



Comptes d'administrateur du stockage local

ONTAP Technical Reports

NetApp
January 23, 2026

Sommaire

Comptes d'administrateur du stockage local	1
Rôles, applications et authentification ONTAP	1
Rôles	1
Méthodes d'application	4
Méthodes d'authentification	5
Comptes d'administration par défaut	6
Répertorie les comptes locaux	6
Définissez le mot de passe du compte de diagnostic (diag)	7
Vérification multi-administrateurs	8
Verrouillage des copies Snapshot	9
Configurez l'accès à l'API basée sur un certificat	9
Authentification basée sur jeton OAuth 2.0 ONTAP pour l'API REST	12
Paramètres de connexion et de mot de passe	12
Nouvelles fonctionnalités de compte local	13
Prise en charge de SHA-512	13
Paramètres de mot de passe	15

Comptes d'administrateur du stockage local

Rôles, applications et authentification ONTAP

ONTAP offre aux entreprises soucieuses de leur sécurité la possibilité de fournir un accès granulaire à différents administrateurs via différentes applications et méthodes de connexion. Les clients peuvent ainsi créer un modèle zéro confiance centré sur les données.

Il s'agit des rôles disponibles pour les administrateurs admin et Storage Virtual machine. Les méthodes d'application de connexion et les méthodes d'authentification de connexion sont spécifiées.

Rôles

Grâce au contrôle d'accès basé sur des rôles (RBAC), les utilisateurs n'ont accès qu'aux systèmes et aux options requis pour leurs rôles et fonctions. La solution RBAC d'ONTAP limite l'accès administratif des utilisateurs au niveau correspondant à leur rôle, ce qui permet aux administrateurs de gérer les utilisateurs par rôle attribué. ONTAP fournit plusieurs rôles prédéfinis. Les opérateurs et les administrateurs peuvent créer, modifier ou supprimer des rôles de contrôle d'accès personnalisés et peuvent spécifier des restrictions de compte pour des rôles spécifiques.

Rôles prédéfinis pour les administrateurs du cluster

Ce rôle...	Dispose de ce niveau d'accès...	Aux commandes ou répertoires de commandes suivants
admin	Tout	Tous les répertoires de commandes (DEFAULT)
admin-no-fsa (Disponible à partir de ONTAP 9.12.1)	Lecture/écriture	<ul style="list-style-type: none">Tous les répertoires de commandes (DEFAULT)security login rest-rolesecurity login role

Lecture seule	<ul style="list-style-type: none"> • security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics 	Aucune
volume file show-disk-usage	autosupport	Tout
<ul style="list-style-type: none"> • set • system node autosupport 	Aucune	Tous les autres répertoires de commandes (DEFAULT)
backup	Tout	vserver services ndmp
Lecture seule	volume	Aucune
Tous les autres répertoires de commandes (DEFAULT)	readonly	Tout
<ul style="list-style-type: none"> • security login password Pour la gestion du mot de passe local et des informations clés du compte utilisateur • set 	Aucune	security

Lecture seule	Tous les autres répertoires de commandes (DEFAULT)	none
---------------	--	------



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

Rôles prédéfinis pour les administrateurs des machines virtuelles de stockage (SVM)

Nom du rôle	Capacités
<code>vsadmin</code>	<ul style="list-style-type: none"> • Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gérez les volumes, à l'exception des déplacements de volumes • Gérez les quotas, les qtrees, les copies Snapshot et les fichiers • Gérer les LUN • Effectuer des opérations SnapLock, sauf la suppression privilégiée • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Surveiller les tâches • Surveiller les connexions réseau et l'interface réseau • Surveiller l'état de santé du SVM
<code>vsadmin-volume</code>	<ul style="list-style-type: none"> • Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gérez les volumes, à l'exception des déplacements de volumes • Gérez les quotas, les qtrees, les copies Snapshot et les fichiers • Gérer les LUN • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Interface réseau du moniteur • Surveiller l'état de santé du SVM

vsadmin-protocol	<ul style="list-style-type: none"> • Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Gérer les LUN • Interface réseau du moniteur • Surveiller l'état de santé du SVM
vsadmin-backup	<ul style="list-style-type: none"> • Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gestion des opérations NDMP • Effectuez une lecture/écriture de volume restauré • Gestion des relations SnapMirror et des copies Snapshot • Afficher les volumes et les informations réseau
vsadmin-snaplock	<ul style="list-style-type: none"> • Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gérez les volumes, à l'exception des déplacements de volumes • Gérez les quotas, les qtrees, les copies Snapshot et les fichiers • Effectuer des opérations SnapLock, y compris la suppression privilégiée • Configuration des protocoles : NFS et SMB • Configuration des services : DNS, LDAP et NIS • Surveiller les tâches • Surveiller les connexions réseau et l'interface réseau
vsadmin_READONLY	<ul style="list-style-type: none"> • Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Surveiller l'état de santé du SVM • Interface réseau du moniteur • Vision des volumes et des LUN • Vision des services et protocoles

Méthodes d'application

La méthode d'application spécifie le type d'accès de la méthode de connexion. Les valeurs possibles incluent `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, et `telnet`.

La définition de ce paramètre sur `service-processor` l'utilisateur l'accès au processeur de service. Lorsque ce paramètre est défini sur `service-processor`, le `-authentication-method` paramètre doit être défini sur `password` car le processeur de service prend uniquement en charge `password` l'authentification. Les comptes utilisateurs SVM ne peuvent pas accéder au processeur de service. Par conséquent, les opérateurs et les administrateurs ne peuvent pas utiliser le `-vserver` paramètre lorsque ce paramètre est défini sur `service-processor`.

Pour restreindre davantage l'accès à l'`service-processor`, utilisez la commande `system service-processor ssh add-allowed-addresses`. La commande `system service-processor api-service` peut être utilisée pour mettre à jour les configurations et les certificats.

Pour des raisons de sécurité, Telnet et le shell distant (RSH) sont désactivés par défaut car NetApp recommande le shell sécurisé (SSH) pour un accès distant sécurisé. S'il existe une exigence ou un besoin unique de Telnet ou RSH, ils doivent être activés.

La `security protocol modify` commande modifie la configuration existante de RSH et Telnet au niveau du cluster. Activez RSH et Telnet dans le cluster en définissant le champ activé sur `true`.

Méthodes d'authentification

Le paramètre de méthode d'authentification spécifie la méthode d'authentification utilisée pour les connexions.

METHODE d'authentification	Description
<code>cert</code>	Authentification par certificat SSL
<code>community</code>	Chaînes de communauté SNMP
<code>domain</code>	Authentification Active Directory
<code>nsswitch</code>	Authentification LDAP ou NIS
<code>password</code>	Mot de passe
<code>publickey</code>	Authentification par clé publique
<code>usm</code>	Modèle de sécurité utilisateur SNMP



L'utilisation de NIS n'est pas recommandée en raison des faiblesses de sécurité du protocole.

À partir de la version ONTAP 9.3, une authentification à deux facteurs est disponible en chaîne pour les comptes SSH locaux `admin` à l'aide des `publickey` deux méthodes d'authentification et `password`. En plus du `-authentication-method` champ de la `security login` commande, un nouveau champ nommé `-second-authentication-method` a été ajouté. `publickey``Ou ``password` peut être spécifié en tant que `-authentication-method` ou `-second-authentication-method`. Cependant, lors de l'authentification SSH, l'ordre est toujours `publickey` avec une authentification partielle, suivie de l'invite de mot de passe pour une authentification complète.

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

À partir de ONTAP 9.4, nsswitch peut être utilisé comme deuxième méthode d'authentification avec publickey.

A partir de ONTAP 9.12.1, FIDO2 peut également être utilisé pour l'authentification SSH à l'aide d'un dispositif d'authentification matérielle YubiKey ou d'autres appareils compatibles FIDO2.

À partir de ONTAP 9.13.1 :

- domain les comptes peuvent être utilisés comme deuxième méthode d'authentification avec publickey.
- Mot de passe à usage unique basé sur l'heure (totp) est un code d'accès temporaire généré par un algorithme qui utilise l'heure actuelle comme l'un de ses facteurs d'authentification pour la deuxième méthode d'authentification.
- La révocation des clés publiques est prise en charge avec les clés publiques SSH ainsi que les certificats qui seront vérifiés pour leur expiration/révocation au cours de SSH.

Pour plus d'informations sur l'authentification multifacteur (MFA) pour ONTAP System Manager, Active IQ Unified Manager et SSH, consultez la section "[Tr-4647 : authentification multifacteur dans ONTAP 9](#)".

Comptes d'administration par défaut

Le compte admin doit être restreint car le rôle d'administrateur est autorisé à accéder à l'aide de toutes les applications. Le compte diag permet l'accès à l'interpréteur de commandes du système et ne doit être réservé qu'au support technique pour effectuer les tâches de dépannage.

Il existe deux comptes d'administration par défaut : admin et diag.

Les comptes orphelins sont un vecteur de sécurité majeur qui entraîne souvent des vulnérabilités, y compris l'escalade des priviléges. Il s'agit de comptes inutiles et inutilisés qui restent dans le référentiel de comptes d'utilisateurs. Il s'agit principalement de comptes par défaut qui n'ont jamais été utilisés ou pour lesquels les mots de passe n'ont jamais été mis à jour ou modifiés. Pour résoudre ce problème, ONTAP prend en charge la suppression et le changement de nom des comptes.



Vous ne pouvez pas supprimer ni renommer les comptes intégrés. Si un administrateur supprime le compte, au redémarrage, le compte intégré sera recréé. **NetApp recommande** de verrouiller tout compte intégré inutile avec la commande lock.

Bien que les comptes orphelins constituent un problème de sécurité important, **NetApp recommande fortement** de tester l'effet de la suppression des comptes du référentiel de comptes local.

Répertorie les comptes locaux

Pour lister les comptes locaux, exécutez la `security login show` commande.

```
cluster1::*> security login show -vserver cluster1

vserver: cluster1
          Authentication          Acct  Is-Nsswitch
User/Group Name Application Method  Role Name  Locked Group
-----
admin          console      password  admin      no      no
admin          http        password  admin      no      no
admin          ontapi       password  admin      no      no
admin          service-processor password admin      no      no
admin          ssh         password  admin      no      no
autosupport    console      password  autosupport      no      no
6 entries were displayed.
```

Définissez le mot de passe du compte de diagnostic (diag)

Un compte de diagnostic nommé `diag` est fourni avec votre système de stockage. Vous pouvez utiliser le `diag` compte pour effectuer des tâches de dépannage dans `systemshell`. Le `diag` compte est le seul compte qui peut être utilisé pour accéder au `systemshell` via la `diag` commande Privileged `systemshell`.

 Le `systemshell` et le compte associé `diag` sont destinés à des fins de diagnostic de bas niveau. Leur accès requiert le niveau de privilège diagnostic et est réservé uniquement pour être utilisé avec l'aide du support technique pour effectuer des tâches de dépannage. Ni le compte ni le `diag systemshell` est destiné à des fins administratives générales.

Avant de commencer

Avant d'accéder au `systemshell`, vous devez définir le `diag` mot de passe du compte à l'aide de la `security login password` commande. Vous devez utiliser des principes de mot de passe forts et modifier le `diag` mot de passe à intervalles réguliers.

Étapes

1. Définissez le `diag` mot de passe de l'utilisateur du compte :

```
cluster1::> set -privilege diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? \{y|n\}: y

cluster1::*> systemshell -node node-01
  (system node systemshell)
diag@node-01's password:

Warning: The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly. Use this environment
only when directed to do so by support personnel.

node-01%
```

Vérification multi-administrateurs

À partir de ONTAP 9.11.1, vous pouvez utiliser la vérification multiadministrateur pour permettre l'exécution de certaines opérations, telles que la suppression de volumes ou de snapshots, uniquement après approbation par les administrateurs désignés. Cela empêche les administrateurs compromis, malveillants ou peu expérimentés d'effectuer des modifications ou de supprimer des données indésirables.

La configuration de MAV comprend les éléments suivants :

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

Après la configuration initiale, seuls les administrateurs d'un groupe d'approbation MAV (administrateurs MAV) peuvent modifier ces éléments.

Lorsque MAV est activé, la réalisation de chaque opération protégée nécessite trois étapes :

1. Lorsqu'un utilisateur lance l'opération, un ["une demande est générée"](#).
2. Avant de pouvoir l'exécuter, le nombre requis de ["Les administrateurs MAV doivent approuver"](#).
3. Après approbation, l'utilisateur termine l'opération.

La MAV n'est pas destinée à être utilisée avec des volumes ou des flux de travail qui impliquent une automatisation poussée car chaque tâche automatisée nécessite une approbation avant que l'opération ne puisse être terminée. Si vous souhaitez utiliser l'automatisation et la vérification multiniveau ensemble, NetApp vous recommande d'utiliser des requêtes pour des opérations de vérification multiniveau 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.

Pour plus d'informations sur MAV, reportez-vous à la "["Documentation de vérification multiadministrateur ONTAP"](#)".

Verrouillage des copies Snapshot

Le verrouillage des snapshots est une fonctionnalité SnapLock dans laquelle les snapshots sont rendus indélébiles manuellement ou automatiquement avec une période de conservation définie dans la règle Snapshot du volume. Le verrouillage des snapshots permet d'empêcher les administrateurs peu scrupuleux ou non approuvés de supprimer des snapshots sur le système ONTAP principal ou secondaire.

Le verrouillage des snapshots a été introduit dans ONTAP 9.12.1. Le verrouillage des snapshots est également appelé verrouillage inviolable des snapshots. Bien qu'il nécessite la licence SnapLock et l'initialisation de l'horloge de conformité, le verrouillage des snapshots n'est pas lié à SnapLock Compliance ou SnapLock Enterprise. Il n'existe aucun administrateur de confiance dans le stockage, comme pour SnapLock Enterprise, et il ne protège pas l'infrastructure de stockage physique sous-jacente, comme pour SnapLock Compliance. Il s'agit d'une amélioration par rapport aux snapshots SnapVaulting sur un système secondaire. La restauration rapide des copies Snapshot verrouillées sur les systèmes primaires peut être effectuée pour restaurer les volumes corrompus par des ransomwares.

Pour plus de détails, voir "["documentation sur le verrouillage des snapshots"](#)".

Configurez l'accès à l'API basée sur un certificat

Au lieu de l'authentification par ID utilisateur et mot de passe pour l'accès à ONTAP par l'API REST ou l'API du SDK de gestion NetApp, l'authentification basée sur certificat doit être utilisée.



Comme alternative à l'authentification basée sur certificat pour l'API REST, utilisez "["Authentification par jeton OAuth 2.0"](#)".

Vous pouvez générer et installer un certificat auto-signé sur ONTAP comme décrit dans ces étapes.

Étapes

1. À l'aide d'OpenSSL, générez un certificat en exécutant la commande suivante :

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'test.key'
```

Cette commande génère un certificat public nommé `test.pem` et une clé privée nommée `key.out`. Le nom commun, CN, correspond à l'ID utilisateur ONTAP.

2. Installez le contenu du certificat public au format courrier amélioré confidentiel (pem) dans ONTAP en exécutant la commande suivante et en collant le contenu du certificat lorsque vous y êtes invité :

```
security certificate install -type client-ca -vserver cluster1
```

```
Please enter Certificate: Press <Enter> when done
```

3. Activez ONTAP pour autoriser l'accès client via SSL et définissez l'ID utilisateur pour l'accès API.

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

Dans l'exemple suivant, l'ID utilisateur `cert_user` est désormais activé pour utiliser l'accès à l'API authentifié par certificat. Un script Python du SDK de gestion simple utilisant `cert_user` pour afficher la version ONTAP apparaît comme suit :

```

#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)

```

La sortie du script affiche la version ONTAP.

```

./version.py

V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018

```

4. Pour effectuer une authentification basée sur un certificat avec l'API REST ONTAP, procédez comme suit :
- a. Dans ONTAP, définissez l'ID utilisateur pour l'accès http :

```

security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1

```

- b. Sur votre client Linux, exécutez la commande suivante qui produit la version ONTAP en tant que sortie :

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key ./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
  "version": {
    "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
    "generation": 9,
    "major": 7,
    "minor": 0
  },
  "_links": {
    "self": {
      "href": "/api/cluster"
    }
  }
}
```

Plus d'informations

- ["Authentification basée sur certificat avec le SDK de gestion NetApp pour ONTAP"](#).

Authentification basée sur jeton OAuth 2.0 ONTAP pour l'API REST

En alternative à l'authentification basée sur certificat, vous pouvez utiliser l'authentification basée sur jeton OAuth 2.0 pour l'API REST.

Depuis ONTAP 9.14.1, 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.

Les jetons OAuth 2.0 remplacent les mots de passe pour l'authentification des comptes utilisateur.

Pour plus d'informations sur l'utilisation d'OAuth 2.0, consultez le ["Documentation ONTAP sur l'authentification et l'autorisation via OAuth 2.0"](#).

Paramètres de connexion et de mot de passe

Une stratégie de sécurité efficace est conforme aux politiques, aux directives et à toute gouvernance ou norme établies de l'entreprise. La durée de vie du nom d'utilisateur, les exigences de longueur du mot de passe, les exigences en termes de caractères et le stockage de ces comptes sont des exemples de ces exigences. La solution ONTAP offre des fonctionnalités pour traiter ces constructions de sécurité.

Nouvelles fonctionnalités de compte local

Pour prendre en charge les stratégies, directives ou normes de compte utilisateur d'une entreprise, notamment la gouvernance, les fonctionnalités suivantes sont prises en charge dans ONTAP :

- Configuration des stratégies de mot de passe pour appliquer un nombre minimum de chiffres, de minuscules ou de majuscules
- Délai nécessaire après un échec de la tentative de connexion
- Définition de la limite d'inactivité du compte
- Expiration d'un compte utilisateur
- Affichage d'un message d'avertissement d'expiration de mot de passe
- Notification d'une connexion non valide



Les paramètres configurables sont gérés à l'aide de la commande `Security login role config modify`.

Prise en charge de SHA-512

Pour améliorer la sécurité des mots de passe, ONTAP 9 prend en charge la fonction de hachage SHA-2 et utilise par défaut la fonction SHA-512 pour hacher les nouveaux mots de passe ou les mots de passe modifiés. Les opérateurs et les administrateurs peuvent également expirer ou verrouiller les comptes selon les besoins.

Les comptes utilisateur ONTAP 9 préexistants avec des mots de passe inchangés continuent d'utiliser la fonction de hachage MD5 après la mise à niveau vers ONTAP 9.0 ou version ultérieure. Cependant, NetApp recommande vivement de migrer ces comptes utilisateur vers la solution SHA-512 plus sécurisée en demandant aux utilisateurs de modifier leur mot de passe.

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

- Afficher les comptes utilisateur correspondant à la fonction de hachage spécifiée :

```
cluster1::>*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name application authentication-method hash-
function
-----
-----
cluster1 NewAdmin          console      password      sha512
cluster1 NewAdmin          ontapi       password      sha512
cluster1 NewAdmin          ssh          password      sha512
```

- Comptes expirés utilisant une fonction de hachage spécifiée (MD5, par exemple), qui oblige les utilisateurs à modifier leur mot de passe lors de la connexion suivante :

```
cluster1::>*> security login expire-password -vserver * -username * -hash
-function md5
```

- Verrouiller les comptes avec des mots de passe utilisant la fonction de hachage spécifiée.

```
cluster1::*> security login lock -vserver * -username * -hash-function
md5
```

La fonction de hachage password est inconnue pour l'utilisateur interne autosupport du SVM d'administration de votre cluster. Ce problème est cosmétique. La fonction de hachage est inconnue car cet utilisateur interne ne dispose pas d'un mot de passe configuré par défaut.

- Pour afficher la fonction de hachage du mot de passe de l' autosupport utilisateur, exécutez les commandes suivantes :

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

          Vserver: cluster1
          User Name or Group Name: autosupport
          Application: console
          Authentication Method: password
          Remote Switch IP Address: -
          Role Name: autosupport
          Account Locked: no
          Comment Text: -
          Whether Ns-switch Group: no
          Password Hash Function: unknown
          Second Authentication Method2: none
```

- Pour définir la fonction de hachage du mot de passe (par défaut : sha512), exécutez la commande suivante :

```
::> security login password -username autosupport
```

La définition du mot de passe n'a pas d'importance.

```

security login show -user-or-group-name autosupport -instance

          Vserver: cluster1
          User Name or Group Name: autosupport
          Application: console
          Authentication Method: password
          Remote Switch IP Address: -
          Role Name: autosupport
          Account Locked: no
          Comment Text: -
          Whether Ns-switch Group: no
          Password Hash Function: sha512
          Second Authentication Method2: none

```

Paramètres de mot de passe

La solution ONTAP prend en charge les paramètres de mot de passe qui répondent aux exigences et directives de l'entreprise et qui les prennent en charge.

Depuis 9.14.1, la complexité et les règles de verrouillage des mots de passe ne s'appliquent qu'aux nouvelles installations de ONTAP.

Tous les mots de passe doivent être distincts du nom d'utilisateur.

Attribut	Description	Valeur par défaut	Gamme
username-minlength	Longueur minimale du nom d'utilisateur requise	3	3-16
username-alphanum	Nom d'utilisateur alphanumérique	désactivé	Activé/Désactivé
passwd-minlength	Longueur minimale du mot de passe requise	8	3-64
passwd-alphanum	Mot de passe alphanumérique	activé	Activé/Désactivé
passwd-min-special-chars	Nombre minimum de caractères spéciaux requis dans le mot de passe	0	0-64
passwd-expiry-time	Heure d'expiration du mot de passe (en jours)	Illimité, ce qui signifie que les mots de passe n'expirent jamais	0-illimité 0 == expire maintenant
require-initial-passwd-update	Exiger la mise à jour initiale du mot de passe lors de la première connexion	Désactivé	Activé/Désactivé Modifications autorisées via la console ou SSH

Attribut	Description	Valeur par défaut	Gamme
max-failed-login-attempts	Nombre maximal de tentatives infructueuses	0, ne pas verrouiller le compte	-
lockout-duration	Durée maximale de verrouillage (en jours)	La valeur par défaut est 0, ce qui signifie que le compte est verrouillé pendant une journée	-
disallowed-reuse	Interdire les N derniers mots de passe	6	Le minimum est de 6
change-delay	Délai entre les modifications du mot de passe (en jours)	0	-
delay-after-failed-login	Délai après chaque tentative de connexion échouée (en secondes)	4	-
passwd-min-lowercase-chars	Nombre minimum de caractères alphabétiques minuscules requis dans le mot de passe	0, qui ne nécessite pas de caractères minuscules	0-64
passwd-min-uppercase-chars	Nombre minimum de caractères alphabétiques majuscules requis	0, qui ne nécessite pas de majuscules	0-64
passwd-min-digits	Nombre minimum de chiffres requis dans le mot de passe	0, qui ne nécessite pas de chiffres	0-64
passwd-expiry-warn-time	Afficher le message d'avertissement avant l'expiration du mot de passe (en jours)	Illimité, ce qui signifie ne jamais avertir de l'expiration du mot de passe	0, ce qui signifie avertir l'utilisateur de l'expiration du mot de passe à chaque connexion réussie
account-expiry-time	Le compte expire dans N jours	Illimité, ce qui signifie que les comptes n'expirent jamais	Le délai d'expiration du compte doit être supérieur à la limite d'inactivité du compte
account-inactive-limit	Durée maximale d'inactivité avant l'expiration du compte (en jours)	Illimité, ce qui signifie que les comptes inactifs n'expirent jamais	La limite d'inactivité du compte doit être inférieure à l'heure d'expiration du compte

Exemple

```
cluster1::*> security login role config show -vserver cluster1 -role admin

          Vserver: cluster1
          Role Name: admin
          Minimum Username Length Required: 3
          Username Alpha-Numeric: disabled
          Minimum Password Length Required: 8
          Password Alpha-Numeric: enabled
          Minimum Number of Special Characters Required in the Password: 0
          Password Expires In (Days): unlimited
          Require Initial Password Update on First Login: disabled
          Maximum Number of Failed Attempts: 0
          Maximum Lockout Period (Days): 0
          Disallow Last 'N' Passwords: 6
          Delay Between Password Changes (Days): 0
          Delay after Each Failed Login Attempt (Secs): 4
          Minimum Number of Lowercase Alphabetic Characters Required in the
          Password: 0
          Minimum Number of Uppercase Alphabetic Characters Required in the
          Password: 0
          Minimum Number of Digits Required in the Password: 0
          Display Warning Message Days Prior to Password Expiry (Days): unlimited
          Account Expires in (Days): unlimited
          Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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