'un utilisateur, même si son accès n'a pas expiré. Si `-vserver` Si l'accès JIT n'est pas spécifié, l'accès JIT est révoqué au niveau du cluster. Si l'utilisateur est dans une session JIT active, la session sera interrompue.

Cas d'utilisation JIT courants

Le tableau suivant présente les cas d'utilisation courants pour l'élévation des privilèges JIT. Pour chaque cas d'utilisation, un rôle RBAC doit être configuré pour donner accès aux commandes concernées. Chaque commande renvoie vers la référence des commandes ONTAP , contenant plus d'informations sur la commande et ses paramètres.

Cas d'utilisation	Commandes	Détails
Gestion des utilisateurs et des rôles	• `security login create` • `security login delete`	Élevez temporairement pour ajouter/supprimer des utilisateurs ou modifier les rôles lors de l'intégration ou de la sortie.

Cas d'utilisation	Commandes	Détails
Gestion des certificats	• `security certificate create` • `security certificate install`	Accorder un accès à court terme pour l'installation ou le renouvellement du certificat.
Contrôle d'accès SSH/CLI	• `security login create -application ssh`	Accordez temporairement l'accès SSH pour le dépannage ou l'assistance du fournisseur.
Gestion des licences	• `system license add` • `system license delete`	Accordez des droits pour ajouter ou supprimer des licences lors de l'activation ou de la désactivation des fonctionnalités.
Mises à niveau et correctifs du système	• `system node image update` • `system node upgrade-revert`	Élevez pour la fenêtre de mise à niveau, puis révoquez.
Paramètres de sécurité du réseau	• `security login role create` • `security login role modify`	Autoriser les modifications temporaires des rôles de sécurité liés au réseau.
Gestion des clusters	• `cluster add-node` • `cluster remove-node` • `cluster modify`	Élévation pour l'extension ou la reconfiguration du cluster.
Gestion SVM	• `vserver create` • `vserver delete` • `vserver modify`	Accordez temporairement à un administrateur SVM des droits d'approvisionnement ou de mise hors service.
Gestion du volume	• `volume create` • `volume delete` • `volume modify`	Élever pour l'approvisionnement, le redimensionnement ou la suppression de volumes.
Gestion des instantanés	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	Élever pour la suppression ou la restauration d'instantanés pendant la récupération.

Cas d'utilisation	Commandes	Détails
Configuration du réseau	• `network interface create` • `network port vlan create`	Accorder des droits pour les modifications du réseau pendant les fenêtres de maintenance.
Gestion des disques/agrégats	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	Élévation pour ajouter ou supprimer des disques ou gérer des agrégats.
Protection des données	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	Élever temporairement pour configurer ou restaurer les relations SnapMirror .
Réglage des performances	• `qos policy-group create` • `qos policy-group modify`	Élevez pour le dépannage ou le réglage des performances.
Accès au journal d'audit	• `security audit log show`	Élever temporairement pour la révision du journal d'audit ou l'exportation pendant les contrôles de conformité.
Gestion des événements et des alertes	• `event notification create` • `event notification modify`	Élévation pour configurer ou tester les notifications d'événements ou les interruptions SNMP.
Accès aux données axé sur la conformité	• `volume show` • `security audit log show`	Accordez un accès temporaire en lecture seule aux auditeurs pour examiner les données ou les journaux sensibles.
Avis sur les accès privilégiés	• `security login show` • `security login role show`	Accordez temporairement un accès privilégié pour examiner et signaler les accès privilégiés. Accordez un accès privilégié en lecture seule pour une durée limitée.

Informations associées

- "cluster"
- "notification d'événement"
- "réseau"
- "groupe de politiques QOS"

- "sécurité"
- "snapmirror"
- "stockage"
- "système"
- "volumétrie"
- "un vserver"

Gérez les comptes d'administrateur

En savoir plus sur la gestion des comptes d'administrateur ONTAP

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 ONTAP

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 `security login publickey create` la commande pour 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 en savoir plus, `security login publickey create` consultez le "Référence de commande ONTAP".

2. Vérifiez la modification en affichant la clé publique :

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

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

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>"
```

Gestion des clés publiques SSH et des certificats X.509 pour les administrateurs ONTAP

Pour une sécurité accrue de l'authentification SSH avec les comptes d'administrateur, vous pouvez utiliser l' `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. Pour en savoir plus, `security certificate install` consultez le "Référence de commande ONTAP".
  - 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 en savoir plus, `security login publickey create` consultez le "Référence de commande ONTAP".

2. Vérifiez la modification en affichant la clé publique :

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

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

Exemple

La commande suivante associe une clé publique et un certificat X.509 au compte d'administrateur du SVM `svmadmin2` Pour la SVM `engData2`. Le numéro d'index 6 est attribué à la clé publique.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -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
   ```

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

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 `svmadmin2` Pour la SVM `engData2` au numéro d'index 6.

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -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`*

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

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
```

Informations associées

- "clé publique de connexion de sécurité"

Configurez Cisco Duo 2FA pour les connexions SSH ONTAP

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` la commande. Dans ce cas, Cisco Duo est activé pour les connexions SSH pour ce cluster ou cette machine virtuelle de stockage. Pour en savoir plus, `security login duo create` consultez le "Référence de commande ONTAP".

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>
```

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 d'une machine virtuelle de stockage (appelée vServer dans l'interface de ligne de commande ONTAP), vous pouvez utiliser `security login duo modify` la commande. Pour en savoir plus, `security login duo modify` consultez le "Référence de commande ONTAP".

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 \
-max-prompts 1|2|3 \
-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` la commande. Pour en savoir plus, `security login duo delete` consultez le "Référence de commande ONTAP".

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 un serveur virtuel de stockage (appelé vServer dans l'interface de ligne de commande ONTAP) à l'aide de la `security login duo show` commande. Pour en savoir plus, `security login duo show` consultez le "Référence de commande ONTAP".

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 de la `security login duo group create` commande. Lorsque vous créez un groupe, vous pouvez exclure certains utilisateurs de ce groupe du processus d'authentification Duo. Pour en savoir plus, `security login duo group create` consultez le "Référence de commande ONTAP".

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> -excluded-users <USER1, USER2>
```

Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local. Les utilisateurs que vous spécifiez avec le paramètre facultatif `-excluded-users` ne seront 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 de la `security login duo group show` commande. Pour en savoir plus, `security login duo group show` consultez le "Référence de commande ONTAP".

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> -excluded-users <USER1, USER2>
```

Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local. Les utilisateurs que vous spécifiez avec le paramètre facultatif `-excluded-users` ne seront pas affichés.

Supprimer un groupe Duo

Vous pouvez supprimer une entrée de groupe Duo à l'aide de la `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. Pour en savoir plus, `security login duo group delete` consultez le "Référence de commande ONTAP".

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 modify -vserver <STORAGE_VM_NAME> -is-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 duo group modify -group-name <GROUP_NAME> -excluded-users
<USER1, USER2>
```

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

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

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".

Générez et installez un certificat de serveur signé par une autorité de certification dans ONTAP

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 `security certificate generate-csr` la commande pour générer une requête de signature de certificat (CSR) et la `security certificate install` commande pour installer le certificat que vous recevez de l'autorité de certification. Pour en savoir plus sur `security certificate generate-csr` et `security certificate install` dans le "Référence de commande ONTAP".

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 RSC avec une clé privée de 2048 bits générée par `SHA256` la fonction de hachage pour utilisation par le `Software` groupe du `IT` service d'une société dont le nom commun personnalisé est `server1.companyname.com`, située à Sunnyvale, en Californie, aux États-Unis. L'adresse e-mail de l'administrateur de 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-----
<certificate_value>
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

NOTE: 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 `security certificate install` la commande pour 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. Pour en savoir plus, `security certificate install` consultez le "Référence de commande ONTAP".

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
```

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-----
<certificate_value>
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----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-----
<certificate_value>
-----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-----
<certificate_value>
-----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.
```

Informations associées

- "certificat de sécurité générer-csr"

Gestion des certificats ONTAP 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	• [install-trusted-cert] • Supprimer une autorité de certification approuvée • Renouvelez une autorité de certification approuvée

Certificats client/serveur	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
Autorités locales de certification	• 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 + Add .
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. Afficher l'onglet **certificats client/serveur**. Voir Afficher les informations sur le certificat.
2. Sélectionnez + Add .
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, puis 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, puis cliquez sur **Renew**.

Créez 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, puis **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 ⋮ en regard 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, puis cliquez sur **Renew**.

Configurez l'accès au contrôleur de domaine Active Directory dans ONTAP

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 ONTAP 9.16.1, vous devez utiliser un tunnel d'authentification pour gérer les comptes d'administrateur du cluster avec AD.

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.

Étapes

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 en savoir plus, `security login domain-tunnel create` consultez le "Référence de commande ONTAP".

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

La commande suivante configure le SVM de données compatible 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.

Depuis ONTAP 9.16.1, vous pouvez utiliser cette procédure pour gérer des comptes d'administrateur de cluster avec AD.

Avant de commencer

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

Étapes

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>
```

Depuis ONTAP 9.16.1, le `-vserver` paramètre accepte le SVM admin Pour en savoir plus, `vserver active-directory create` consultez le "Référence de commande ONTAP".

La commande suivante crée un compte ordinateur nommé `ADSERVER1` sur le domaine de `example.com`

la 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:
```

Configurez l'accès au serveur LDAP ou NIS dans ONTAP

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 la 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 en savoir plus, `vserver services name-service ldap client create` consultez le "Référence de commande ONTAP".

   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
   ```

   > Le `-ldap-servers` le champ remplace le `-servers` champ. Vous pouvez utiliser le `-ldap-servers` champ pour spécifier soit un nom d'hôte soit 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 en savoir plus, `vserver services name-service ldap create` consultez le "Référence de commande ONTAP".

   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
   ```

   > Le `vserver services name-service ldap create` La commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP ne parvient pas à 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".                                                   |
```

Vous pouvez utiliser le `name service check` commande pour valider l'état des serveurs de noms.

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

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> -nis-servers <NIS_server_IPs>
   ```

   Pour en savoir plus, `vserver services name-service nis-domain create` consultez le "Référence de commande ONTAP".

   > Le `-nis-servers` le champ remplace le `-servers` champ. Vous pouvez utiliser le `-nis-servers` champ pour spécifier soit un nom d'hôte soit une adresse IP pour le serveur NIS.

   La commande suivante crée une configuration de domaine NIS sur SVM `engData`. Le domaine NIS `nisdomain` 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 -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 en savoir plus, `vserver services name-service ns-switch modify` consultez le "Référence de commande ONTAP".

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

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

Modifier le mot de passe d'un administrateur ONTAP

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 `security login role config modify` la commande pour modifier les règles relatives aux mots de passe pour les comptes associés à un rôle donné.

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:
```

Informations associées

- "modification de la configuration du rôle de connexion de sécurité"
- "mot de passe de connexion de sécurité"

Verrouiller et déverrouiller un compte d'administrateur ONTAP

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
   ```

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

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
   ```

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

Informations associées

- "connexion de sécurité"

Gérer les échecs de connexion dans ONTAP

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 `security login role config modify` la commande pour effectuer ces tâches. Pour en savoir plus, `security login role config modify` consultez le "Référence de commande ONTAP".

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

- Utilisez `security ssh modify` la commande pour limiter le nombre d'échecs de connexion pour tous les SVM nouvellement créés. Pour en savoir plus, `security ssh modify` consultez le "Référence de commande ONTAP".
- Migrez les comptes d'algorithme MD5 existants vers l'algorithme SHA-512 plus sécurisé en exigeant des utilisateurs de modifier leurs mots de passe.

Appliquez la fonction SHA-2 sur les mots de passe des comptes d'administrateur ONTAP

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.

Informations associées

- "mot de passe d'expiration de connexion de sécurité"
- "déverrouillage de la connexion de sécurité"

Diagnostiquez et corrigez les problèmes d'accès aux fichiers ONTAP avec System Manager

Depuis ONTAP 9.8, vous pouvez suivre et afficher 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

En savoir plus sur la vérification multiadministrateur ONTAP

À partir de ONTAP 9.11.1, vous pouvez utiliser la vérification multiadministrateur pour vous assurer que certaines opérations, telles que la suppression de volumes ou de snapshots, ne peuvent être exécutées qu'après approbation des 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 multiadministrateur est activée, la réalisation de chaque opération protégée nécessite les étapes suivantes :

1. Lorsqu'un utilisateur lance l'opération, un "la demande a été générée."
2. Avant de pouvoir exécuter l'opération, au moins un "L'administrateur MAV doit approuver."
3. Après approbation, l'utilisateur est invité et termine l'opération.

ⓘ Si vous devez désactiver la fonctionnalité de vérification multi-administrateur sans l'approbation de l'administrateur MAV, contactez le support NetApp et mentionnez les éléments suivants"Base de connaissances NetApp : Comment désactiver la vérification multi-administrateur si l'administrateur MAV n'est pas disponible" .

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 MAV ensemble, il est recommandé d'utiliser des requêtes pour des opérations MAV spécifiques. Par exemple, vous pouvez appliquer `volume delete` des règles MAV uniquement aux volumes pour lesquels l'automatisation n'est pas impliquée, et vous pouvez désigner ces volumes avec un schéma de nommage particulier.

ⓘ La vérification multiadministrateur n'est pas disponible avec Cloud Volumes ONTAP.

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` exploitation `*`

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

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

  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 opérations définies par le système, les commandes suivantes sont protégées par défaut lorsque la vérification multi-administrateur est activée, mais vous pouvez modifier les règles pour supprimer la protection de ces commandes :

- "mot de passe de connexion de sécurité"
- "déverrouillage de la connexion de sécurité"
- "jeu"

Chaque version de ONTAP fournit plus de commandes que vous pouvez choisir de protéger avec des règles de vérification multi-admin. Choisissez votre version ONTAP pour obtenir la liste complète des commandes disponibles pour la protection.

9.17.1

- `cluster date modify` [3]
- `cluster log-forwarding create` [3]
- `cluster log-forwarding delete` [3]
- `cluster log-forwarding modify` [3]
- `cluster peer delete`
- `cluster time-service ntp server create` [3]
- `cluster time-service ntp server delete` [3]
- `cluster time-service ntp key create` [3]
- `cluster time-service ntp key delete` [3]
- `cluster time-service ntp key modify` [3]
- `cluster time-service ntp server modify` [3]
- `event config modify`
- `event config set-mail-server-password` [3]
- `lun delete` [3]
- `security anti-ransomware volume attack clear-suspect` [1]
- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume event-log modify` [2]
- `security anti-ransomware volume pause` [1]
- `security anti-ransomware vserver event-log modify` [2]
- `security audit modify` [3]
- `security ipsec config modify` [3]
- `security ipsec policy create` [3]
- `security ipsec policy delete` [3]
- `security ipsec policy modify` [3]
- `security login create`
- `security login delete`
- `security login modify`
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase` [3]
- `security saml-sp create` [3]

- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete [4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]

- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume rename [5]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]

- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.16.1

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]
- cluster time-service ntp key delete [3]
- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]

- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- security key-manager onboard update-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete [4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]

- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]
- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]

- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.15.1

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]
- cluster time-service ntp key delete [3]
- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]
- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete

- security login publickey modify
- security key-manager onboard update-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume file privileged-delete [3]

- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]

- vserver security file-directory remove-slag [3]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.14.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot delete

- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver create [2]
- vserver modify [2]
- vserver peer delete

9.13.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume pause [1]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

9.12.1/9.11.1

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

1. Nouvelle commande protégée par des règles pour 9.13.1
2. Nouvelle commande protégée par des règles pour 9.14.1
3. Nouvelle commande protégée par des règles pour 9.15.1
4. Nouvelle commande protégée par des règles pour 9.16.1
5. Nouvelle commande protégée par des règles pour la version 9.17.1

*Cette commande n’est disponible qu’avec l’interface de ligne de commande et n’est pas disponible pour

System Manager dans certaines versions.

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 lancer des opérations protégées ; les administrateurs réguliers doivent lancer des opérations protégées et l'administrateur MAV peut uniquement approuver.
- 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.

> Un demandeur ne peut pas approuver ses propres demandes, même s'il fait partie du groupe d'approbation (bien qu'il puisse recevoir des notifications par e-mail pour ses propres demandes). 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.

Les règles MAV sont évaluées avant l'exécution de l'opération protégée. Cela signifie que les règles sont appliquées en fonction de l'état actuel du système. Par exemple, si une règle MAV est créée pour `volume modify` avec une requête de `-size 5GB` , en utilisant `volume modify` redimensionner un volume de 5 Go à 2 Go nécessitera l'approbation du MAV, mais redimensionner un volume de 2 Go à 5 Go ne le nécessitera pas.

Informations associées

- "cluster"
- "lun"
- "sécurité"
- "extrémité à verrouillage automatique à maintien légal"
- "agrégat de stockage"
- "chiffrement du stockage"
- "système"

Gérer les groupes d'approbation d'administrateurs ONTAP pour MAV

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.

À partir d' ONTAP 9.15.1, vous pouvez configurer les utilisateurs Active Directory (AD) en tant

qu'administrateurs MAV. L'utilisateur AD doit être"configuré en tant qu'administrateur ONTAP" .

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 → en regard de **utilisateurs et rôles.**
   c. Cliquez + 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 **sécurité**. (Vous verrez l' ⚙ icône 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
   ```

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

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

Si vous voulez…	Saisissez cette commande
Afficher les administrateurs actuels	`security login show`
Modifier les informations d'identification des administrateurs actuels	`security login modify <parameters>`
Créer de nouveaux comptes d'administrateur	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

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

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. Pour les utilisateurs d'AD, utilisez le format `domain\user` . Par exemple : `mydomain\pavan` .
- `-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	`security multi-admin-verify approval-group modify [parameters]`
Ajouter ou supprimer des membres	`security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2…]][-approvers-to-remove approver1[,approver2…]]`
Supprimer un groupe	`security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name`

Informations associées

- "sécurité multi-administrateur-vérification"

Activer ou désactiver la vérification multiadministrateur dans ONTAP

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 devez désactiver la fonctionnalité de vérification multi-administrateur sans l'approbation de l'administrateur MAV, contactez le support NetApp et mentionnez les éléments suivants"Base de connaissances NetApp : Comment désactiver la vérification multi-administrateur si l'administrateur MAV 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 → en regard de **utilisateurs et rôles.**
   c. Cliquez + 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 **sécurité**.
   c. Cliquez + Add sur 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 **sécurité**.
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	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`
	
	Exemple : la commande suivante active MAV avec 1 groupe d'approbation, 2 approbateurs requis et périodes d'expiration par défaut.
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	Terminez la configuration initiale en ajoutant au moins une configuration "règle de fonctionnement."

Modifier une configuration MAV (nécessite l'approbation MAV)	`security multi-admin-verify approval-group modify [-approval-groups group1 [,group2…]] [-required-approvers nn ] [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`

Vérifier la fonctionnalité MAV	`security multi-admin-verify show`
	
	Exemple:
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution Approval Approval`
	`Enabled Approvers Expiry Expiry Groups`
	`------- --------- --------- -------- ----------`
	`true 2 1h 1h mav-grp1`

Désactiver la fonctionnalité MAV (nécessite l'approbation MAV)	`security multi-admin-verify modify -enabled false`

Informations associées

- "sécurité multi-administrateur-vérification"

Gérez des règles de vérification multiadministrateur pour les opérations protégées dans ONTAP

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.

Vous pouvez créer des règles à protéger "ces commandes". Vous pouvez protéger chaque commande en commençant par la version ONTAP dans laquelle la fonctionnalité de protection pour la commande a été mise à disposition pour la première fois.

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

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

- "mot de passe de connexion de sécurité"
- "déverrouillage de la connexion de sécurité"
- "jeu"

Contraintes de règle

Lorsque vous créez une règle, vous pouvez éventuellement spécifier l' `-query`option permettant de limiter la demande à un sous-ensemble de la fonctionnalité de commande. L' `-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 la `volume snapshot delete` commande, `-query` peut être défini sur `-snapshot !hourly*,!daily*,!weekly*`, ce qui signifie que les snapshots de volume prédéfinis avec des attributs horaires, quotidiens ou hebdomadaires sont exclus des protections MAV.

```
smci-vsim20::> security multi-admin-verify rule show
                                              Required  Approval
Vserver Operation                             Approvers 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'une commande correspondante `security multi-admin-verify request create "protected_operation"` est générée automatiquement lorsqu'une opération protégée est saisie. Vous pouvez modifier cette valeur par défaut pour exiger que la `request create` commande soit 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 **sécurité**.
3. Sélectionnez + Add cette option 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	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

Si vous voulez…	Saisissez cette commande

Modifier les informations d'identification des administrateurs actuels	`security login modify <parameters>`
	
	Exemple : la règle suivante nécessite l'approbation pour supprimer le volume racine.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

Modifier une règle	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
Supprimer une règle	`security multi-admin-verify rule delete -operation "protected_operation"`
Afficher les règles	`security multi-admin-verify rule show`

Informations associées

- "règle de sécurité multi-administrateur-vérification"
- "modification de la connexion de sécurité"

Demander l'exécution d'opérations protégées par MAV dans ONTAP

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 vol1 -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 vol1
             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 vol1 -vserver vs0

Info: Volume "vol1" 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 vol1_*" 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 "vol1" 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 vol1
             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 vol1 -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".
```

Informations associées

- "sécurité multi-administrateur-vérification"

Gérer les demandes d'opérations protégées par MAV dans ONTAP

Lorsque les administrateurs d'un groupe d'approbation MAV (administrateurs MAV) sont informés d'une demande d'exécution d'opération en attente, ils doivent répondre avec un message d'approbation ou de veto dans un délai déterminé (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.

> `multi-admin-verify`les demandes dans un état terminal peuvent être écrasées ou supprimées automatiquement. Utilisez le"journal d'audit" pour revoir les demandes précédentes.

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.

System Manager

Les administrateurs MAV reçoivent des messages électroniques 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 en accédant à **Événements et travaux > Demandes** dans le Gestionnaire système.

La fenêtre **Demandes** est disponible lorsque la vérification multi-administrateur est activée, affichant les demandes en attente en fonction de l'ID de connexion de l'utilisateur et du 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.

CLI

1. Lorsque vous êtes informé des demandes en attente par courrier électronique, 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	`security multi-admin-verify request approve` *nn*
Veto sur une demande	`security multi-admin-verify request veto` *nn*
Affiche toutes les demandes, les demandes en attente ou une seule demande	`security multi-admin-verify request { show

Si vous voulez…	Saisissez cette commande
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  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 `-fields` paramètre) ou à propos de tous les champs (en utilisant le `-instance` paramètre).
Supprimer une demande	`security multi-admin-verify request delete` *nn*

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: -
```

Informations associées

- "sécurité multi-administrateur-vérification"

Gérer l'autorisation dynamique

En savoir plus sur l'autorisation dynamique ONTAP

À partir de ONTAP 9.15.1, les administrateurs peuvent configurer et activer l'autorisation dynamique afin d'accroître la sécurité de l'accès à distance à ONTAP, tout en limitant les dommages potentiels causés par un acteur malveillant. Avec ONTAP 9.15.1, l'autorisation dynamique fournit une structure initiale pour attribuer une note de sécurité aux utilisateurs et, si leur activité semble suspecte, les défier avec des vérifications d'autorisation supplémentaires ou refuser complètement une opération. Les administrateurs peuvent créer des règles, attribuer des scores de confiance et restreindre des commandes pour déterminer si certaines activités sont autorisées ou refusées pour un utilisateur. Les administrateurs peuvent activer l'autorisation dynamique à l'échelle du

cluster ou pour des machines virtuelles de stockage individuelles.

Fonctionnement de l'autorisation dynamique

L'autorisation dynamique utilise un système de notation de confiance pour attribuer aux utilisateurs un niveau de confiance différent en fonction des stratégies d'autorisation. En fonction du niveau de confiance de l'utilisateur, une activité qu'il effectue peut être autorisée ou refusée, ou l'utilisateur peut être invité à demander une authentification supplémentaire.

Reportez-vous "Personnaliser l'autorisation dynamique"à la pour en savoir plus sur la configuration de la pondération des scores des critères et d'autres attributs d'autorisation dynamique.

Périphériques de confiance

Lorsque l'autorisation dynamique est utilisée, la définition d'un périphérique approuvé est un périphérique utilisé par un utilisateur pour se connecter à ONTAP à l'aide de l'authentification par clé publique comme une des méthodes d'authentification. Le périphérique est approuvé car seul cet utilisateur possède la clé privée correspondante.

Exemple d'autorisation dynamique

Prenons l'exemple de trois utilisateurs différents qui tentent de supprimer un volume. Lorsqu'ils tentent d'effectuer l'opération, la cote de risque de chaque utilisateur est examinée :

- Le premier utilisateur se connecte à partir d'un périphérique de confiance avec très peu d'échecs d'authentification précédents, ce qui rend son niveau de risque faible ; l'opération est autorisée sans authentification supplémentaire.
- Le deuxième utilisateur se connecte à partir d'un périphérique de confiance avec un pourcentage modéré d'échecs d'authentification précédents, ce qui rend la note de risque modérée ; il est invité à demander une authentification supplémentaire avant que l'opération ne soit autorisée.
- Le troisième utilisateur se connecte à partir d'un périphérique non approuvé avec un pourcentage élevé d'échecs d'authentification précédents, ce qui rend l'indice de risque élevé ; l'opération n'est pas autorisée.

Et la suite

- "Activer ou désactiver l'autorisation dynamique"
- "Personnaliser l'autorisation dynamique"

Activer ou désactiver l'autorisation dynamique dans ONTAP

À partir de ONTAP 9.15.1, les administrateurs peuvent configurer et activer l'autorisation dynamique dans `visibility` pour tester la configuration, ou dans `enforced` Mode pour activer la configuration des utilisateurs de l'interface de ligne de commande qui se connectent via SSH. Si vous n'avez plus besoin d'une autorisation dynamique, vous pouvez la désactiver. Lorsque vous désactivez l'autorisation dynamique, les paramètres de configuration restent disponibles et vous pouvez les utiliser ultérieurement si vous décidez de la réactiver.

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

Activer l'autorisation dynamique pour les tests

Vous pouvez activer l'autorisation dynamique en mode visibilité, ce qui vous permet de tester la fonction et de vous assurer que les utilisateurs ne seront pas accidentellement verrouillés. Dans ce mode, le score de confiance est vérifié avec chaque activité restreinte, mais pas appliqué. Cependant, toute activité qui aurait été refusée ou qui aurait fait l'objet de défis d'authentification supplémentaires est consignée. Il est recommandé de tester les paramètres souhaités dans ce mode avant de les appliquer.

> Vous pouvez suivre cette étape pour activer l'autorisation dynamique pour la première fois, même si vous n'avez pas encore configuré d'autres paramètres d'autorisation dynamique. Reportez-vous "Personnaliser l'autorisation dynamique"à la section pour connaître les étapes de configuration d'autres paramètres d'autorisation dynamique afin de les personnaliser en fonction de votre environnement.

Étapes

1. Activez l'autorisation dynamique en mode visibilité en configurant les paramètres globaux et en définissant l'état de la fonction sur `visibility`. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Vérifiez le résultat à l'aide de `show` commande pour afficher la configuration globale :

```
security dynamic-authorization show
```

Activer l'autorisation dynamique en mode imposé

Vous pouvez activer l'autorisation dynamique en mode imposé. En général, vous utilisez ce mode une fois les tests effectués en mode visibilité. Dans ce mode, le score de confiance est vérifié pour chaque activité restreinte et les restrictions d'activité sont appliquées si les conditions de restriction sont remplies. L'intervalle de suppression est également appliqué, ce qui évite des problèmes d'authentification supplémentaires dans l'intervalle spécifié.

> Cette étape suppose que vous avez précédemment configuré et activé l'autorisation dynamique dans `visibility` ce qui est fortement recommandé.

Étapes

1. Activer l'autorisation dynamique dans `enforced` en changeant son état à `enforced`. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage_VM_name>
```

2. Vérifiez le résultat à l'aide de `show` commande pour afficher la configuration globale :

```
security dynamic-authorization show
```

Désactiver l'autorisation dynamique

Vous pouvez désactiver l'autorisation dynamique si vous n'avez plus besoin de la sécurité d'authentification supplémentaire.

Étapes

1. Désactivez l'autorisation dynamique en changeant son état à `disabled`. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. Vérifiez le résultat à l'aide de `show` commande pour afficher la configuration globale :

```
security dynamic-authorization show
```

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

Et la suite

(Facultatif) selon votre environnement, reportez-vous "Personnaliser l'autorisation dynamique"à la section pour configurer d'autres paramètres d'autorisation dynamique.

Personnaliser l'autorisation dynamique dans ONTAP

En tant qu'administrateur, vous pouvez personnaliser différents aspects de votre configuration d'autorisation dynamique afin d'améliorer la sécurité des connexions SSH d'administrateur distant avec votre cluster ONTAP.

Vous pouvez personnaliser les paramètres d'autorisation dynamiques suivants en fonction de vos besoins en matière de sécurité :

- Configurer les paramètres globaux d'autorisation dynamique

- Configurer les composants de score de confiance d'autorisation dynamique
- Configurez un fournisseur de score de confiance personnalisé
- Configurer les commandes restreintes
- Configurer des groupes d'autorisation dynamiques

Configurer les paramètres globaux d'autorisation dynamique

Vous pouvez configurer des paramètres globaux pour l'autorisation dynamique, y compris la VM de stockage à sécuriser, l'intervalle de suppression pour les défis d'authentification et les paramètres de score de confiance.

Pour en savoir plus, `security login domain-tunnel create` consultez le "Référence de commande ONTAP".

Étapes

1. Configurer les paramètres globaux pour l'autorisation dynamique. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement :

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Afficher la configuration résultante :

```
security dynamic-authorization show
```

Configurer les commandes restreintes

Lorsque vous activez l'autorisation dynamique, la fonction inclut un ensemble par défaut de commandes restreintes. Vous pouvez modifier cette liste en fonction de vos besoins. Reportez-vous à la "Documentation de vérification multiadministrateur" pour plus d'informations sur la liste par défaut des commandes restreintes.

Ajouter une commande restreinte

Vous pouvez ajouter une commande à la liste des commandes dont l'autorisation dynamique est limitée.

Pour en savoir plus, `security dynamic-authorization rule create` consultez le "Référence de commande ONTAP".

Étapes

1. Ajoutez la commande. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage_VM_name>
```

2. Afficher la liste résultante des commandes restreintes :

```
security dynamic-authorization rule show
```

Supprime une commande restreinte

Vous pouvez supprimer une commande de la liste des commandes dont l'autorisation dynamique est limitée.

Pour en savoir plus, `security dynamic-authorization rule delete` consultez le "Référence de commande ONTAP".

Étapes

1. Supprimez la commande. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage_VM_name>
```

2. Afficher la liste résultante des commandes restreintes :

```
security dynamic-authorization rule show
```

Configurer des groupes d'autorisation dynamiques

Par défaut, l'autorisation dynamique s'applique à tous les utilisateurs et groupes dès que vous l'activez. Toutefois, vous pouvez créer des groupes à l'aide de `security dynamic-authorization group create` de sorte que l'autorisation dynamique ne s'applique qu'à ces utilisateurs spécifiques.

Ajouter un groupe d'autorisation dynamique

Vous pouvez ajouter un groupe d'autorisation dynamique.

Pour en savoir plus, `security dynamic-authorization group create` consultez le "Référence de commande ONTAP".

Étapes

1. Créez le groupe. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization group create \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name> \
-excluded-usernames <user1,user2,user3...>
```

2. Afficher les groupes d'autorisation dynamiques résultants :

```
security dynamic-authorization group show
```

Supprimer un groupe d'autorisation dynamique

Vous pouvez supprimer un groupe d'autorisation dynamique.

Pour en savoir plus, `security dynamic-authorization group delete` consultez le "Référence de commande ONTAP".

Étapes

1. Supprimez le groupe. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization group delete \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. Afficher les groupes d'autorisation dynamiques résultants :

```
security dynamic-authorization group show
```

Configurer les composants de score de confiance d'autorisation dynamique

Vous pouvez configurer la pondération maximale du score pour modifier la priorité des critères de notation ou pour supprimer certains critères de l'évaluation du risque.

> Dans le cadre de la meilleure pratique, vous devez laisser les valeurs de pondération par défaut en place et les ajuster uniquement si nécessaire.

Pour en savoir plus, `security dynamic-authorization trust-score-component modify` consultez le "Référence de commande ONTAP".

Vous pouvez modifier les composants suivants, ainsi que leur score par défaut et leur pondération en

pourcentage :

Critères	Nom du composant	Pondération de score brut par défaut	Poids en pourcentage par défaut
Périphérique de confiance	`trusted-device`	20	50
Historique d'authentification de connexion utilisateur	`authentication-history`	20	50

Étapes

1. Modifier les composants du score de confiance. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. Afficher les paramètres des composants du score de confiance obtenu :

```
security dynamic-authorization trust-score-component show
```

Réinitialiser le score de confiance d'un utilisateur

Si l'accès d'un utilisateur est refusé en raison de stratégies système et qu'il est capable de prouver son identité, l'administrateur peut réinitialiser le score de confiance de l'utilisateur.

Pour en savoir plus, `security dynamic-authorization user-trust-score reset` consultez le "Référence de commande ONTAP".

Étapes

1. Ajoutez la commande. Reportez-vous à la section Configurer les composants de score de confiance d'autorisation dynamique pour obtenir une liste des composants de score de confiance que vous pouvez réinitialiser. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

Afficher votre score de confiance

Un utilisateur peut afficher son propre score de confiance pour une session de connexion.

Étapes

1. Afficher votre score de confiance :

   ```
   security login whoami
   ```

   Vous devez voir les résultats similaires à ce qui suit :

   ```
   User: admin
   Role: admin
   Trust Score: 50
   ```

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

Configurez un fournisseur de score de confiance personnalisé

Si vous recevez déjà des méthodes de notation d'un fournisseur de score de confiance externe, vous pouvez ajouter le fournisseur personnalisé à la configuration d'autorisation dynamique.

Avant de commencer

- Le fournisseur de score de confiance personnalisé doit renvoyer une réponse JSON. Les conditions de syntaxe suivantes doivent être remplies :
  - Le champ qui renvoie le score de confiance doit être un champ scalaire et non un élément d'un tableau.
  - Le champ qui renvoie le score de confiance peut être un champ imbriqué, tel que `trust_score.value`.
  - Il doit y avoir un champ dans la réponse JSON qui renvoie un score de confiance numérique. Si ce n'est pas disponible en natif, vous pouvez écrire un script wrapper pour renvoyer cette valeur.
- La valeur fournie peut être un score de confiance ou un score de risque. La différence est que le score de confiance est dans l'ordre croissant avec un score plus élevé indiquant un niveau de confiance plus élevé, alors que le score de risque est dans l'ordre décroissant. Par exemple, un score de confiance de 90 pour une plage de scores de 0 à 100 indique que le score est très digne de confiance et qu'il est susceptible d'aboutir à un « Autoriser » sans défi supplémentaire, bien qu'un score de risque de 90 pour une plage de scores de 0 à 100 indique un risque élevé et risque de donner lieu à un « refus » sans défi supplémentaire.
- Le fournisseur de score de confiance personnalisé doit être accessible via l'API REST de ONTAP.
- Le fournisseur de score de confiance personnalisé doit être configurable à l'aide de l'un des paramètres pris en charge. Les fournisseurs de score de confiance personnalisés qui nécessitent une configuration ne figurant pas dans la liste des paramètres pris en charge ne sont pas pris en charge.

  Pour en savoir plus, `security dynamic-authorization trust-score-component create` consultez le "Référence de commande ONTAP".

Étapes

1. Ajoutez un fournisseur de score de confiance personnalisé. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. Afficher les paramètres du fournisseur de score de confiance :

```
security dynamic-authorization trust-score-component show
```

Configurer les balises de fournisseur de score de confiance personnalisé

Vous pouvez communiquer avec des fournisseurs externes de score de confiance à l'aide de balises. Cela vous permet d'envoyer des informations dans l'URL au fournisseur de score de confiance sans exposer d'informations sensibles.

Pour en savoir plus, `security dynamic-authorization trust-score-component create` consultez le "Référence de commande ONTAP".

Étapes

1. Activer les balises de fournisseur de score de confiance. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

   Par exemple :

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

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 les serveurs d'autorisation les plus courants

L'implémentation de ONTAP OAuth 2.0 a été testée avec plusieurs serveurs ou services courants basés sur la version ONTAP comme suit :

- ONTAP 9.16.1 (prise en charge de l'UUID de groupe pour le mappage de noms et des rôles externes) :
  - ID Microsoft Entra
- ONTAP 9.14.1 (prise en charge des fonctionnalités OAuth 2.0 standard)
  - Auth0
  - ADFS (Active Directory Federation Service)
  - Porte-clés

Voir "Serveurs d'autorisation et jetons d'accès" pour plus d'informations sur les fonctionnalités disponibles dans chaque version de ONTAP.

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.
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'IFAI"
- "ONGLET"
- "IANA - JWT"

Produits et services

- "Auth0"
- "ID de l'Entra"
- "Présentation de l'ADFS"
- "Porte-clés"

Outils et utilitaires supplémentaires

- "JWT par Auth0"
- "OpenSSL"

Documentation et ressources de NetApp

- "Documentation sur l'automatisation ONTAP"

Concepts

Serveurs d’autorisation OAuth 2.0 et jetons d’accès dans ONTAP

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`.

Pour en savoir plus, `security oauth2 client create` consultez le "Référence de commande ONTAP".

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.

Fonctionnalités OAuth 2.0 prises en charge dans ONTAP

La prise en charge d'OAuth 2.0 était initialement disponible avec ONTAP 9.14.1 et continue d'être améliorée avec les versions ultérieures. Les fonctions OAuth 2.0 prises en charge par ONTAP sont décrites ci-dessous.

> Les fonctionnalités introduites avec une version spécifique de ONTAP sont reportées dans les prochaines versions.

ONTAP 9.16.1

ONTAP 9.16.1 étend les fonctions standard d'OAuth 2.0 pour inclure des extensions spécifiques d'Entra ID pour les groupes d'ID Entra natifs. Cela implique l'utilisation de GUID dans le jeton d'accès au lieu de noms. En outre, la version ajoute la prise en charge du mappage de rôles externes pour mapper les rôles de fournisseur d'identité natif aux rôles ONTAP à l'aide du champ « rôles » du jeton d'accès.

ONTAP 9.14.1

À partir de ONTAP 9.14.1, les serveurs d'autorisation sont pris en charge par le biais des fonctionnalités standard OAuth 2.0 suivantes pour les applications utilisant :

- OAuth 2.0 avec les champs standard, y compris "iss", "aud" et "exp", comme décrit dans "RFC6749: Le cadre d'autorisation OAuth 2.0" et "RFC 7519 : jeton Web JSON (JWT)". Cela inclut également la prise en charge de l'identification unique des utilisateurs via les champs du jeton d'accès tels que "upn", "appid", "sub", "username" ou "preferred_username".
- Extensions ADFS spécifiques au fournisseur pour les noms de groupe avec le champ « groupe ».
- Extensions spécifiques au fournisseur Azure pour les UUID de groupe avec le champ « group ».

- Extensions ONTAP pour la prise en charge des autorisations à l'aide de rôles autonomes et nommés dans le périmètre du jeton d'accès OAuth 2.0. Cela inclut les champs « portée » et « scp » ainsi que les noms de groupe dans le périmètre.

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.
Expiration	date	Heure après laquelle le jeton expire et doit être rejeté.

Voir "RFC 7519 : tokens Web JSON" pour en savoir plus.

Autorisation du client

Présentation et options de l'autorisation client ONTAP

L'implémentation ONTAP OAuth 2.0 est conçue pour être flexible et robuste, et vous offre les fonctionnalités dont vous avez besoin pour sécuriser votre environnement ONTAP. Plusieurs options de configuration mutuellement exclusives sont disponibles. Les décisions d'autorisation sont finalement basées sur les rôles REST ONTAP contenus dans ou dérivés des jetons d'accès OAuth 2.0.

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.

ONTAP applique l'option d'autorisation la plus appropriée en fonction de votre configuration. Pour plus d'informations sur la manière dont ONTAP prend les décisions d'accès client, reportez-vous à la section"Comment ONTAP détermine l'accès".

Oscilloscopes autonomes OAuth 2.0

Ces étendues contiennent un ou plusieurs rôles REST personnalisés, chacun encapsulé dans une seule chaîne dans le jeton d'accès. Ils sont indépendants des définitions de rôles ONTAP. Vous devez configurer les chaînes de portée sur votre serveur d'autorisation. Voir "Oscilloscopes OAuth 2.0 autonomes" pour plus d'informations.

Rôles REST ONTAP locaux

Un seul rôle REST nommé, intégré ou personnalisé, peut être utilisé. La syntaxe de portée d'un rôle nommé est **ontap-role-**<URL-encoded-ONTAP-role-name>. Par exemple, si le rôle ONTAP est `admin` la chaîne de portée sera `ontap-role-admin`.

Utilisateurs

Le nom d'utilisateur dans le jeton d'accès défini avec l'accès à l'application « http » peut être utilisé. Un utilisateur est testé dans l'ordre suivant en fonction de la méthode d'authentification définie : mot de passe, domaine (Active Directory), nsswitch (LDAP).

Groupes

Les serveurs d'autorisation peuvent être configurés pour utiliser des groupes ONTAP pour l'autorisation. 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).

Voir "Travailler avec des groupes IdP OAuth 2.0 ou SAML dans ONTAP" pour plus d'informations.

Portées OAuth 2.0 autonomes dans ONTAP

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 ONTAP CLI `cluster identity show` pour afficher l'UUID de votre cluster. Si elle n'est pas spécifiée, la portée s'applique à tous les clusters. Pour en savoir plus, `cluster identity show` consultez le "Référence de commande ONTAP".

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.
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
```

Pour en savoir plus, `security oauth2 scope` consultez le "Référence de commande ONTAP".

Mappage des rôles externes OAuth 2.0 dans ONTAP

Un rôle externe est défini dans un fournisseur d'identification configuré pour une utilisation par ONTAP. Vous pouvez créer et gérer des relations de mappage entre ces rôles externes et les rôles ONTAP à l'aide de l'interface de ligne de commandes ONTAP.

Vous pouvez également configurer la fonction de mappage de rôles externes à l'aide de l'API REST ONTAP. Pour en savoir plus, consultez le "Documentation sur l'automatisation ONTAP".

Rôles externes dans un jeton d'accès

Voici un fragment d'un jeton d'accès JSON contenant deux rôles externes.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

Configuration

Vous pouvez utiliser l'interface de ligne de commande ONTAP pour administrer la fonction de mappage de rôle externe.

Création

Vous pouvez définir une configuration de mappage de rôles à l'aide de la `security login external-role-mapping create` commande. Vous devez être au niveau de privilège ONTAP **admin** pour exécuter cette commande ainsi que les options associées.

Paramètres

Les paramètres utilisés pour créer un mappage de groupe sont décrits ci-dessous.

Paramètre	Description
`external-role`	Nom du rôle défini au niveau du fournisseur d'identité externe.
`provider`	Nom du fournisseur d'identité. Il doit s'agir de l'identifiant du système.
`ontap-role`	Indique le rôle ONTAP existant vers lequel le rôle externe est mappé.

Exemple

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

Pour en savoir plus, `security login external-role-mapping create` consultez le "Référence de commande ONTAP".

Autres opérations de l'interface de ligne de commande

La commande prend en charge plusieurs opérations supplémentaires, notamment :

- Afficher
- Modifier
- Supprimer

Informations associées

- "Référence de commande ONTAP"

Comment ONTAP détermine l'accès client

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. Les principales étapes permettant de déterminer l'accès sont présentées ci-dessous en fonction de la version de ONTAP.

Il n'y a pas eu de mises à jour OAuth 2.0 significatives avec ONTAP 9.15.1. Si vous utilisez la version 9.15.1, reportez-vous à la description de ONTAP 9.14.1.

Informations associées

- "Fonctionnalités OAuth 2.0 prises en charge dans ONTAP"

ONTAP 9.16.1

ONTAP 9.16.1 étend la prise en charge standard d'OAuth 2.0 pour inclure des extensions spécifiques d'Entra ID Microsoft pour les groupes d'ID Entra natifs ainsi que le mappage de rôles externes.

Déterminez l'accès client pour ONTAP 9.16.1

Étape 1 : oscilloscopes autonomes

Si le jeton d'accès contient des étendues autonomes, ONTAP examine d'abord ces étendues. 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 le paramètre booléen `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 dans le `scope` champ ou `scp`, ou en tant que sinistre, ONTAP utilise le 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

Extrayez le nom d'utilisateur du jeton d'accès et essayez de le faire correspondre aux utilisateurs ayant accès à l'application « http ». Les utilisateurs sont examinés en fonction de la méthode d'authentification dans l'ordre suivant :

- mot de passe
- Domaine (Active Directory)
- Nsswitch (LDAP)

Si un utilisateur correspondant est trouvé, ONTAP utilise le rôle défini pour l'utilisateur afin de prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

Si un utilisateur 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 : groupes

Si un ou plusieurs groupes sont inclus, le format est examiné. Si les groupes sont représentés par des UUID, une recherche est effectuée dans une table de mappage de groupes interne. En cas de correspondance entre un groupe et un rôle associé, ONTAP utilise le rôle défini pour le groupe afin de prendre une décision d'accès. Cela aboutit systématiquement à une décision d'autorisation (**ALLOW**) ou de refus (**DENY**), et le traitement est terminé. "Travailler avec des groupes IdP OAuth 2.0 ou SAML dans ONTAP" .

Si les groupes sont représentés par des noms et configurés avec l'autorisation domaine ou nsswitch, ONTAP tente de les faire correspondre à un groupe Active Directory ou LDAP, respectivement. 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.

ONTAP 9.14.1

La version initiale de OAuth 2.0 prise en charge est introduite avec ONTAP 9.14.1 en fonction des fonctionnalités standard de OAuth 2.0.

Déterminez l'accès client pour ONTAP 9.14.1

Étape 1 : oscilloscopes autonomes

Si le jeton d'accès contient des étendues autonomes, ONTAP examine d'abord ces étendues. 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 le paramètre booléen `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 dans le `scope` champ ou `scp`, ONTAP utilise le 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

Extrayez le nom d'utilisateur du jeton d'accès et essayez de le faire correspondre aux utilisateurs ayant accès à l'application « http ». Les utilisateurs sont examinés en fonction de la méthode d'authentification dans l'ordre suivant :

- mot de passe
- Domaine (Active Directory)
- Nsswitch (LDAP)

Si un utilisateur correspondant est trouvé, ONTAP utilise le rôle défini pour l'utilisateur afin de prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

Si un utilisateur 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 : groupes

Si un ou plusieurs groupes sont inclus et configurés avec l'autorisation domain ou nsswitch, ONTAP tente de les associer à un groupe Active Directory ou LDAP, respectivement.

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 avec ONTAP

Plusieurs options de configuration sont disponibles lors de la définition d'un serveur d'autorisation dans ONTAP. En fonction de ces options, vous pouvez définir un serveur d'autorisation approprié à votre environnement à l'aide de l'un des scénarios de déploiement suivants.

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.

> Le nom utilisé pour un paramètre ou un champ individuel peut varier en fonction de l'interface d'administration de ONTAP. Pour tenir compte des différences dans les interfaces administratives, un nom générique unique est utilisé pour chaque paramètre de la table. Le nom exact utilisé avec une interface spécifique 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.
Demande d'utilisateur à distance	Autre nom utilisé par ONTAP pour correspondre aux utilisateurs locaux. Utilisez le `sub` champ du jeton d'accès correspondant au nom d'utilisateur local.
Public	Ce champ définit les points de terminaison où le jeton d'accès peut être utilisé.

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.

Informations associées

- "Afficher le client OAuth2 de sécurité"

Authentification client ONTAP à l'aide d'OAuth 2.0 Mutual TLS

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 `x5t#S256`) 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.

Informations associées

- "client de sécurité oauth2"

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. Notez que certains serveurs d'autorisation, y compris Microsoft Entra ID, représentent des groupes utilisant des UUID au lieu de noms.

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.

Groupes en tant qu'UUID et mappage d'identité

Si vous utilisez un serveur d'autorisation qui représente des groupes utilisant des UUID, vous devez planifier la façon de les mapper aux noms de groupe et éventuellement aux rôles associés.

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. En fonction de votre serveur d'autorisation, cela peut également inclure l'administration de groupes basés sur des valeurs UUID.

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 les certificats d'autorité de certification racine du serveur d'autorisation

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-----
   <certificate_value>
   -----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
   ```

   Pour en savoir plus, `security oauth2 client create` consultez le "Référence de commande ONTAP".

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
   ```

Informations associées

- "installation du certificat de sécurité"
- "certificat de sécurité afficher"
- "sécurité oauth2 modifier"
- "sécurité oauth2 afficher"

Émettre un appel d'API REST ONTAP 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=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

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"
```

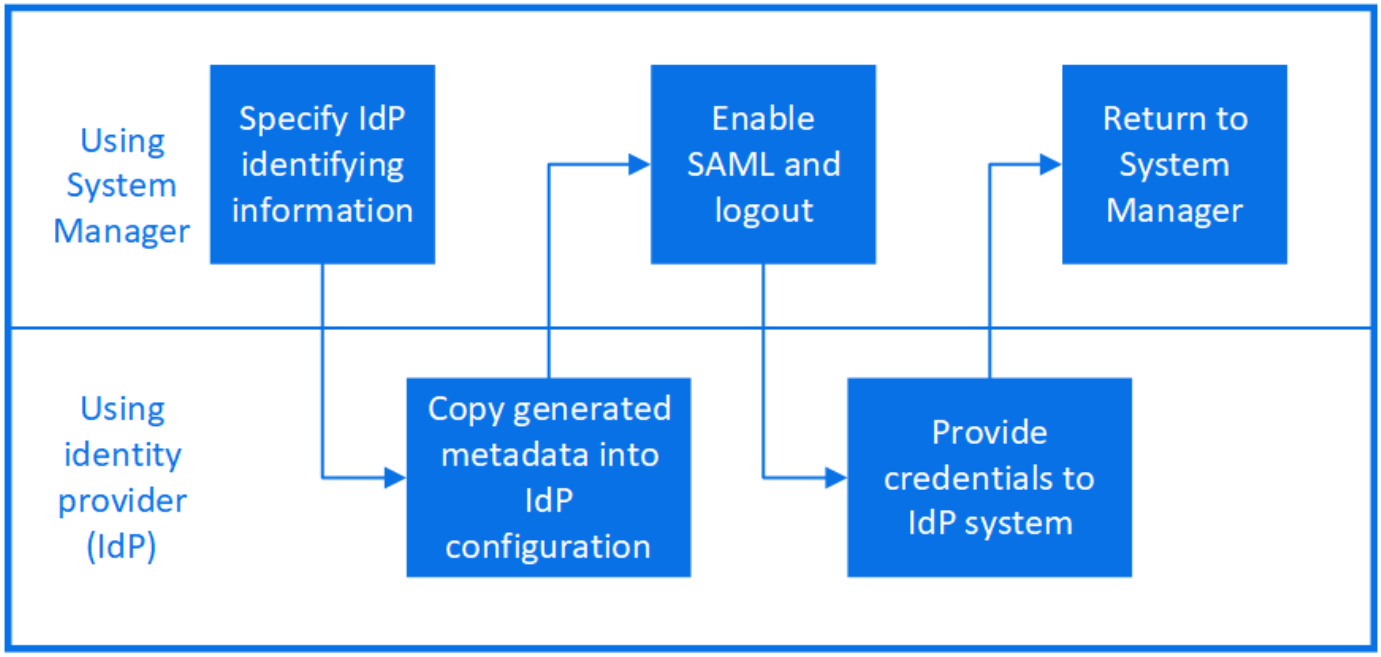
Configurer l’authentification SAML pour les utilisateurs ONTAP distants

À partir d' ONTAP 9.3, vous pouvez configurer l’authentification SAML (Security Assertion Markup Language) pour les services Web. Lorsque l’authentification SAML est configurée et activée, les utilisateurs sont authentifiés par un fournisseur d’identité (IdP) externe plutôt que par les fournisseurs de services d’annuaire tels qu’Active Directory et LDAP. Lorsque l’authentification SAML est désactivée, les fournisseurs de services d’annuaire configurés, tels qu’Active Directory et LDAP, sont utilisés pour l’authentification.

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.

Une fois l’authentification SAML activée, seuls les utilisateurs distants configurés pour l’authentification SAML peuvent accéder à l’interface utilisateur graphique de System Manager. Les utilisateurs locaux ne peuvent pas accéder à l’interface utilisateur graphique de System Manager après l’activation de l’authentification SAML.



Description de la tâche

- L’authentification SAML s’applique uniquement à ONTAP `http` et `ontapi` candidatures.

  Le `http` et `ontapi` les applications sont utilisées par les services Web suivants : Service Processor Infrastructure, API ONTAP et System Manager.

- L’authentification SAML est applicable uniquement pour l’accès au SVM d’administration.
- Depuis ONTAP 9.17.1, les informations de groupe fournies par l’IdP peuvent être associées aux rôles ONTAP . Cela permet d’attribuer des rôles aux utilisateurs en fonction des groupes définis dans l’IdP. Pour plus d’informations, consultez la section "Travailler avec des groupes IdP OAuth 2.0 ou SAML dans

ONTAP" .

Les PDI suivants ont été validés avec System Manager :

- ID Microsoft Entra (validé avec ONTAP 9.17.1 et versions ultérieures)
- 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")
  - Versions de correctifs 9.8P17 et ultérieures 9.8
  - Versions de correctifs 9.9.1P13 et ultérieures 9.9.1
  - Versions de correctifs 9.10.1P9 et ultérieures 9.10.1
  - Versions de correctifs 9.11.1P4 et ultérieures 9.11.1
  - versions 9.12.1 et ultérieures
- Hurlent

Avant de commencer

- L'IdP que vous prévoyez d'utiliser pour l'authentification à distance doit être configuré. Vous devez connaître l'URI de l'IdP. URI de l'IdP est l'adresse Web à laquelle ONTAP envoie les requêtes d'authentification et reçoit les réponses.
- Le port 443 doit être ouvert entre le cluster ONTAP et l'IdP.
- Le cluster ONTAP et l'IdP doivent chacun pouvoir pinger le nom de domaine complet de l'autre. Assurez-vous que le DNS est correctement configuré et que le certificat du cluster n'est pas expiré.
- Si nécessaire, ajoutez l'autorité de certification (CA) de confiance du fournisseur d'identité à ONTAP. Vous pouvez "gérer les certificats ONTAP avec System Manager" . Vous devrez peut-être configurer le certificat de cluster ONTAP dans l'IdP.
- Vous devez pouvoir accéder au cluster ONTAP "Processeur de service (SP)" console. Si SAML est mal configuré, vous devrez le désactiver depuis la console SP .
- Si vous utilisez Entra ID (validé à partir d' ONTAP 9.17.1), vous devez configurer Entra ID avec les métadonnées ONTAP avant de créer la configuration SAML ONTAP . Entra ID ne fournira pas l'URI IdP tant qu'il n'aura pas été configuré avec les métadonnées ONTAP . L'URI IdP est requis pour créer la configuration SAML ONTAP .
  - Si vous utilisez System Manager pour configurer SAML, laissez le champ URI IdP vide jusqu'à ce que System Manager fournisse les métadonnées ONTAP . Configurez l'ID Entra avec les métadonnées ONTAP , puis copiez l'URI IdP dans System Manager avant d'activer la configuration SAML.
  - Si vous utilisez l'interface de ligne de commande ONTAP pour configurer SAML, vous devez générer les métadonnées ONTAP avant d'activer la configuration SAML ONTAP . Vous pouvez générer le fichier de métadonnées ONTAP avec la commande suivante :

    ```
    security saml-sp default-metadata create -sp-host <ontap_host_name>
    ```

    `ontap_host_name` est le nom d'hôte ou l'adresse IP de l'hôte du fournisseur de services SAML, qui, dans ce cas, est le système ONTAP . Par défaut, l'adresse IP de gestion du cluster est utilisée. Vous pouvez éventuellement fournir les informations du certificat du serveur ONTAP . Par défaut, les informations du certificat du serveur Web ONTAP sont utilisées.

Configurez l’ID Entra avec les métadonnées fournies. Vous devez configurer l’ID Entra avant de créer la configuration SAML ONTAP . Une fois Entra configuré, suivez la procédure CLI ci-dessous.

- Vous ne pouvez pas générer les métadonnées ONTAP pour Entra ID tant que tous les nœuds du cluster ne sont pas sur la version 9.17.1.

Étapes

Effectuez les opérations suivantes en fonction de votre environnement :

System Manager

1. Cliquez sur **Cluster > Paramètres**.
2. En regard de **SAML Authentication**, cliquez sur .
3. Vérifiez que la case **Activer l'authentification SAML** est cochée.
4. Saisissez l’URL de l’URI IdP (y compris "https://"). Si vous utilisez Entra ID, ignorez cette étape.
5. Modifiez l'adresse du système hôte si nécessaire. Il s'agit de l'adresse vers laquelle l'IdP redirigera après l'authentification. L'adresse par défaut est l'adresse IP de gestion du cluster.
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 spécifié et copiez les métadonnées depuis votre presse-papiers pour les mettre à jour. Si vous utilisez Entra ID, copiez l'URI IdP dans ONTAP après avoir configuré Entra ID avec 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. Sur la page de connexion de l'IdP, saisissez vos identifiants SAML. Une fois vos identifiants vérifiés, vous serez redirigé vers la page d'accueil du Gestionnaire système.

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.

   > Certaines URL contiennent un point d'interrogation (?). Ce point active l'aide active de la ligne de commande ONTAP . Pour saisir une URL avec un point d'interrogation, vous devez d'abord désactiver l'aide active avec la commande. `set -active-help false` . L'aide active peut être réactivée ultérieurement avec la commande `set -active-help true` . En savoir plus dans le "Référence de commande ONTAP" .

   `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 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 ONTAP user configuration.
```

L'URL permettant d'accéder aux métadonnées de l'hôte ONTAP s'affiche.

2. Depuis l'hôte IdP, configurer l'IdP avec les métadonnées de l'hôte ONTAP . Si vous utilisez Entra ID, vous avez déjà effectué cette étape.
3. Une fois l'IdP configuré, activez 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` Après la configuration de SAML, spécifiez SAML comme méthode d'authentification pour les nouveaux utilisateurs. Avant ONTAP 9.17.1, une connexion SAML était automatiquement créée pour les utilisateurs existants. `http` ou `ontapi` utilisateurs lorsque SAML est activé. Les nouveaux utilisateurs doivent être configurés pour SAML. À partir d' ONTAP 9.17.1, tous les utilisateurs créés avec `password` , `domain` , ou `nsswitch` les méthodes d'authentification sont automatiquement authentifiées auprès de l'IdP lorsque SAML est activé.

   a. Créez une méthode de connexion pour les nouveaux utilisateurs avec authentification SAML . `user_name` doit correspondre au nom d'utilisateur configuré dans l'IdP :

      > La `user_name` valeur est sensible à la casse. Sauf si vous utilisez Entra ID, incluez uniquement le nom d'utilisateur, et n'incluez aucune partie du domaine. Si vous utilisez Entra ID, vous pouvez créer le nom d'utilisateur avec le domaine, par exemple *user_name@domain.com*.

      `security login create -user-or-group-name <user_name> -application [http | ontapi] -authentication-method saml -vserver <svm_name>`

      Exemple :

```
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`

Exemple :

```
cluster_12::> security login show

Vserver: cluster_12

Second
User/Group                  Authentication                 Acct
Authentication
Name            Application Method        Role Name        Locked
Method
--------------- ----------- ------------- ---------------- ------
--------------
admin           console     password      admin            no
none
admin           http        password      admin            no
none
admin           http        saml          admin            -
none
admin           ontapi      password      admin            no
none
admin           ontapi      saml          admin            -
none
admin           service-processor
                            password      admin            no
none
admin           ssh         password      admin            no
none
admin1          http        password      backup           no
none
admin1          http        saml          backup           -
none
```

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

Désactivez l’authentification SAML

Vous pouvez désactiver l’authentification SAML si vous souhaitez arrêter l’authentification des utilisateurs distants du Gestionnaire système auprès d’un fournisseur d’identité externe (IdP). Lorsque l’authentification SAML est désactivée, l’authentification des utilisateurs locaux ou les fournisseurs de services d’annuaire configurés, tels qu’Active Directory et LDAP, sont utilisés pour authentifier les utilisateurs.

Effectuez les opérations suivantes en fonction de votre environnement :

Exemple 4. 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 décocher 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
   ```

Configurer un IdP tiers

Description de la tâche

Pour vous authentifier avec ONTAP, vous devrez peut-être modifier les paramètres de votre fournisseur d’identité. Les sections suivantes fournissent des informations de configuration pour les fournisseurs d’identité pris en charge.

ID de l'Entra

Lors de la configuration d'Entra ID, créez une nouvelle application et configurez l'authentification SAML avec les métadonnées fournies par ONTAP. Une fois l'application créée, modifiez la section « Attributs et revendications » des paramètres SAML de l'application pour qu'elle corresponde aux valeurs suivantes :

Réglage	Valeur
Nom	urn:oid:0.9.2342.19200300.100.1.1
Espace de noms	*Laisser vide*
Format du nom	URI
Source	Attribut
Attribut source	utilisateur.userprincipalname

Si vous souhaitez utiliser des groupes avec Entra ID, ajoutez une revendication de groupe avec les paramètres suivants :

Réglage	Valeur
Nom	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
Espace de noms	*Laisser vide*
Attribut source	ID de groupe

Entra ID fournit des informations de groupe au format UUID. Pour plus d'informations sur l'utilisation des groupes avec Entra ID, consultez "Gestion des groupes avec des UUID" .

L'URL des métadonnées de la fédération d'applications fournie dans la section « Certificat SAML » des paramètres SAML de l'application est l'URI IdP que vous saisirez dans ONTAP.

Pour plus d'informations sur la configuration de l'authentification multifacteur Entra ID, reportez-vous à "Planifier un déploiement d'authentification multifacteur Microsoft Entra" .

Pour plus d'informations, reportez-vous à la "Documentation d'identification Entra" .

Services de fédération Active Directory

Lors de la configuration des services de fédération Active Directory (AD FS), vous devez ajouter une nouvelle approbation de partie de confiance prenant en charge les revendications, avec les métadonnées du fournisseur de services fournies par ONTAP. Une fois l'approbation de partie de confiance créée, ajoutez les règles de revendication suivantes à sa politique d'émission de revendications à l'aide du modèle « Envoyer les attributs LDAP comme revendications » :

Magasin d'attributs	attribut LDAP	Type de réclamation sortante
Active Directory	nom-du-compte-SAM	Nom d'identification
Active Directory	nom-du-compte-SAM	urn:oid:0.9.2342.19200300.100.1.1
Active Directory	Format du nom	urne:oasis:noms:tc:SAML:2.0:attrname-format:uri

Magasin d'attributs	attribut LDAP	Type de réclamation sortante
Active Directory	Groupes de jetons - Qualifiés par nom de domaine	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
Active Directory	sAMAccountName	urn:oid:1.2.840.113556.1.4.221

AD FS fournit des informations sur les groupes sous forme de noms. Pour plus d'informations sur l'utilisation des groupes avec AD FS, consultez "Gérer les groupes avec des noms" .

Pour plus d'informations, reportez-vous à la "Documentation AD FS" .

Duo Cisco

Se référer à la "Documentation Cisco Duo" pour les informations de configuration.

Hurlent

Avant de configurer l'IdP Shibboleth, vous devez avoir configuré un serveur LDAP.

Lors de l'activation de SAML sur ONTAP, enregistrez le fichier XML de métadonnées d'hôte fourni. Sur l'hôte où Shibboleth est installé, remplacez le contenu de `metadata/sp-metadata.xml` avec les métadonnées XML de l'hôte dans le répertoire personnel de Shibboleth IdP.

Pour plus d'informations, reportez-vous à "Hurlent" .

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
   ```

   Exemple :

```
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.
```

Pour en savoir plus, `security saml-sp status show` consultez le "Référence de commande ONTAP".

3. Corrigez la configuration SAML sur le nœud défaillant :

   `security saml-sp repair -node <node_name>`

   Exemple :

```
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.

   Pour en savoir plus, `security saml-sp repair` consultez le "Référence de commande ONTAP".

4. Vérifiez que le langage SAML est configuré sur tous les nœuds :

   `security saml-sp status show -instance`

Exemple :

```
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.
```

Pour en savoir plus, `security saml-sp status show` consultez le "Référence de commande ONTAP".

Informations associées

- "Référence de commande ONTAP"
- "sécurité saml-SP"
- "création d'une connexion de sécurité"

Travailler avec des groupes IdP OAuth 2.0 ou SAML dans ONTAP

ONTAP propose plusieurs options pour configurer des groupes en fonction de votre serveur d'autorisation OAuth 2.0 ou de votre fournisseur d'identité SAML (IdP). Les groupes peuvent ensuite être mappés aux rôles utilisés par ONTAP pour déterminer l'accès.

À partir d' ONTAP 9.17.1, les informations de groupe fournies par le fournisseur d'identité SAML peuvent être mappées aux rôles ONTAP . Cela permet d'attribuer des rôles aux utilisateurs en fonction des groupes définis dans le fournisseur d'identité. Pour plus d'informations, voir "Configurez l'authentification SAML". Depuis ONTAP 9.14.1, ONTAP prend en charge l'authentification par nom de groupe pour OAuth 2.0. Depuis ONTAP 9.16.1, ONTAP prend en charge l'authentification par UUID de groupe OAuth 2.0 et le mappage de rôles. "Présentation de la mise en œuvre de ONTAP OAuth 2.0" .

Comment les groupes sont identifiés

Lorsque vous configurez un groupe sur un serveur d'autorisation ou un fournisseur d'identité SAML, il est identifié et transmis dans un jeton d'accès OAuth 2.0 ou une assertion SAML à l'aide d'un nom ou d'un UUID. Vous devez connaître la façon dont votre serveur d'autorisation ou votre fournisseur d'identité SAML gère les groupes avant de configurer ONTAP.

Si plusieurs groupes sont inclus dans un jeton d'accès, ONTAP tente d'utiliser chacun d'eux jusqu'à ce qu'il y ait correspondance.

Noms de groupe

De nombreux serveurs d'autorisation et fournisseurs d'identité SAML, comme Active Directory Federation Service (ADFS), identifient et représentent les groupes à l'aide d'un nom. Voici un fragment d'un jeton d'accès JSON OAuth 2.0 généré par ADFS et contenant plusieurs groupes. Voir Gérer les groupes avec des noms pour plus d'informations.

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

UUID de groupe

Certains serveurs d'autorisation et fournisseurs d'identité SAML, comme Microsoft Entra ID, identifient et représentent les groupes à l'aide d'un UUID. Voici un fragment d'un jeton d'accès OAuth 2.0 généré par Entra ID et contenant plusieurs groupes. Voir Gestion des groupes avec des UUID pour plus d'informations.

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

Gérer les groupes avec des noms

Si votre serveur d'autorisation ou votre fournisseur d'identité SAML utilise des noms pour identifier les groupes, vous devez vous assurer que chaque groupe est défini pour votre cluster ONTAP . Selon votre

environnement de sécurité, le groupe est peut-être déjà défini.

Voici un exemple de commande CLI définissant un groupe ONTAP . Notez qu'elle utilise un groupe nommé issu de l'exemple de jeton d'accès. Vous devez disposer du niveau de privilège ONTAP **admin** pour exécuter cette commande.

Exemple

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

Utiliser `-authentication-method domain` ou `nsswitch` pour les groupes de serveurs d'autorisation SAML IdP et OAuth 2.0.

Vous pouvez également configurer cette fonctionnalité à l'aide de l'API REST ONTAP . Pour en savoir plus, consultez le "Documentation sur l'automatisation ONTAP" .

Gestion des groupes avec des UUID

Si votre serveur d'autorisation ou votre fournisseur d'identité SAML représente des groupes utilisant des valeurs UUID, vous devez effectuer une configuration en deux étapes avant d'utiliser un groupe. Depuis ONTAP 9.16.1, deux fonctionnalités de mappage sont disponibles et ont été testées avec Entra ID. Entra ID pour OAuth 2.0 est pris en charge depuis ONTAP 9.16.1, et Entra ID pour SAML est pris en charge depuis ONTAP 9.17.1. Vous devez disposer du niveau de privilège ONTAP **admin** pour exécuter les commandes CLI.

Vous pouvez également configurer ces fonctionnalités à l'aide de l'API REST ONTAP. Pour en savoir plus, consultez le "Documentation sur l'automatisation ONTAP".

Mapper un UUID de groupe sur un nom de groupe

Si vous utilisez un serveur d'autorisation ou un fournisseur d'identité SAML qui représente des groupes à l'aide de valeurs UUID, vous devez mapper les UUID de groupe aux noms de groupe. Les principales opérations de l'interface de ligne de commande ONTAP sont décrites ci-dessous.

Création

Vous pouvez définir une nouvelle configuration de mappage de groupe avec le `security login group create` Commande. L'UUID et le nom du groupe doivent correspondre à la configuration du serveur d'autorisation ou du fournisseur d'identité SAML. En savoir plus `security login group create` dans le "Référence de commande ONTAP" .

Paramètres

Les paramètres utilisés pour créer un mappage de groupe sont décrits ci-dessous.

Paramètre	Description
`vserver`	Spécifier éventuellement le nom du SVM (vserver) auquel le groupe est associé. Si vous omettez le paramètre, le groupe est associé au cluster ONTAP.
`name`	Nom unique du groupe que ONTAP utilisera.

Paramètre	Description
`type`	Cette valeur indique le fournisseur d'identité dont provient le groupe.
`uuid`	Spécifie l'identifiant unique universel du groupe tel que fourni par le serveur d'autorisation ou l'IdP SAML.

Voici un exemple de commande CLI définissant un groupe pour ONTAP. Notez qu'elle utilise un groupe UUID issu de l'exemple de jeton d'accès.

Exemple

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

Une fois le groupe créé, un identifiant d'entier unique en lecture seule est généré pour le groupe.

Autres opérations de l'interface de ligne de commande

La commande prend en charge plusieurs opérations supplémentaires, notamment :

- Afficher
- Modifier
- Supprimer

Vous pouvez utiliser `show` l'option pour récupérer l'ID de groupe unique généré pour un groupe. Pour en savoir plus, `show` consultez le "Référence de commande ONTAP".

Mapper un UUID de groupe à un rôle

Si vous utilisez un serveur d'autorisation ou un fournisseur d'identité SAML représentant des groupes à l'aide de valeurs UUID, vous pouvez associer le groupe à un rôle. Pour plus d'informations sur le contrôle d'accès basé sur les rôles dans ONTAP, voir "En savoir plus sur la gestion des rôles de contrôle d'accès ONTAP". Les principales opérations de l'interface de ligne de commande ONTAP sont décrites ci-dessous. devez disposer du niveau de privilège ONTAP **admin** pour exécuter les commandes.

> Vous devez d'abord mapper un UUID de groupe à un nom de groupe et récupérez l'identifiant entier unique généré pour le groupe. Cet identifiant est nécessaire pour associer le groupe à un rôle.

Création

Vous pouvez définir un nouveau mappage de rôles avec le `security login group role-mapping create` commande. En savoir plus sur `security login group role-mapping create` dans le "Référence de commande ONTAP" .

Paramètres

Les paramètres utilisés pour mapper un groupe à un rôle sont décrits ci-dessous.

Paramètre	Description
`group-id`	Spécifie l'ID unique généré pour le groupe à l'aide de la commande `security login group create`.
`role`	Nom du rôle ONTAP auquel le groupe est mappé.

Exemple

```
security login group role-mapping create -group-id 1 -role admin
```

Autres opérations de l'interface de ligne de commande

La commande prend en charge plusieurs opérations supplémentaires, notamment :

- Afficher
- Modifier
- Supprimer

Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Informations associées

- "Mappage de rôles externes"

Authentification et autorisation à l'aide de WebAuthn MFA

En savoir plus sur l'authentification multifacteur WebAuthn pour les utilisateurs d'ONTAP System Manager

À partir de ONTAP 9.16.1, les administrateurs peuvent activer l'authentification multifacteur (MFA) WebAuthn pour les utilisateurs qui se connectent au Gestionnaire système. Cela permet de se connecter à System Manager en utilisant une clé FIDO2 (telle qu'une YubiKey) comme deuxième forme d'authentification. Par défaut, WebAuthn MFA est désactivé pour les utilisateurs ONTAP nouveaux et existants.

WebAuthn MFA est pris en charge pour les utilisateurs et les groupes qui utilisent les types d'authentification suivants pour la première méthode d'authentification :

- Utilisateurs : mot de passe, domaine ou nsswitch
- Groupes : domaine ou nsswitch

Après avoir activé WebAuthn MFA comme deuxième méthode d'authentification pour un utilisateur, l'utilisateur est invité à enregistrer un authentificateur matériel lors de sa connexion à System Manager. Après l'enregistrement, la clé privée est stockée dans l'authentificateur et la clé publique est stockée dans ONTAP.

ONTAP prend en charge une autorisation WebAuthn par utilisateur. Si un utilisateur perd un authentificateur et doit le remplacer, l'administrateur ONTAP doit supprimer les informations d'identification WebAuthn pour que l'utilisateur puisse enregistrer un nouvel authentificateur lors de la prochaine connexion.

Les utilisateurs pour lesquels WebAuthn MFA "https://192.168.100.200"est activé comme deuxième méthode d’authentification doivent utiliser le FQDN (par exemple, "https://myontap.example.com") au lieu de l’adresse IP (par exemple,) pour accéder à System Manager. Pour les utilisateurs avec WebAuthn MFA activé, les tentatives de connexion à System Manager à l’aide de l’adresse IP sont rejetées.

Activez WebAuthn MFA pour les utilisateurs ou les groupes ONTAP System Manager

En tant qu'administrateur ONTAP, vous pouvez activer l'authentification WebAuthn MFA pour un utilisateur ou un groupe du Gestionnaire système en ajoutant un nouvel utilisateur ou un nouveau groupe avec l'option WebAuthn MFA activée ou en activant l'option pour un utilisateur ou un groupe existant.

Après avoir activé WebAuthn MFA comme deuxième méthode d'authentification pour un utilisateur ou un groupe, l'utilisateur (ou tous les utilisateurs de ce groupe) sera invité à enregistrer un périphérique FIDO2 matériel lors de la prochaine connexion à System Manager. Cet enregistrement est géré par le système d'exploitation local de l'utilisateur et consiste généralement à insérer la clé de sécurité, à créer une clé d'authentification et à appuyer sur la clé de sécurité (si elle est prise en charge).

Activez WebAuthn MFA lors de la création d'un nouvel utilisateur ou d'un nouveau groupe

Vous pouvez créer un nouvel utilisateur ou un nouveau groupe avec l'authentification WebAuthn MFA activée via System Manager ou l'interface de ligne de commande ONTAP.

System Manager

1. Sélectionnez **Cluster > Paramètres**.
2. Sélectionnez l'icône en forme de flèche en regard de **utilisateurs et rôles**.
3. Sélectionnez **Ajouter** sous **utilisateurs**.
4. Spécifiez un nom d'utilisateur ou de groupe et sélectionnez un rôle dans le menu déroulant pour **role**.
5. Spécifiez une méthode de connexion et un mot de passe pour l'utilisateur ou le groupe.

   WebAuthn MFA prend en charge les méthodes de connexion « password », « domain » ou « nsswitch » pour les utilisateurs, et « domain » ou « nsswitch » pour les groupes.
6. Dans la colonne **MFA pour HTTP**, sélectionnez **Enabled**.
7. Sélectionnez **Enregistrer**.

CLI

1. Créez un nouvel utilisateur ou un nouveau groupe avec WebAuthn MFA activé.

   Dans l'exemple suivant, WebAuthn MFA est activé en choisissant "publickey" pour la deuxième méthode d'authentification :

   ```
   security login create -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

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

Activez WebAuthn MFA pour un utilisateur ou un groupe existant

Vous pouvez activer WebAuthn MFA pour un utilisateur ou un groupe existant.

System Manager

1. Sélectionnez **Cluster > Paramètres**.
2. Sélectionnez l'icône en forme de flèche en regard de **utilisateurs et rôles**.
3. Dans la liste des utilisateurs et des groupes, sélectionnez le menu d'options de l'utilisateur ou du groupe que vous souhaitez modifier.

   WebAuthn MFA prend en charge les méthodes de connexion « password », « domain » ou « nsswitch » pour les utilisateurs, et « domain » ou « nsswitch » pour les groupes.
4. Dans la colonne **MFA pour HTTP** de cet utilisateur, sélectionnez **activé**.
5. Sélectionnez **Enregistrer**.

CLI

1. Modifiez un utilisateur ou un groupe existant pour activer WebAuthn MFA pour cet utilisateur ou ce groupe.

   Dans l'exemple suivant, WebAuthn MFA est activé en choisissant "publickey" pour la deuxième méthode d'authentification :

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

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

Désactivez WebAuthn MFA pour les utilisateurs du Gestionnaire système ONTAP

En tant qu'administrateur ONTAP, vous pouvez désactiver l'authentification WebAuthn MFA pour un utilisateur ou un groupe en modifiant l'utilisateur ou le groupe à l'aide de System Manager ou de l'interface de ligne de commande ONTAP.

Désactivez WebAuthn MFA pour un utilisateur ou un groupe existant

Vous pouvez désactiver WebAuthn MFA à tout moment pour un utilisateur ou un groupe existant.

> Si vous désactivez les informations d'identification enregistrées, les informations d'identification sont conservées. Si vous activez à nouveau les informations d'identification à l'avenir, les mêmes informations d'identification sont utilisées, de sorte que l'utilisateur n'a pas besoin de s'enregistrer à nouveau lors de la connexion.

System Manager

1. Sélectionnez **Cluster > Paramètres**.
2. Sélectionnez l'icône en forme de flèche en regard de **utilisateurs et rôles**.
3. Dans la liste des utilisateurs et des groupes, sélectionnez l'utilisateur ou le groupe à modifier.
4. Dans la colonne **MFA pour HTTP** de cet utilisateur, sélectionnez **Désactivé**.
5. Sélectionnez **Enregistrer**.

CLI

1. Modifiez un utilisateur ou un groupe existant pour désactiver WebAuthn MFA pour cet utilisateur ou ce groupe.

   Dans l'exemple suivant, WebAuthn MFA est désactivé en choisissant « aucun » pour la deuxième méthode d'authentification.

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method none \
                         -application http \
                         -role admin
   ```

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

Afficher les paramètres ONTAP WebAuthn MFA et gérer les informations d'identification

En tant qu'administrateur ONTAP, vous pouvez afficher les paramètres de l'authentification WebAuthn MFA à l'échelle du cluster et gérer les informations d'identification d'utilisateur et de groupe pour l'authentification WebAuthn MFA.

Afficher les paramètres de cluster pour WebAuthn MFA

Vous pouvez afficher les paramètres de cluster pour WebAuthn MFA via l'interface de ligne de commande ONTAP.

Étapes

1. Afficher les paramètres de cluster pour WebAuthn MFA Vous pouvez éventuellement spécifier une VM de stockage à l'aide de l' `vserver`argument suivant :

   ```
   security webauthn show -vserver <storage_vm_name>
   ```

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

Afficher les algorithmes de clé publique WebAuthn MFA pris en charge

Vous pouvez afficher les algorithmes de clé publique pris en charge pour WebAuthn MFA pour une VM de stockage ou un cluster.

Étapes

1. Répertorie les algorithmes de clé publique WebAuthn MFA pris en charge. Vous pouvez éventuellement spécifier une VM de stockage à l'aide de l' `vserver`argument suivant :

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

Pour en savoir plus, `security webauthn supported-algorithms show` consultez le "Référence de commande ONTAP".

Afficher les informations d'identification WebAuthn MFA enregistrées

En tant qu'administrateur ONTAP, vous pouvez afficher les informations d'identification WebAuthn enregistrées pour tous les utilisateurs. Les utilisateurs non administrateurs qui utilisent cette procédure peuvent uniquement afficher leurs propres informations d'identification WebAuthn enregistrées.

Étapes

1. Afficher les informations d'identification WebAuthn MFA enregistrées :

```
security webauthn credentials show
```

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

Supprimez les informations d'identification WebAuthn MFA enregistrées

Vous pouvez supprimer une information d'identification WebAuthn MFA enregistrée. Ceci est utile lorsqu'une clé matérielle d'un utilisateur a été perdue, volée ou n'est plus utilisée. Vous pouvez également supprimer une information d'identification enregistrée lorsque l'utilisateur dispose toujours de l'authentificateur matériel d'origine, mais souhaite la remplacer par une nouvelle. Une fois les informations d'identification retirées, l'utilisateur est invité à enregistrer l'authentificateur de remplacement.

> La suppression d'une information d'identification enregistrée pour un utilisateur ne désactive pas WebAuthn MFA pour l'utilisateur. Si un utilisateur perd un authentificateur matériel et doit se connecter avant de le remplacer, vous devez supprimer les informations d'identification en suivant ces étapes et également "Désactivez WebAuthn MFA" pour l'utilisateur.

System Manager

1. Sélectionnez **Cluster > Paramètres**.
2. Sélectionnez l'icône en forme de flèche en regard de **utilisateurs et rôles**.
3. Dans la liste des utilisateurs et des groupes, sélectionnez le menu d'options de l'utilisateur ou du groupe dont vous souhaitez supprimer les informations d'identification.
4. Sélectionnez **Supprimer MFA pour les informations d'identification HTTP**.
5. Sélectionnez **Supprimer**.

CLI

1. Supprimez les informations d'identification enregistrées. Notez ce qui suit :
   - Vous pouvez éventuellement spécifier une VM de stockage de l'utilisateur. Si vous omettez le paramètre, les informations d'identification sont supprimées au niveau du cluster.
   - Vous pouvez éventuellement spécifier un nom d'utilisateur de l'utilisateur pour lequel vous supprimez les informations d'identification. Si omis, les informations d'identification sont supprimées pour l'utilisateur actuel.

     ```
     security webauthn credentials delete -vserver <storage_vm_name>
     -username <username>
     ```

     Pour en savoir plus, `security webauthn credentials delete` consultez le "Référence de commande ONTAP".

Gérer les services Web

Présentation de la gestion des services Web

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

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

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

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

- L'utilisateur doit être authentifié.

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

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

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

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

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

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

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

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

Gérer l'accès aux services Web ONTAP

Un service Web est une application que les utilisateurs peuvent accéder via HTTP ou HTTPS. L'administrateur du cluster peut configurer le moteur de protocole Web, configurer SSL, activer un service Web et permettre aux utilisateurs d'un rôle d'accéder à un service Web.

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

- Infrastructure du processeur de service (`spi`)

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

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

- Les API ONTAP (`ontapi`)

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

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

- Détection Data ONTAP (`disco`)

  Ce service permet aux applications de gestion externes de découvrir le cluster sur le réseau. Le paramètre

par défaut est `enabled`.

- Diagnostics du support (`supdiag`)

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

- System Manager (`sysmgr`)

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

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

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

- Documentation ONTAP (`docs`)

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

- API RESTful ONTAP (`docs_api`)

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

- Téléchargement de fichiers (`fud`)

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

- Messagerie ONTAP (`ontapmsg`)

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

- Portail ONTAP (`portal`)

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

- Interface ONTAP RESTful (`rest`)

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

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

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

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

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

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

- Fichiers de sauvegarde de configuration (`backups`)

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

- Sécurité ONTAP (`security`)

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

Gérer le moteur de protocole Web dans ONTAP

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

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

- Vous pouvez indiquer si les clients distants peuvent utiliser HTTP ou HTTPS pour accéder au contenu du service Web à l'aide de l' `system services web modify` commande avec `-external` paramètre.
- Vous pouvez spécifier si SSLv3 doit être utilisé pour un accès Web sécurisé à l'aide de l' `security config modify` commande avec `-supported-protocol` paramètre.
  Par défaut, SSLv3 est désactivé. La sécurité de la couche de transport 1.0 (TLSv1) est activée et elle peut être désactivée si nécessaire.

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

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

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

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

conformité FIPS 140-2 puis désactivez-le, TLSv1 et SSLv3 restent désactivés, mais TLSv1.2 ou les deux TLSv1.1 et TLSv1.2 sont activés en fonction de la configuration précédente.

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

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

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

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

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

Commandes ONTAP pour la gestion du moteur de protocole Web

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

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

Les fonctions que vous recherchez…	Utilisez cette commande…
Associer une politique de pare-feu à une LIF	`network interface modify` Vous pouvez utiliser le `-firewall-policy` Paramètre pour modifier la politique de pare-feu d'une LIF.

Informations associées

- "modification de l'interface réseau"

Configurer l'accès aux services Web ONTAP

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

Étapes

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

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

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

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

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

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

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

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

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

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

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

commande.

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

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

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

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

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

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

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

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

Commandes ONTAP pour la gestion des services Web

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

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

Les fonctions que vous recherchez…	Utilisez cette commande…
Afficher les rôles autorisés pour accéder aux services web sur le cluster ou anSVM	`vserver services web access show`
Empêcher un rôle d'accéder à un service Web sur le cluster ou anSVM	`vserver services web access delete`

Informations associées

"Référence de commande ONTAP"

Commandes de gestion des points de montage sur les nœuds ONTAP

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

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

Informations associées

"Référence de commande ONTAP"

Gérer SSL dans ONTAP

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

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

- Activation de SSL
- Génération et installation d'un certificat numérique et son association au cluster ou à la SVM
- Affichage de la configuration SSL pour voir si SSL a été activé et, le cas échéant, le nom du certificat SSL

- Configuration de politiques de pare-feu pour le cluster ou SVM, de sorte que les demandes d'accès Web puissent passer par
- Définition des versions SSL pouvant être utilisées
- Limiter l'accès aux requêtes HTTPS uniquement pour un service Web

Commandes pour la gestion de SSL

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

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

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

Utiliser HSTS pour les services Web ONTAP

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

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

Description de la tâche

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

Avant de commencer

- Des privilèges avancés sont requis pour les tâches suivantes.

Afficher la configuration HSTS

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

Étapes

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

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

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

Activer HSTS et définir l'âge maximum

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

Étapes

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

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

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

Désactiver HSTS

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

Étapes

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

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

Informations associées

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

Résoudre les problèmes d'accès au service Web ONTAP

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

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

Ce problème d'accès…	Se produit en raison de cette erreur de configuration…	Pour résoudre l'erreur…
Votre navigateur Web renvoie un `unable to connect` ou `failure to establish a connection` erreur lorsque vous essayez d'accéder à un service web.	Votre LIF n'est peut-être pas configurée correctement.	Assurez-vous de pouvoir envoyer une requête ping à la LIF qui fournit le service Web. Vous utilisez `network ping` la commande pour envoyer une requête ping à une LIF.

Ce problème d'accès…	Se produit en raison de cette erreur de configuration…	Pour résoudre l'erreur…
Votre pare-feu est peut-être configuré de manière incorrecte.	Assurez-vous qu'une politique de pare-feu est configurée pour prendre en charge HTTP ou HTTPS et que la politique est attribuée à la LIF qui fournit le service Web. Vous utilisez le `system services firewall policy` commandes permettant de gérer les politiques de pare-feu. Vous utilisez le `network interface modify` commande avec `-firewall -policy` Paramètre pour associer une policy à une LIF.	Votre moteur de protocole Web peut être désactivé.
Assurez-vous que le moteur de protocole Web est activé pour que les services Web soient accessibles. Vous utilisez le `system services web` commandes permettant de gérer le moteur de protocole web pour le cluster.	Votre navigateur Web renvoie un `not found` erreur lorsque vous essayez d'accéder à un service web.	Le service Web est peut-être désactivé.
Assurez-vous que chaque service Web auquel vous souhaitez autoriser l'accès est activé individuellement. Vous utilisez le `vserver services web modify` commande permettant d'activer un service web pour l'accès.	Le navigateur Web ne parvient pas à se connecter à un service Web avec le nom de compte et le mot de passe d'un utilisateur.	L'utilisateur ne peut pas être authentifié, la méthode d'accès n'est pas correcte ou l'utilisateur n'est pas autorisé à accéder au service Web.

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

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

Informations associées

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

Vérifiez l'identité des serveurs distants à l'aide de certificats

En savoir plus sur la vérification de l'identité des serveurs distants à l'aide de certificats dans ONTAP

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.

Vérifier la validité des certificats numériques à l'aide d'OCSP dans ONTAP

Le protocole OCSP (Online Certificate Status Protocol) permet aux applications ONTAP qui utilisent les communications TLS (Transport Layer Security) de recevoir l'état du certificat numérique lorsque 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.

Avant de commencer

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	`security config ocsp enable -app app name`
Désactivé	`security config ocsp disable -app app name`

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	`security config ocsp enable`
	
	`-app all`

Désactivé	`security config ocsp disable`
	
	`-app all`

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 ocsp show` Commande pour afficher toutes les applications qui prennent en charge OCSP et leur état de support.

```
cluster::*> security config ocsp 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.
```

Informations associées

- "configuration de sécurité ocsp activer"
- "configuration de sécurité ocsp désactivée"
- "configuration de sécurité ocsp show"

Afficher les certificats par défaut pour les applications basées sur TLS dans ONTAP

ONTAP fournit un ensemble par défaut de certificats racine approuvés pour les applications ONTAP utilisant Transport Layer Security (TLS).

Avant de commencer

Les certificats par défaut sont installés uniquement sur le SVM d'administration lors de sa création ou lors d'une mise à niveau.

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`

   ```
   cluster1::> security certificate show

   Vserver    Serial Number   Certificate Name
   Type
   ---------- --------------- ----------------------------------------
   ---------
   vs0        4F4E4D7B         www.example.com
   server
       Certificate Authority:  www.example.com
             Expiration Date: Thu Feb 28 16:08:28 2013
   ```

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

Authentifier mutuellement le cluster et un serveur KMIP

Authentification mutuelle du cluster ONTAP et d'un aperçu du 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.

Générez une demande de signature de certificat pour le cluster dans ONTAP

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.

Avant de commencer

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 en savoir plus, `security certificate generate-csr` consultez le "Référence de commande ONTAP".

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-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----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.

Installer un certificat de serveur signé par une autorité de certification pour le cluster ONTAP

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.

Avant de commencer

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.

   Pour en savoir plus, `security certificate create` consultez le "Référence de commande ONTAP".

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.

Informations associées

- "installation du certificat de sécurité"
- "certificat de sécurité afficher"

Installer un certificat client signé par une autorité de certification pour le serveur KMIP dans ONTAP

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-----
<certificate_value>
-----END CERTIFICATE-----


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

cluster1::>
```

Informations associées

- "installation du certificat de sécurité"