



# Gérer les paramètres de sécurité du serveur SMB

ONTAP 9

NetApp  
September 12, 2024

# Sommaire

Gérer les paramètres de sécurité du serveur SMB .....	1
Gestion de l'authentification client SMB par ONTAP .....	1
Instructions relatives aux paramètres de sécurité des serveurs SMB dans une configuration de reprise d'activité des SVM .....	1
Affiche des informations sur les paramètres de sécurité du serveur SMB .....	2
Activez ou désactivez la complexité requise des mots de passe pour les utilisateurs SMB locaux .....	3
Modifiez les paramètres de sécurité Kerberos du serveur CIFS .....	5
Définissez le niveau de sécurité d'authentification minimum du serveur SMB .....	6
Configurez une sécurité forte pour les communications Kerberos à l'aide du chiffrement AES .....	7
Activez ou désactivez le chiffrement AES pour les communications basées sur Kerberos .....	8
Utilisez la signature SMB pour améliorer la sécurité du réseau .....	12
Configurez le chiffrement SMB requis sur les serveurs SMB pour les transferts de données via SMB .....	23
Communication de session LDAP sécurisée .....	32

# Gérer les paramètres de sécurité du serveur SMB

## Gestion de l'authentification client SMB par ONTAP

Avant que les utilisateurs puissent créer des connexions SMB pour accéder aux données contenues dans la SVM, ils doivent être authentifiés par le domaine auquel le serveur SMB appartient. Le serveur SMB prend en charge deux méthodes d'authentification, Kerberos et NTLM (NTLMv1 ou NTLMv2). Kerberos est la méthode par défaut utilisée pour authentifier les utilisateurs du domaine.

### Authentification Kerberos

ONTAP supporte l'authentification Kerberos lors de la création de sessions SMB authentifiées.

Kerberos est le service principal d'authentification pour Active Directory. Le serveur Kerberos, ou le Kerberos Key distribution Center (KDC) service, stocke et récupère des informations sur les principes de sécurité dans Active Directory. A la différence du modèle NTLM, les clients Active Directory qui souhaitent établir une session avec un autre ordinateur, tel que le serveur SMB, contactez directement un KDC pour obtenir leurs credentials de session.

### Authentification NTLM

L'authentification du client NTLM est effectuée à l'aide d'un protocole de réponse de défi basé sur une connaissance partagée d'un secret spécifique à un utilisateur basé sur un mot de passe.

Si un utilisateur crée une connexion SMB à l'aide d'un compte utilisateur Windows local, l'authentification est effectuée localement par le serveur SMB à l'aide de NTLMv2.

## Instructions relatives aux paramètres de sécurité des serveurs SMB dans une configuration de reprise d'activité des SVM

Avant de créer un SVM configuré en tant que destination de reprise d'activité pour laquelle l'identité n'est pas conservée (le `-identity-preserve` l'option est définie sur `false` En configuration SnapMirror), il est important de savoir comment les paramètres de sécurité des serveurs SMB sont gérés sur la SVM de destination.

- Les paramètres de sécurité du serveur SMB non par défaut ne sont pas répliqués sur la destination.

Lorsque vous créez un serveur SMB sur le SVM de destination, tous les paramètres de sécurité du serveur SMB sont définis sur les valeurs par défaut. Lors de l'initialisation, de la destination de reprise après incident du SVM, de la mise à jour ou de la resynchronisation, les paramètres de sécurité du serveur SMB sur la source ne sont pas répliqués sur la destination.

- Vous devez configurer manuellement les paramètres de sécurité du serveur SMB non par défaut.

Si vous avez configuré sur la SVM source des paramètres de sécurité du serveur SMB non par défaut,

vous devez configurer manuellement ces mêmes paramètres sur le SVM de destination après que la destination devienne read-write (après une interruption de la relation SnapMirror).

## Affiche des informations sur les paramètres de sécurité du serveur SMB

Vous pouvez afficher des informations sur les paramètres de sécurité du serveur SMB sur vos serveurs virtuels de stockage (SVM). Vous pouvez utiliser ces informations pour vérifier que les paramètres de sécurité sont corrects.

### Description de la tâche

Un paramètre de sécurité affiché peut être la valeur par défaut pour cet objet ou une valeur non par défaut configurée à l'aide de l'interface de ligne de commande ONTAP ou à l'aide d'objets de stratégie de groupe Active Directory.

N'utilisez pas le `vserver cifs security show` Commande pour les serveurs SMB en mode groupe de travail, car certaines options ne sont pas valides.

### Étape

1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher des informations sur...	Entrez la commande...
Tous les paramètres de sécurité sur un SVM spécifié	<code>vserver cifs security show -vserver <i>vserver_name</i></code>
Un paramètre de sécurité ou des paramètres spécifiques sur la SVM	<code>vserver cifs security show -vserver <i>_vserver_name_</i> -fields [fieldname,...]</code> Vous pouvez entrer <code>-fields ?</code> pour déterminer les champs que vous pouvez utiliser.

### Exemple

L'exemple suivant montre tous les paramètres de sécurité pour SVM vs1 :

```
cluster1::> vservers cifs security show -vservers vs1

Vserver: vs1

Kerberos Clock Skew: 5 minutes
Kerberos Ticket Age: 10 hours
Kerberos Renewal Age: 7 days
Kerberos KDC Timeout: 3 seconds
Is Signing Required: false
Is Password Complexity Required: true
Use start_tls For AD LDAP connection: false
Is AES Encryption Enabled: false
LM Compatibility Level: lm-ntlm-ntlmv2-krb
Is SMB Encryption Required: false
Client Session Security: none
SMB1 Enabled for DC Connections: false
SMB2 Enabled for DC Connections: system-default
LDAP Referral Enabled For AD LDAP connections: false
Use LDAPS for AD LDAP connection: false
Encryption is required for DC Connections: false
AES session key enabled for NetLogon channel: false
Try Channel Binding For AD LDAP Connections: false
```

Notez que les paramètres affichés dépendent de la version ONTAP en cours d'exécution.

L'exemple suivant montre l'inclinaison de l'horloge Kerberos pour le SVM vs1 :

```
cluster1::> vservers cifs security show -vservers vs1 -fields kerberos-
clock-skew

vservers kerberos-clock-skew
-----
vs1      5
```

#### Informations associées


[Affichage des informations sur les configurations GPO](#)

## Activez ou désactivez la complexité requise des mots de passe pour les utilisateurs SMB locaux

Au-dessus de vos SVM, la complexité requise par mot de passe renforce la sécurité des utilisateurs SMB locaux. La fonction de complexité de mot de passe requise est activée par défaut. Vous pouvez le désactiver et le réactiver à tout moment.

Avant de commencer

Les utilisateurs locaux, les groupes locaux et l'authentification des utilisateurs locaux doivent être activés sur le serveur CIFS.



**Description de la tâche**

Vous ne devez pas utiliser le `vserver cifs security modify` Commande pour un serveur CIFS en mode groupe de travail car certaines options ne sont pas valides.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous voulez que les utilisateurs de PME locales aient besoin de complexité de mot de passe...	Entrez la commande...
Activé	<code>vserver cifs security modify -vserver vserver_name -is-password-complexity -required true</code>
Désactivé	<code>vserver cifs security modify -vserver vserver_name -is-password-complexity -required false</code>

2. Vérifiez le paramètre de sécurité pour connaître la complexité requise du mot de passe : `vserver cifs security show -vserver vserver_name`

Exemple

L'exemple suivant montre que la complexité requise des mots de passe est activée pour les utilisateurs SMB locaux pour le SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
-----
vs1      true
```

Informations associées

- [Affichage d'informations sur les paramètres de sécurité du serveur CIFS](#)
- [Utilisation d'utilisateurs et de groupes locaux pour l'authentification et l'autorisation](#)
- [Conditions requises pour les mots de passe des utilisateurs locaux](#)
- [Modification des mots de passe des comptes utilisateur locaux](#)

# Modifiez les paramètres de sécurité Kerberos du serveur CIFS

Vous pouvez modifier certains paramètres de sécurité Kerberos pour le serveur CIFS, notamment le temps d'inclinaison maximal autorisé de l'horloge Kerberos, la durée de vie du ticket Kerberos et le nombre maximum de jours de renouvellement de ticket.

## Description de la tâche

Modification des paramètres Kerberos du serveur CIFS à l'aide de `vserver cifs security modify` La commande modifie les paramètres uniquement sur la machine virtuelle de stockage (SVM) que vous spécifiez avec le `-vserver` paramètre. Vous pouvez gérer de manière centralisée les paramètres de sécurité Kerberos pour tous les SVM du cluster appartenant au même domaine Active Directory à l'aide des objets de stratégie de groupe Active Directory.

## Étapes

- 1. Effectuez une ou plusieurs des opérations suivantes :

Les fonctions que vous recherchez...	Entrer...
Spécifiez le temps maximal autorisé d'inclinaison de l'horloge Kerberos en minutes (9.13.1 et versions ultérieures) ou en secondes (9.12.1 ou versions antérieures).	<pre>vserver cifs security modify -vserver vserver_name -kerberos-clock-skew integer_in_minutes</pre> <p>La valeur par défaut est 5 minutes.</p>
Spécifiez la durée de vie du ticket Kerberos en heures.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-ticket-age integer_in_hours</pre> <p>Le paramètre par défaut est 10 heures.</p>
Spécifiez le nombre maximum de jours de renouvellement de billet.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days</pre> <p>Le paramètre par défaut est 7 jours.</p>
Spécifiez le délai d'expiration des sockets sur les KDC après lequel tous les KDC sont marqués comme inaccessibles.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds</pre> <p>Le réglage par défaut est de 3 secondes.</p>

- 2. Vérifiez les paramètres de sécurité Kerberos :

```
vserver cifs security show -vserver vserver_name
```

## Exemple

L'exemple suivant apporte les modifications suivantes à la sécurité Kerberos : « Kerberos Clock Skew » est

défini sur 3 minutes et « Kerberos Ticket Age » est défini sur 8 heures pour le SVM vs1 :

```
cluster1::> vsserver cifs security modify -vsserver vs1 -kerberos-clock-skew  
3 -kerberos-ticket-age 8
```

```
cluster1::> vsserver cifs security show -vsserver vs1
```

Vserver: vs1

Kerberos Clock Skew:	3 minutes
Kerberos Ticket Age:	8 hours
Kerberos Renewal Age:	7 days
Kerberos KDC Timeout:	3 seconds
Is Signing Required:	false
Is Password Complexity Required:	true
Use start_tls For AD LDAP connection:	false
Is AES Encryption Enabled:	false
LM Compatibility Level:	lm-ntlm-ntlmv2-krb
Is SMB Encryption Required:	false

#### Informations associées

["Affichage d'informations sur les paramètres de sécurité du serveur CIFS"](#)

["Stratégies de groupe prises en charge"](#)

["Application d'objets de stratégie de groupe aux serveurs CIFS"](#)

## Définissez le niveau de sécurité d'authentification minimum du serveur SMB

Vous pouvez définir le niveau de sécurité minimum du serveur SMB, également appelé *LMCompatibilityLevel*, sur votre serveur SMB afin de répondre aux besoins de sécurité de votre entreprise pour l'accès client SMB. Le niveau de sécurité minimum est le niveau minimum des jetons de sécurité que le serveur SMB accepte des clients SMB.



#### Description de la tâche

- Les serveurs SMB en mode groupe de travail prennent uniquement en charge l'authentification NTLM. L'authentification Kerberos n'est pas prise en charge.
- *LMCompatibilityLevel* s'applique uniquement à l'authentification du client SMB, et non à l'authentification de l'administrateur.

Vous pouvez définir le niveau de sécurité d'authentification minimum sur l'un des quatre niveaux de sécurité pris en charge.



Valeur	Description
lm-ntlm-ntlmv2-krb (valeur par défaut)	La machine virtuelle de stockage (SVM) accepte les authentifications LM, NTLM, NTLMv2 et Kerberos.
ntlm-ntlmv2-krb	Le SVM accepte la sécurité d'authentification NTLM, NTLMv2, et Kerberos. Le SVM refuse l'authentification LM.
ntlmv2-krb	Le SVM accepte la sécurité d'authentification NTLMv2 et Kerberos. Le SVM refuse l'authentification LM et NTLM.
krb	Le SVM n'accepte que la sécurité d'authentification Kerberos. Le SVM refuse l'authentification LM, NTLM et NTLMv2.

## Étapes

1. Définissez le niveau de sécurité d'authentification minimum : `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Vérifiez que le niveau de sécurité d'authentification est défini sur le niveau souhaité : `vserver cifs security show -vserver vserver_name`

## Informations associées

[Activation ou désactivation du chiffrement AES pour les communications basées sur Kerberos](#)

# Configurez une sécurité forte pour les communications Kerberos à l'aide du chiffrement AES

Pour une sécurité renforcée avec les communications basées sur Kerberos, vous pouvez activer le chiffrement AES-256 et AES-128 sur le serveur SMB. Par défaut, lorsque vous créez un serveur SMB sur le SVM, le chiffrement Advanced Encryption Standard (AES) est désactivé. Elle doit permettre aux services IT de bénéficier de la sécurité renforcée fournie par le cryptage AES.

La communication Kerberos pour SMB est utilisée lors de la création du serveur SMB sur le SVM, ainsi que lors de la phase d'installation de la session SMB. Le serveur SMB prend en charge les types de chiffrement suivants pour les communications Kerberos :

- AES 256
- AES 128
- DES
- RC4-HMAC

Si vous souhaitez utiliser le type de chiffrement le plus élevé pour les communications Kerberos, vous devez activer le chiffrement AES pour la communication Kerberos sur la SVM.

Lorsque le serveur SMB est créé, le contrôleur de domaine crée un compte de machine informatique dans Active Directory. À l'heure actuelle, le KDC prend connaissance des capacités de cryptage du compte machine particulier. Par la suite, un type de chiffrement particulier est sélectionné pour le chiffrement du ticket de service que le client présente au serveur lors de l'authentification.

À partir de ONTAP 9.12.1, vous pouvez spécifier les types de cryptage à publier sur le KDC Active Directory (AD). Vous pouvez utiliser le `-advertised-enc-types` pour activer les types de cryptage recommandés, vous pouvez l'utiliser pour désactiver les types de cryptage les plus faibles. Découvrez comment ["Activez et désactivez les types de cryptage pour les communications Kerberos"](#).



Intel AES New instructions (Intel AES ni) est disponible dans SMB 3.0. Il améliore l'algorithme AES et accélère le chiffrement des données avec les familles de processeurs prises en charge. À partir de SMB 3.1.1, AES-128-GCM remplace AES-128-CCM en tant qu'algorithme de hachage utilisé par le chiffrement SMB.

#### Informations associées

[Modification des paramètres de sécurité Kerberos du serveur CIFS](#)

## Activez ou désactivez le chiffrement AES pour les communications basées sur Kerberos

Pour bénéficier de la sécurité la plus forte des communications basées sur Kerberos, vous devez utiliser le chiffrement AES-256 et AES-128 sur le serveur SMB. À partir de ONTAP 9.13.1, le chiffrement AES est activé par défaut. Si vous ne souhaitez pas que le serveur SMB sélectionne les types de cryptage AES pour les communications basées sur Kerberos avec le KDC Active Directory (AD), vous pouvez désactiver le cryptage AES.

Le fait que le cryptage AES soit activé par défaut et que vous puissiez spécifier des types de cryptage dépend de votre version de ONTAP.

Version ONTAP	Le cryptage AES est activé ...	Vous pouvez spécifier des types de cryptage ?
9.13.1 et versions ultérieures	Par défaut	Oui.
9.12.1	Manuellement	Oui.
9.11.1 et versions antérieures	Manuellement	Non

Depuis ONTAP 9.12.1, le chiffrement AES est activé et désactivé à l'aide du `-advertised-enc-types`. Cette option permet de spécifier les types de cryptage annoncés dans AD KDC. Le paramètre par défaut est `rc4` et `des`. Mais lorsqu'un type AES est spécifié, le cryptage AES est activé. Vous pouvez également utiliser l'option pour désactiver explicitement les types de cryptage RC4 et DES les plus faibles. Dans ONTAP 9.11.1 et les versions antérieures, vous devez utiliser le `-is-aes-encryption-enabled`. Option permettant d'activer et de désactiver le cryptage AES, et les types de cryptage ne peuvent pas être spécifiés.

Pour renforcer la sécurité, la machine virtuelle de stockage (SVM) modifie le mot de passe de son compte machine dans l'AD à chaque modification de l'option de sécurité AES. La modification du mot de passe peut nécessiter des informations d'identification AD administratives pour l'unité organisationnelle qui contient le compte de la machine.

Si un SVM est configuré en tant que destination de reprise sur incident où l'identité n'est pas conservée (le

-identity-preserve l'option est définie sur `false` Dans la configuration SnapMirror), les paramètres de sécurité du serveur SMB non par défaut ne sont pas répliqués sur la destination. Si vous avez activé le chiffrement AES sur la SVM source, vous devez l'activer manuellement.

## Exemple 1. Étapes

### ONTAP 9.12.1 et versions ultérieures

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que les types de cryptage AES soient utilisés pour les communications Kerberos...	Entrez la commande...
Activé	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256</pre>
Désactivé	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4</pre>

**Remarque :** le `-is-aes-encryption-enabled` Cette option est obsolète dans ONTAP 9.12.1 et peut être supprimée dans une version ultérieure.

2. Vérifiez que le chiffrement AES est activé ou désactivé selon les besoins :

```
vserver cifs
security show -vserver vserver_name -fields advertised-enc-types
```

### Exemples

L'exemple suivant active les types de chiffrement AES pour le serveur SMB sur SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-----
vs1      aes-128,aes-256
```

L'exemple suivant active les types de cryptage AES pour le serveur SMB sur le SVM vs2.

L'administrateur est invité à saisir les informations d'identification AD d'administration pour l'UO contenant le serveur SMB.

```
cluster1::> vsriver cifs security modify -vsriver vs2 -advertised-enc
-types aes-128,aes-256
```

Info: In order to enable SMB AES encryption, the password for the SMB server machine account must be reset. Enter the username and password for the SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

```
cluster1::> vsriver cifs security show -vsriver vs2 -fields advertised-
enc-types
```

```
vsriver  advertised-enc-types
-----  -----
vs2      aes-128,aes-256
```

## ONTAP 9.11.1 et versions antérieures

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que les types de cryptage AES soient utilisés pour les communications Kerberos...	Entrez la commande...
Activé	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled true</pre>
Désactivé	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled false</pre>

2. Vérifiez que le chiffrement AES est activé ou désactivé selon les besoins :

```
vsriver cifs
security show -vsriver vsriver_name -fields is-aes-encryption-enabled
```

Le `is-aes-encryption-enabled` s'affiche `true` Si le cryptage AES est activé et `false` s'il est désactivé.

## Exemples

L'exemple suivant active les types de chiffrement AES pour le serveur SMB sur SVM vs1 :

```
cluster1::> vsserver cifs security modify -vsserver vs1 -is-aes
-encryption-enabled true

cluster1::> vsserver cifs security show -vsserver vs1 -fields is-aes-
encryption-enabled

vsserver  is-aes-encryption-enabled
-----
vs1       true
```

L'exemple suivant active les types de cryptage AES pour le serveur SMB sur le SVM vs2.  
L'administrateur est invité à saisir les informations d'identification AD d'administration pour l'UO contenant le serveur SMB.

```
cluster1::> vsserver cifs security modify -vsserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vsserver cifs security show -vsserver vs2 -fields is-aes-
encryption-enabled

vsserver  is-aes-encryption-enabled
-----
vs2       true
```

#### Informations associées

"L'utilisateur du domaine ne parvient pas à se connecter au cluster avec Domain-tunnel"

## Utilisez la signature SMB pour améliorer la sécurité du réseau

### Utilisez la signature SMB pour améliorer la présentation de la sécurité réseau

La signature SMB contribue à garantir que le trafic réseau entre le serveur SMB et le client n'est pas compromis. Elle empêche les attaques de relecture. Par défaut, ONTAP

prend en charge la signature SMB sur demande du client. L'administrateur du stockage peut éventuellement configurer le serveur SMB afin de nécessiter une signature SMB.


**Comment les stratégies de signature SMB affectent la communication avec un serveur CIFS**

Outre les paramètres de sécurité de signature SMB du serveur CIFS, deux stratégies de signature SMB sur les clients Windows contrôlent la signature numérique des communications entre les clients et le serveur CIFS. Vous pouvez configurer le paramètre qui répond aux besoins de votre entreprise.

Les stratégies SMB du client sont contrôlées via les paramètres de stratégie de sécurité locale de Windows, qui sont configurés à l'aide des stratégies de groupe MMC (Microsoft Management Console) ou Active Directory. Pour plus d'informations sur les problèmes de sécurité et de signature SMB du client, consultez la documentation Microsoft Windows.

Voici les descriptions des deux stratégies de signature SMB sur les clients Microsoft :

- `Microsoft network client: Digitally sign communications (if server agrees)`  
  
Ce paramètre détermine si la fonctionnalité de signature SMB du client est activée. Elle est activée par défaut. Lorsque ce paramètre est désactivé sur le client, les communications client avec le serveur CIFS dépendent du paramètre de signature SMB sur le serveur CIFS.
- `Microsoft network client: Digitally sign communications (always)`  
  
Ce paramètre détermine si le client requiert la signature SMB pour communiquer avec un serveur. Elle est désactivée par défaut. Lorsque ce paramètre est désactivé sur le client, le comportement de signature SMB est basé sur le paramètre de stratégie pour `Microsoft network client: Digitally sign communications (if server agrees)` Et le paramètre sur le serveur CIFS.



Si votre environnement inclut des clients Windows configurés pour exiger une signature SMB, vous devez activer la signature SMB sur le serveur CIFS. Dans le cas contraire, le serveur CIFS ne peut pas transmettre de données à ces systèmes.

Les résultats effectifs des paramètres de signature SMB du client et du serveur CIFS dépendent du fait que les sessions SMB utilisent SMB 1.0 ou SMB 2.x et versions ultérieures.

Le tableau suivant récapitule le comportement de signature SMB efficace si la session utilise SMB 1.0 :

Client	Signature ONTAP : non requise	Signature ONTAP requise
Signature désactivée et non requise	Non signé	Signé
Signature activée et non requise	Non signé	Signé
Signature désactivée et requise	Signé	Signé
Signature activée et requise	Signé	Signé



Les anciens clients Windows SMB 1 et certains clients non Windows SMB 1 peuvent ne pas se connecter si la signature est désactivée sur le client mais requise sur le serveur CIFS.

Le tableau suivant récapitule le comportement de signature SMB efficace si la session utilise SMB 2.x ou SMB 3.0 :



Pour les clients SMB 2.x et SMB 3.0, la signature SMB est toujours activée. Elle ne peut pas être désactivée.

Client	Signature ONTAP : non requise	Signature ONTAP requise
Signature non requise	Non signé	Signé
Signature requise	Signé	Signé

Le tableau suivant récapitule le comportement de signature SMB du serveur et du client Microsoft par défaut :

Protocole	Algorithme de hachage	Peut activer/désactiver	Peut exiger/non requis	Client par défaut	Serveur par défaut	DC par défaut
SMB 1.0	MD5	Oui.	Oui.	Activé (non requis)	Désactivé (non requis)	Obligatoire
SMB 2.x	HMAC SHA-256	Non	Oui.	Non requis	Non requis	Obligatoire
SMB 3.0	AES-CMAC.	Non	Oui.	Non requis	Non requis	Obligatoire



Microsoft ne recommande plus d'utiliser Digitally sign communications (if client agrees) ou Digitally sign communications (if server agrees) Paramètres de stratégie de groupe. Microsoft ne recommande plus par ailleurs l'utilisation du EnableSecuritySignature paramètres du registre. Ces options n'affectent que le comportement du SMB 1 et peuvent être remplacées par le Digitally sign communications (always) Stratégie de groupe ou RequireSecuritySignature paramètre de registre. Vous pouvez également obtenir plus d'informations sur le blog Microsoft.principes de base de la signature SMB [The \(SMB1 et SMB2\)](#)

## Impact de la signature SMB sur les performances

Lorsque les sessions SMB utilisent la signature SMB, toutes les communications SMB vers et depuis les clients Windows subissent un impact sur les performances, ce qui affecte à la fois les clients et le serveur (c'est-à-dire les nœuds sur le cluster exécutant le SVM contenant le serveur SMB).

L'impact sur les performances indique que l'utilisation accrue du CPU sur les clients et le serveur est augmentée, même si le volume du trafic réseau ne change pas.

La mesure de l'impact sur les performances dépend de la version de ONTAP 9 que vous utilisez. Depuis



ONTAP 9.7, un nouvel algorithme de déchargement du cryptage peut permettre d'améliorer les performances du trafic SMB signé. L'allègement de la charge des signatures SMB est activé par défaut lorsque la signature SMB est activée.

L'amélioration des performances de signature SMB requiert une fonctionnalité de déchargement AES-ni. Consultez le Hardware Universe (HWU) pour vérifier que le déchargement AES-ni est pris en charge par votre plate-forme.

D'autres améliorations des performances sont également possibles si vous pouvez utiliser SMB version 3.11 qui prend en charge l'algorithme GCM beaucoup plus rapide.

Selon votre réseau, la version ONTAP 9, la version SMB et l'implémentation SVM, l'impact de la signature SMB sur les performances peut varier fortement. Vous pouvez la vérifier uniquement par le biais de tests dans l'environnement réseau.

La plupart des clients Windows négocient la signature SMB par défaut si elle est activée sur le serveur. Si vous avez besoin d'une protection SMB pour certains de vos clients Windows et si le SMB Signing génère des problèmes de performances, vous pouvez désactiver la signature SMB sur l'un de vos clients Windows ne nécessitant pas de protection contre les attaques de rejeu. Pour plus d'informations sur la désactivation de la signature SMB sur les clients Windows, consultez la documentation Microsoft Windows.

## Recommandations pour la configuration de la signature SMB

Vous pouvez configurer le comportement de signature SMB entre les clients SMB et le serveur CIFS pour répondre à vos exigences de sécurité. Les paramètres que vous choisissez lors de la configuration de la signature SMB sur votre serveur CIFS dépendent de vos exigences de sécurité.

Vous pouvez configurer la signature SMB sur le client ou sur le serveur CIFS. Tenez compte des recommandations suivantes lors de la configuration de la signature SMB :

Si...	Recommandation...
Vous souhaitez augmenter la sécurité de la communication entre le client et le serveur	Assurez-vous que le SMB Signing est requis au niveau du client en activant le <code>Require Option (Sign always)</code> paramètre de sécurité sur le client.
Vous souhaitez que tous les trafics SMB vers une certaine machine virtuelle de stockage (SVM) signée	Configurez les paramètres de sécurité pour exiger la signature SMB sur le serveur CIFS.

Pour plus d'informations sur la configuration des paramètres de sécurité du client Windows, reportez-vous à la documentation Microsoft.

## Consignes de signature SMB lorsque plusieurs LIF de données sont configurées

Si vous activez ou désactivez le SMB Signing requis sur le serveur SMB, vous devez connaître les instructions relatives aux configurations de plusieurs LIF de données pour un SVM.

Lorsque vous configurez un serveur SMB, plusieurs LIF de données peuvent être configurées. Si c'est le cas, le serveur DNS contient plusieurs A Entrées d'enregistrement pour le serveur CIFS, toutes utilisant le même

nom d'hôte de serveur SMB, mais chacune avec une adresse IP unique. Par exemple, un serveur SMB dont deux LIF de données sont configurées peut avoir le DNS suivant A entrées d'enregistrement :

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

Le comportement normal est qu'après modification du paramètre de signature SMB requis, seules les nouvelles connexions des clients sont affectées par la modification du paramètre de signature SMB. Cependant, il y a une exception à ce comportement. Il existe un cas où un client dispose d'une connexion existante à un partage, et le client crée une nouvelle connexion au même partage après la modification du paramètre, tout en maintenant la connexion d'origine. Dans ce cas, la connexion SMB, nouvelle et existante, adopte les nouvelles exigences de signature SMB.

Prenons l'exemple suivant :

1. Client1 se connecte à un partage sans avoir à signer SMB à l'aide du chemin `O:\`.
2. L'administrateur du stockage modifie la configuration du serveur SMB afin de exiger la signature SMB.
3. Client1 se connecte au même partage avec la signature SMB requise à l'aide du chemin `S:\` (tout en maintenant la connexion à l'aide du chemin `O:\`).
4. Par conséquent, le SMB Signing est utilisé pour accéder aux données sur le système `O:\` et `S:\` disques.

## Activer ou désactiver la signature SMB requise pour le trafic SMB entrant

Vous pouvez imposer aux clients l'exigence de signer les messages SMB en activant la signature SMB requise. S'il est activé, ONTAP n'accepte que les messages SMB s'ils ont une signature valide. Si vous souhaitez autoriser la signature SMB, mais pas l'exiger, vous pouvez désactiver la signature SMB requise.

### Description de la tâche

Par défaut, le SMB Signing requis est désactivé. Vous pouvez activer ou désactiver la signature SMB requise à tout moment.

La signature SMB n'est pas désactivée par défaut dans les cas suivants :



1. Le signature SMB requis est activé et le cluster est rétabli sur une version d'ONTAP qui ne prend pas en charge la signature SMB.
2. Le cluster est ensuite mis à niveau vers une version de ONTAP qui prend en charge la signature SMB.

Dans ce cas, la configuration de signature SMB qui a été configurée à l'origine sur une version prise en charge de ONTAP est conservée par le biais d'une nouvelle version et d'une mise à niveau ultérieure.

Lorsque vous configurez une relation de reprise d'activité de machine virtuelle de stockage (SVM), la valeur que vous sélectionnez pour le système `-identity-preserve` de la `snapmirror create` La commande détermine les détails de configuration répliqués dans le SVM de destination.

Si vous définissez le `-identity-preserve` option à `true` (ID-preserve), le paramètre de sécurité de

signature SMB est répliqué sur la destination.

Si vous définissez le `-identity-preserve` option à `false` (Non-ID-preserve), le paramètre de sécurité de signature SMB n'est pas répliqué sur la destination. Dans ce cas, les paramètres de sécurité du serveur CIFS sur la destination sont définis sur les valeurs par défaut. Si vous avez activé la signature SMB requise sur le SVM source, vous devez activer manuellement le SMB Signing requis sur le SVM de destination.

### Étapes

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que le SMB soit connecté...	Entrez la commande...
Activé	<code>vserver cifs security modify -vserver vserver_name -is-signing-required true</code>
Désactivé	<code>vserver cifs security modify -vserver vserver_name -is-signing-required false</code>

2. Vérifiez que la signature SMB requise est activée ou désactivée en déterminant si la valeur dans l' `Is Signing Required` le champ de la sortie de la commande suivante est défini sur la valeur souhaitée :  
`vserver cifs security show -vserver vserver_name -fields is-signing-required`

### Exemple

L'exemple suivant active la signature SMB requise pour le SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-required
vserver  is-signing-required
-----  -
vs1      true
```



Les modifications apportées aux paramètres de cryptage prennent effet pour les nouvelles connexions. Les connexions existantes ne sont pas affectées.

## Déterminez si les sessions SMB sont signées

Vous pouvez afficher des informations sur les sessions SMB connectées sur le serveur CIFS. Vous pouvez utiliser ces informations pour déterminer si les sessions SMB sont signées. Cela peut être utile pour déterminer si les sessions client SMB se connectent aux paramètres de sécurité souhaités.

### Étapes

1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher des informations sur...	Entrez la commande...
Toutes les sessions signées sur une machine virtuelle de stockage (SVM) spécifiée	<code>vserver cifs session show -vserver <i>vserver_name</i> -is-session-signed true</code>
Détails d'une session signée avec un ID de session spécifique sur le SVM	<code>vserver cifs session show -vserver <i>vserver_name</i> -session-id integer -instance</code>

## Exemples

La commande suivante affiche les informations relatives aux sessions signées sur le SVM vs1. La sortie de résumé par défaut n'affiche pas le champ de sortie « session signée is » :

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:      node1
Vserver:   vs1
Connection Session
ID          ID      Workstation      Windows User      Open      Idle
-----
3151272279  1        10.1.1.1        DOMAIN\joe        2         23s
```

La commande suivante affiche des informations détaillées sur la session, notamment si elle est signée, dans une session SMB avec l'ID de session 2 :

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

## Informations associées

[Contrôle des statistiques de session signées SMB](#)

## Surveiller les statistiques de session signées SMB

Vous pouvez surveiller les statistiques des sessions SMB et déterminer les sessions établies qui sont signées et qui ne le sont pas.

### Description de la tâche

Le `statistics` la commande au niveau de privilège avancé fournit le `signed_sessions` Compteur que vous pouvez utiliser pour surveiller le nombre de sessions SMB signées. Le `signed_sessions` le compteur est disponible avec les objets de statistiques suivants :

- `cifs` Permet de surveiller la signature SMB pour toutes les sessions SMB.
- `smb1` Permet de surveiller la signature SMB pour les sessions SMB 1.0.
- `smb2` Permet de surveiller la signature SMB pour les sessions SMB 2.x et SMB 3.0.

Les statistiques SMB 3.0 sont incluses dans les résultats de `smb2` objet.

Si vous souhaitez comparer le nombre de sessions signées au nombre total de sessions, vous pouvez comparer les résultats de la session `signed_sessions` compteur avec la sortie pour le `established_sessions` compteur.

Vous devez démarrer une collecte d'échantillons de statistiques avant de pouvoir afficher les données

résultantes. Vous pouvez afficher les données de l'échantillon si vous n'arrêtez pas la collecte de données. L'arrêt de la collecte de données vous donne un échantillon fixe. L'option ne pas arrêter la collecte de données vous permet d'obtenir des données mises à jour que vous pouvez utiliser pour comparer à des requêtes précédentes. La comparaison vous aide à identifier les tendances.

Étapes

- 1. Définissez le niveau de privilège sur avancé :  
`set -privilege advanced`
- 2. Démarrer une collecte de données :  
`statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

Si vous ne spécifiez pas le `-sample-id` Paramètre, la commande génère un exemple d'identificateur pour vous et définit cet échantillon comme échantillon par défaut pour la session de l'interface de ligne de commande. La valeur pour `-sample-id` est une chaîne de texte. Si vous exécutez cette commande pendant la même session CLI et ne spécifiez pas le `-sample-id` paramètre, la commande remplace l'échantillon par défaut précédent.

Vous pouvez spécifier le nœud sur lequel vous souhaitez collecter les statistiques. Si vous ne spécifiez pas le nœud, l'exemple collecte les statistiques de tous les nœuds du cluster.

- 3. Utilisez le `statistics stop` commande pour arrêter la collecte des données de l'échantillon.
- 4. Afficher les statistiques de signature SMB :

Si vous souhaitez afficher les informations pour...	Entrer...
Sessions signées	<code>`show -sample-id sample_ID -counter signed_sessions</code>
<code>node_name [-node node_name]</code>	Sessions signées et sessions établies
<code>`show -sample-id sample_ID -counter signed_sessions</code>	<code>established_sessions</code>

Si vous souhaitez afficher les informations pour un seul nœud, spécifiez l'option `-node` paramètre.

- 5. Revenir au niveau de privilège admin :  
`set -privilege admin`

## Exemples

L'exemple suivant montre comment surveiller les statistiques de signature SMB 2.x et SMB 3.0 sur la machine virtuelle de stockage (SVM) vs1.

La commande suivante permet d'accéder au niveau de privilège avancé :

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

La commande suivante démarre la collecte de données pour un nouvel échantillon :

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample  
-vserver vs1
```

```
Statistics collection is being started for Sample-id: smbsigning_sample
```

La commande suivante arrête la collecte des données de l'échantillon :

```
cluster1::*> statistics stop -sample-id smbsigning_sample
```

```
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

La commande suivante affiche les sessions SMB signées et les sessions SMB établies par nœud à partir de l'exemple :

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|established_sessions|node_name
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:03:04

Cluster: cluster1

Counter	Value
-----	-----
established_sessions	0
node_name	node1
signed_sessions	0
established_sessions	1
node_name	node2
signed_sessions	1
established_sessions	0
node_name	node3
signed_sessions	0
established_sessions	0
node_name	node4
signed_sessions	0

La commande suivante affiche les sessions SMB signées pour le nœud 2 à partir de l'exemple :

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|node_name -node node2
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:22:43

Cluster: cluster1

Counter	Value
-----	-----
node_name	node2
signed_sessions	1

La commande suivante revient au niveau de privilège admin :

```
cluster1::*> set -privilege admin
```



## Configurez le chiffrement SMB requis sur les serveurs SMB pour les transferts de données via SMB

### Présentation du chiffrement SMB

Le chiffrement SMB pour les transferts de données via SMB est une amélioration de sécurité que vous pouvez activer ou désactiver sur les serveurs SMB. Vous pouvez également configurer le paramètre de chiffrement SMB souhaité sur une base partage par partage à l'aide d'un paramètre de propriété de partage.

Par défaut, lorsque vous créez un serveur SMB sur la machine virtuelle de stockage (SVM), le chiffrement SMB est désactivé. Vous devez leur permettre de bénéficier de la sécurité améliorée fournie par le chiffrement SMB.

Pour créer une session SMB chiffrée, le client SMB doit prendre en charge le chiffrement SMB. Les clients Windows commençant par Windows Server 2012 et Windows 8 prennent en charge le cryptage SMB.

Le chiffrement SMB sur la SVM est contrôlé par deux paramètres :

- Option de sécurité du serveur SMB qui active la fonctionnalité sur le SVM
- Propriété de partage SMB qui configure le paramètre de chiffrement SMB partage par partage

Vous pouvez décider s'il faut un chiffrement pour accéder à toutes les données de la SVM ou bien demander un chiffrement SMB pour accéder aux données uniquement dans les partages sélectionnés. Les paramètres des SVM prévalent sur les paramètres de niveau partage.

La configuration de cryptage SMB efficace dépend de la combinaison des deux paramètres. Elle est décrite dans le tableau suivant :

Chiffrement SMB du serveur SMB activé	Le paramètre partage des données de chiffrement est activé	Comportement de cryptage côté serveur
Vrai	Faux	Le chiffrement au niveau du serveur est activé pour tous les partages du SVM. Avec cette configuration, le chiffrement s'effectue pour toute la session SMB.

Chiffrement SMB du serveur SMB activé	Le paramètre partage des données de chiffrement est activé	Comportement de cryptage côté serveur
Vrai	Vrai	Le chiffrement au niveau du serveur est activé pour tous les partages de la SVM indépendamment du chiffrement au niveau du partage. Avec cette configuration, le chiffrement s'effectue pour toute la session SMB.
Faux	Vrai	Le chiffrement au niveau du partage est activé pour les partages spécifiques. Avec cette configuration, le chiffrement se produit à partir de l'arborescence à connecter.
Faux	Faux	Aucun chiffrement n'est activé.

Les clients SMB qui ne prennent pas en charge le chiffrement ne peuvent pas se connecter à un serveur SMB ou à un partage qui nécessite un chiffrement.

Les modifications apportées aux paramètres de cryptage prennent effet pour les nouvelles connexions. Les connexions existantes ne sont pas affectées.

## Impact du chiffrement SMB sur les performances

Lorsque les sessions SMB utilisent le chiffrement SMB, toutes les communications SMB vers et depuis les clients Windows rencontrent un impact sur les performances, qui affecte à la fois les clients et le serveur (c'est-à-dire les nœuds sur le cluster exécutant le SVM qui contient le serveur SMB).

L'impact sur les performances indique que l'utilisation accrue du CPU sur les clients et le serveur est augmentée, même si le volume du trafic réseau ne change pas.

La mesure de l'impact sur les performances dépend de la version de ONTAP 9 que vous utilisez. Depuis ONTAP 9.7, un nouvel algorithme de désactivation du chiffrement permet d'améliorer les performances du trafic SMB chiffré. Le délestage du chiffrement SMB est activé par défaut lorsque le chiffrement SMB est activé.

L'optimisation des performances de chiffrement SMB requiert une fonctionnalité de déchargement AES-ni. Consultez le Hardware Universe (HWU) pour vérifier que le déchargement AES-ni est pris en charge par votre plate-forme.

D'autres améliorations des performances sont également possibles si vous pouvez utiliser SMB version 3.11 qui prend en charge l'algorithme GCM beaucoup plus rapide.

Selon votre réseau, la version ONTAP 9, la version SMB et l'implémentation SVM, l'impact du cryptage SMB sur les performances peut varier fortement. Vous pouvez le vérifier uniquement par le biais de tests dans

l'environnement réseau.

Le chiffrement SMB est désactivé par défaut sur le serveur SMB. Vous devez activer le chiffrement SMB uniquement sur les partages SMB ou les serveurs SMB qui nécessitent un chiffrement. Avec le cryptage SMB, ONTAP effectue un traitement supplémentaire du décryptage des demandes et du cryptage des réponses à chaque demande. Le chiffrement SMB ne doit donc être activé que lorsque cela est nécessaire.

## Activez ou désactivez le chiffrement SMB requis pour le trafic SMB entrant

Si vous souhaitez exiger le cryptage SMB pour le trafic SMB entrant, vous pouvez l'activer sur le serveur CIFS ou au niveau du partage. Par défaut, le chiffrement SMB n'est pas requis.

### Description de la tâche

Vous pouvez activer le chiffrement SMB sur le serveur CIFS, qui s'applique à tous les partages du serveur CIFS. Si vous ne souhaitez pas utiliser le cryptage SMB requis pour tous les partages du serveur CIFS ou si vous souhaitez activer le cryptage SMB requis pour le trafic SMB entrant, partage par partage, vous pouvez désactiver le cryptage SMB requis sur le serveur CIFS.

Lorsque vous configurez une relation de reprise d'activité de machine virtuelle de stockage (SVM), la valeur que vous sélectionnez pour le système `-identity-preserve` de la `snapmirror create` La commande détermine les détails de configuration répliqués dans le SVM de destination.

Si vous définissez le `-identity-preserve` option à `true` (ID-preserve), le paramètre de sécurité du cryptage SMB est répliqué sur la destination.

Si vous définissez le `-identity-preserve` option à `false` (Non ID-preserve), le paramètre de sécurité du cryptage SMB n'est pas répliqué sur la destination. Dans ce cas, les paramètres de sécurité du serveur CIFS sur la destination sont définis sur les valeurs par défaut. Si vous avez activé le chiffrement SMB sur le SVM source, vous devez activer manuellement le chiffrement SMB du serveur CIFS sur la destination.

### Étapes

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que le chiffrement SMB soit requis pour le trafic SMB entrant sur le serveur CIFS...	Entrez la commande...
Activé	<pre>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true</pre>
Désactivé	<pre>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false</pre>

2. Vérifiez que le chiffrement SMB requis sur le serveur CIFS est activé ou désactivé, selon les besoins :  

```
vserver cifs security show -vserver vserver_name -fields is-smb-encryption-  
required
```

Le `is-smb-encryption-required` s'affiche `true` Le cas échéant, le cryptage SMB est activé sur le

serveur CIFS et false s'il est désactivé.

### Exemple

L'exemple suivant permet le cryptage SMB requis pour le trafic SMB entrant pour le serveur CIFS sur le SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-----
vs1      true
```

## Déterminez si les clients sont connectés à l'aide de sessions SMB cryptées

Vous pouvez afficher des informations sur les sessions SMB connectées pour déterminer si les clients utilisent des connexions SMB chiffrées. Cela peut être utile pour déterminer si les sessions client SMB se connectent aux paramètres de sécurité souhaités.

### Description de la tâche

Les sessions client SMB peuvent avoir l'un des trois niveaux de chiffrement suivants :

- unencrypted

La session SMB n'est pas chiffrée. Ni le chiffrement au niveau des serveurs virtuels de stockage ou du partage n'est configuré.

- partially-encrypted

Le chiffrement est lancé lorsque l'arborescence se connecte. Le chiffrement au niveau du partage est configuré. Le chiffrement au niveau des SVM n'est pas activé.

- encrypted

La session SMB est entièrement chiffrée. Le chiffrement au niveau des SVM est activé. Le chiffrement au niveau du partage peut être activé ou non. Le paramètre de cryptage au niveau SVM remplace le paramètre de cryptage au niveau du partage.

### Étapes

1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher des informations sur...	Entrez la commande...
Sessions avec un paramètre de chiffrement spécifié pour les sessions sur un SVM spécifié	`vserver cifs session show -vserver vserver_name {unencrypted

Si vous voulez afficher des informations sur...	Entrez la commande...
partially-encrypted	encrypted} -instance`
Paramètre de chiffrement pour un ID de session spécifique sur un SVM spécifié	<code>vserver cifs session show -vserver <i>vserver_name</i> -session-id <i>integer</i> -instance</code>

## Exemples

La commande suivante affiche des informations détaillées sur la session, y compris le paramètre de chiffrement, sur une session SMB avec l'ID de session 2 :

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

## Contrôle des statistiques de chiffrement SMB

Vous pouvez surveiller les statistiques de cryptage SMB et déterminer les sessions établies et les connexions de partage qui sont cryptées et qui ne le sont pas.

### Description de la tâche

Le `statistics` Le niveau de privilège avancé fournit les compteurs suivants, que vous pouvez utiliser pour surveiller le nombre de sessions SMB chiffrées et de connexions pour le partage :

Nom du compteur	Descriptions
<code>encrypted_sessions</code>	Indique le nombre de sessions SMB 3.0 cryptées
<code>encrypted_share_connections</code>	Indique le nombre de partages cryptés sur lesquels une arborescence s'est connectée
<code>rejected_unencrypted_sessions</code>	Indique le nombre de configurations de session rejetées en raison d'un manque de capacité de chiffrement du client
<code>rejected_unencrypted_shares</code>	Indique le nombre de mappages de partage rejetés en raison d'un manque de capacité de chiffrement du client

Ces compteurs sont disponibles avec les objets de statistiques suivants :

- `cifs` Permet de surveiller le chiffrement SMB pour toutes les sessions SMB 3.0.

Les statistiques SMB 3.0 sont incluses dans les résultats de `cifs` objet. Si vous souhaitez comparer le nombre de sessions chiffrées au nombre total de sessions, vous pouvez comparer les résultats de l'`encrypted_sessions` compteur avec la sortie pour le `established_sessions` compteur.

Si vous souhaitez comparer le nombre de connexions de partage chiffrées au nombre total de connexions de partage, vous pouvez comparer la sortie du `encrypted_share_connections` compteur avec la sortie pour le `connected_shares` compteur.

- `rejected_unencrypted_sessions` Indique le nombre de tentatives d'établissement d'une session SMB nécessitant un chiffrement d'un client qui ne prend pas en charge le chiffrement SMB.
- `rejected_unencrypted_shares` Indique combien de fois une tentative de connexion à un partage SMB nécessite un chiffrement d'un client ne prenant pas en charge le chiffrement SMB.

Vous devez démarrer une collecte d'échantillons de statistiques avant de pouvoir afficher les données résultantes. Vous pouvez afficher les données de l'échantillon si vous n'arrêtez pas la collecte de données. L'arrêt de la collecte de données vous donne un échantillon fixe. L'option ne pas arrêter la collecte de données vous permet d'obtenir des données mises à jour que vous pouvez utiliser pour comparer à des requêtes précédentes. La comparaison vous aide à identifier les tendances.

## Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Démarrer une collecte de données :

```
statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]
```

Si vous ne spécifiez pas le `-sample-id` Paramètre, la commande génère un exemple d'identificateur pour vous et définit cet échantillon comme échantillon par défaut pour la session de l'interface de ligne de commande. La valeur pour `-sample-id` est une chaîne de texte. Si vous exécutez cette commande pendant la même session CLI et ne spécifiez pas le `-sample-id` paramètre, la commande remplace l'échantillon par défaut précédent.

Vous pouvez spécifier le nœud sur lequel vous souhaitez collecter les statistiques. Si vous ne spécifiez pas le nœud, l'exemple collecte les statistiques de tous les nœuds du cluster.

3. Utilisez le `statistics stop` commande pour arrêter la collecte des données de l'échantillon.
4. Afficher les statistiques de chiffrement SMB :

Si vous souhaitez afficher les informations pour...	Entrer...
Sessions chiffrées	<code>`show -sample-id <i>sample_ID</i> -counter encrypted_sessions</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	Sessions chiffrées et sessions établies
<code>`show -sample-id <i>sample_ID</i> -counter encrypted_sessions</code>	<code>established_sessions</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	Connexions de partage cryptées
<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>
Connexions de partage cryptées et partages connectés	<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections</code>
<code>connected_shares</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>
Sessions non chiffrées rejetées rejetées	<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_sessions</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	Les connexions de partage non chiffrées ont été rejetées
<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_share</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>

Si vous souhaitez afficher les informations uniquement pour un seul nœud, spécifiez l'option `-node` paramètre.

5. Revenir au niveau de privilège admin :  
`set -privilege admin`

## Exemples

L'exemple suivant montre comment surveiller les statistiques de cryptage SMB 3.0 sur la machine virtuelle de stockage (SVM) vs1.

La commande suivante permet d'accéder au niveau de privilège avancé :

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

La commande suivante démarre la collecte de données pour un nouvel échantillon :

```
cluster1::*> statistics start -object cifs -sample-id  
smbencryption_sample -vserver vs1  
Statistics collection is being started for Sample-id:  
smbencryption_sample
```

La commande suivante arrête la collecte des données pour cet échantillon :

```
cluster1::*> statistics stop -sample-id smbencryption_sample  
Statistics collection is being stopped for Sample-id:  
smbencryption_sample
```

La commande suivante affiche les sessions SMB chiffrées et les sessions SMB établies par le nœud à partir de l'exemple :



```
cluster2::*> statistics show -object cifs -counter  
established_sessions|encrypted_sessions|node_name -node node_name
```

Object: cifs

Instance: [proto\_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:45

Scope: vsim2

Counter	Value
established_sessions	1
encrypted_sessions	1

2 entries were displayed

La commande suivante affiche le nombre de sessions SMB non chiffrées rejetées par le nœud à partir de l'exemple :

```
clus-2::*> statistics show -object cifs -counter  
rejected_unencrypted_sessions -node node_name
```

Object: cifs

Instance: [proto\_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:51

Scope: vsim2

Counter	Value
rejected_unencrypted_sessions	1

1 entry was displayed.

La commande suivante indique le nombre de partages SMB connectés et de partages SMB chiffrés par le nœud à partir de l'exemple :

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name
```

Object: cifs  
Instance: [proto\_ctx:003]  
Start-time: 4/12/2016 10:41:38  
End-time: 4/12/2016 10:41:43  
Scope: vsim2

Counter	Value
connected_shares	2
encrypted_share_connections	1

2 entries were displayed.

La commande suivante affiche le nombre de connexions de partage SMB non chiffrées rejetées par le nœud à partir de l'exemple :

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name
```

Object: cifs  
Instance: [proto\_ctx:003]  
Start-time: 4/12/2016 10:41:38  
End-time: 4/12/2016 10:42:06  
Scope: vsim2

Counter	Value
rejected_unencrypted_shares	1

1 entry was displayed.

## Informations associées

[Détermination des objets statistiques et des compteurs disponibles](#)

["Contrôle des performances et présentation de la gestion"](#)

# Communication de session LDAP sécurisée

## Concepts de signature et d'étanchéité LDAP

Depuis ONTAP 9, vous pouvez configurer la signature et le chiffrement pour activer la

sécurité des sessions LDAP sur les requêtes vers un serveur Active Directory (AD). Vous devez configurer les paramètres de sécurité du serveur CIFS sur la machine virtuelle de stockage (SVM) de sorte qu'ils correspondent à ceux du serveur LDAP.

La signature valide l'intégrité des données LDAP à l'aide d'une technologie à clé secrète. Le chiffrement crypte les données LDAP afin de ne pas transmettre de données sensibles en clair. Une option *LDAP Security Level* indique si le trafic LDAP doit être signé, signé et scellé, ou non. La valeur par défaut est `none`.

La signature et le chiffrement LDAP sur le trafic CIFS sont activés sur le SVM avec le `-session-security-for-ad-ldap` à la `vserver cifs security modify` commande.

## Activez le chiffrement et la signature LDAP sur le serveur CIFS

Avant que votre serveur CIFS puisse utiliser la signature et le chiffrement pour sécuriser la communication avec un serveur LDAP Active Directory, vous devez modifier les paramètres de sécurité du serveur CIFS pour activer la signature et le chiffrement LDAP.

### Avant de commencer

Vous devez consulter votre administrateur de serveur AD pour déterminer les valeurs de configuration de sécurité appropriées.

### Étapes

1. Configurez le paramètre de sécurité du serveur CIFS qui autorise le trafic signé et scellé avec les serveurs LDAP Active Directory : `vserver cifs security modify -vserver vserver_name -session-security-for-ad-ldap {none|sign|seal}`

Vous pouvez activer la signature (`sign`, intégrité des données), signature et scellage (`seal`, intégrité et chiffrement des données), ou ni l'un ni l'autre `none`, pas de signature ou d'étanchéité). La valeur par défaut est `none`.

2. Vérifiez que le paramètre de sécurité de signature et de chiffrement LDAP est défini correctement :

```
vserver cifs security show -vserver vserver_name
```



Si le SVM utilise le même serveur LDAP pour effectuer des requêtes name-mapping ou d'autres informations UNIX, comme les utilisateurs, les groupes et les netgroups, alors vous devez activer le paramètre correspondant avec le `-session-security` de la `vserver services name-service ldap client modify` commande.

## Configurer LDAP sur TLS

### Exporter une copie du certificat de l'autorité de certification racine auto-signé

Pour utiliser LDAP sur SSL/TLS pour sécuriser la communication Active Directory, vous devez d'abord exporter une copie du certificat d'autorité de certification racine auto-signé du service de certificats Active Directory en fichier de certificat et la convertir en fichier texte ASCII. Ce fichier texte est utilisé par ONTAP pour installer le certificat sur la machine virtuelle de stockage (SVM).

### Avant de commencer

Le service de certificat Active Directory doit déjà être installé et configuré pour le domaine auquel le serveur CIFS appartient. Vous trouverez des informations sur l'installation et la configuration des services de certificats Active Director en consultant la bibliothèque Microsoft TechNet.

["Bibliothèque Microsoft TechNet : technet.microsoft.com"](http://technet.microsoft.com)

### Étape

1. Obtenez un certificat d'autorité de certification racine du contrôleur de domaine qui se trouve dans le .pem format de texte.

["Bibliothèque Microsoft TechNet : technet.microsoft.com"](http://technet.microsoft.com)

### Une fois que vous avez terminé

Installer le certificat sur le SVM.

### Informations associées

["Bibliothèque Microsoft TechNet"](http://technet.microsoft.com)

### Installer le certificat d'autorité de certification racine auto-signé sur le SVM

Si l'authentification LDAP avec TLS est requise lorsqu'il s'agit de serveurs LDAP, vous devez d'abord installer le certificat AC racine auto-signé sur le SVM.

### Description de la tâche

Lorsque LDAP sur TLS est activé, le client LDAP ONTAP sur la SVM ne prend pas en charge les certificats révoqués dans ONTAP 9.0 et 9.1.

Depuis ONTAP 9.2, toutes les applications de ONTAP qui utilisent les communications TLS peuvent vérifier le statut du certificat numérique à l'aide du protocole OCSP (Online Certificate Status Protocol). Si OCSP est activé pour LDAP sur TLS, les certificats révoqués sont rejetés et la connexion échoue.

### Étapes

1. Installez le certificat d'autorité de certification racine auto-signé :
  - a. Commencez l'installation du certificat : `security certificate install -vserver vserver_name -type server-ca`  
  
La sortie de la console affiche le message suivant : `Please enter Certificate: Press <Enter> when done`
  - b. Ouvrez le certificat .pem fichier avec un éditeur de texte, copiez le certificat, y compris les lignes commençant par `-----BEGIN CERTIFICATE-----` et se terminant par `-----END CERTIFICATE-----`, puis collez le certificat après l'invite de commande.
  - c. Vérifiez que le certificat s'affiche correctement.
  - d. Terminez l'installation en appuyant sur entrée.
2. Vérifiez que le certificat est installé : `security certificate show -vserver vserver_name`

### Activez LDAP sur TLS sur le serveur

Avant que votre serveur SMB puisse utiliser TLS pour sécuriser les communications avec un serveur LDAP Active Directory, vous devez modifier les paramètres de sécurité du

## serveur SMB pour activer LDAP sur TLS.

Depuis ONTAP 9.10.1, la liaison des canaux LDAP est prise en charge par défaut pour les connexions LDAP Active Directory (AD) et services de noms. ONTAP essaiera la liaison des canaux avec les connexions LDAP uniquement si Start-TLS ou LDAPS est activé avec la sécurité de session définie sur Sign ou SEAL. Pour désactiver ou réactiver la liaison des canaux LDAP avec les serveurs AD, utilisez le `-try-channel-binding-for-ad-ldap` paramètre avec le `vserver cifs security modify` commande.

Pour en savoir plus, voir :

- ["Présentation LDAP"](#)
- ["2020 exigences de liaison des canaux LDAP et de signature LDAP pour Windows"](#).

### Étapes

1. Configurez le paramètre de sécurité du serveur SMB permettant une communication LDAP sécurisée avec les serveurs LDAP Active Directory : `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. Vérifiez que le paramètre de sécurité LDAP sur TLS est défini sur `true`: `vserver cifs security show -vserver vserver_name`



Si le SVM utilise le même serveur LDAP pour effectuer des requêtes name-mapping ou d'autres informations UNIX (par exemple, utilisateurs, groupes et netgroups), alors vous devez également modifier `-use-start-tls` à l'aide de `vserver services name-service ldap client modify` commande.

## Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

## Informations sur les marques commerciales

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