SMB 서버 보안 설정을 관리합니다

ONTAP 9

NetApp
September 12, 2024

목차

SMB 서버 보안 설정을 관리합니다

ONTAP가 SMB 클라이언트 인증을 처리하는 방법

사용자가 SVM에 포함된 데이터에 액세스하기 위해 SMB 연결을 생성하려면 먼저 SMB 서버가 속해 있는 도메인에서 인증을 받아야 합니다. SMB 서버는 Kerberos와 NTLM(NTLMv1 또는 NTLMv2)의 두 가지 인증 방법을 지원합니다. Kerberos는 도메인 사용자를 인증하는 데 사용되는 기본 방법입니다.

Kerberos 인증

ONTAP는 인증된 SMB 세션을 생성할 때 Kerberos 인증을 지원합니다.

Kerberos는 Active Directory의 기본 인증 서비스입니다. Kerberos 서버 또는 Kerberos KDC(Key Distribution Center) 서비스는 Active Directory에 보안 원칙에 대한 정보를 저장하고 검색합니다. NTLM 모델과 달리 SMB 서버와 같은 다른 컴퓨터와 세션을 설정하려는 Active Directory 클라이언트는 KDC에 직접 문의하여 세션 자격 증명을 얻습니다.

NTLM 인증

NTLM 클라이언트 인증은 암호를 기반으로 사용자별 비밀번호에 대한 공유 지식을 기반으로 하는 본인 확인 응답 프로토콜을 사용하여 수행됩니다.

사용자가 로컬 Windows 사용자 계정을 사용하여 SMB 연결을 만들면 NTLMv2를 사용하여 SMB 서버에서 로컬로 인증이 수행됩니다.

SVM 재해 복구 구성의 SMB 서버 보안 설정 지침

ID가 보존되지 않는 재해 복구 대상으로 구성된 SVM(SnapMirror 구성에서 '-identity-preserve' 옵션이 'false'로 설정됨)을 생성하기 전에 SVM 대상에서 SMB 서버 보안 설정이 관리되는 방식을 알아야 합니다.

- 기본이 아닌 SMB 서버 보안 설정은 대상에 복제되지 않습니다.

  대상 SVM에서 SMB 서버를 생성할 때 모든 SMB 서버 보안 설정이 기본값으로 설정됩니다. SVM 재해 복구 대상이 초기화, 업데이트 또는 재동기화되면 소스의 SMB 서버 보안 설정이 타겟으로 복제되지 않습니다.

- 기본이 아닌 SMB 서버 보안 설정을 수동으로 구성해야 합니다.

  소스 SVM에 기본값이 아닌 SMB 서버 보안 설정이 구성되어 있는 경우 SnapMirror 관계가 깨진 후, 대상이 읽기-쓰기 상태가 되면 대상 SVM에서 동일한 설정을 수동으로 구성해야 합니다.

SMB 서버 보안 설정에 대한 정보를 표시합니다

SMB 서버 보안 설정에 대한 정보를 SVM(스토리지 가상 머신)에 표시할 수 있습니다. 이 정보를 사용하여 보안 설정이 올바른지 확인할 수 있습니다.

이 작업에 대해

표시된 보안 설정은 해당 개체의 기본값이거나 ONTAP CLI를 사용하거나 Active Directory 그룹 정책 개체(GPO)를 사용하여 구성된 기본값이 아닌 값일 수 있습니다.

일부 옵션이 유효하지 않으므로 워크그룹 모드에서 SMB 서버에 대해 "vserver cifs security show" 명령을 사용하지 마십시오.

단계

1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 표시하려면...	명령 입력...
지정된 SVM의 모든 보안 설정	'vserver cifs security show -vserver_vserver_name_'
SVM의 특정 보안 설정 또는 설정	'vserver cifs security show -vserver_vserver_name_ - 필드 [fieldname,...]'를 입력하면 '-fields?'를 입력할 수 있습니다 사용할 수 있는 필드를 결정합니다.

예

다음 예는 SVM VS1 보안 설정을 모두 보여줍니다.

```
cluster1::> vserver cifs security show -vserver 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
```

표시되는 설정은 실행 중인 ONTAP 버전에 따라 다릅니다.

다음 예에서는 SVM VS1 Kerberos 클록 편중을 보여 줍니다.

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

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

관련 정보

GPO 구성에 대한 정보 표시

로컬 SMB 사용자에 대해 필요한 암호 복잡성을 설정하거나 해제합니다

필수 비밀번호 복잡성은 스토리지 가상 시스템(SVM)의 로컬 SMB 사용자를 위해 향상된 보안을 제공합니다. 필요한 암호 복잡성 기능은 기본적으로 활성화되어 있습니다. 이 기능을 사용하지 않도록 설정하고 언제든지 다시 사용하도록 설정할 수 있습니다.

시작하기 전에

CIFS 서버에서 로컬 사용자, 로컬 그룹 및 로컬 사용자 인증을 설정해야 합니다.

> 이 작업에 대해
>
> 일부 옵션이 유효하지 않으므로 워크그룹 모드에서 CIFS 서버에 대해 "vserver cifs security modify" 명령을 사용하면 안 됩니다.

단계

1. 다음 작업 중 하나를 수행합니다.

로컬 **SMB** 사용자에 대한 암호 복잡성에 필요한 경우...	명령 입력...
활성화됨	'vserver cifs security modify -vserver_vserver_name_-is-password-Complexity -required true'
사용 안 함	'vserver cifs security modify -vserver_vserver_name_-is-password-Complexity -required false'

2. 필요한 암호 복잡성에 대한 보안 설정을 확인합니다. 'vserver cifs security show -vserver_vserver_name_'

예

다음 예에서는 SVM VS1 용 로컬 SMB 사용자에 대해 필요한 암호 복잡성이 활성화된 것을 보여 줍니다.

```
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
```

관련 정보

CIFS 서버 보안 설정에 대한 정보를 표시합니다

로컬 사용자 및 그룹을 인증 및 인증에 사용합니다

로컬 사용자 암호 요구 사항

로컬 사용자 계정 암호 변경

CIFS 서버 Kerberos 보안 설정을 수정합니다

허용되는 최대 Kerberos 클록 비뚤어짐 시간, Kerberos 티켓 수명 및 티켓 갱신 최대 일 수를 비롯한 특정 CIFS 서버 Kerberos 보안 설정을 수정할 수 있습니다.

이 작업에 대해

'vserver cifs security modify' 명령을 사용하여 CIFS 서버 Kerberos 설정을 수정하면 '-vserver' 매개 변수로 지정한 단일 SVM(스토리지 가상 머신)에서만 설정이 수정됩니다. Active Directory 그룹 정책 개체(GPO)를 사용하여 동일한 Active Directory 도메인에 속한 클러스터의 모든 SVM에 대한 Kerberos 보안 설정을 중앙에서 관리할 수 있습니다.

단계

1. 다음 작업 중 하나 이상을 수행합니다.

원하는 작업	입력…
허용되는 최대 Kerberos 클럭 편중 시간을 분(9.13.1 이상) 또는 초(9.12.1 이하)로 지정합니다.	'vserver cifs security modify -vserver_vserver_name_-Kerberos-clock -suts_integer_in_minutes_' 기본 설정은 5분입니다.
Kerberos 티켓 수명(시간)을 지정합니다.	'vserver cifs security modify -vserver_vserver_name_-Kerberos-티켓-age integer_in_hours'를 선택합니다 기본 설정은 10시간입니다.

티켓 갱신 최대 일 수를 지정하십시오.	'vserver cifs security modify - vserver_vserver_name_ - Kerberos - renew - age_integer_in_days _' 기본 설정은 7일입니다.
모든 KDC가 도달할 수 없음으로 표시되는 KDC의 소켓에 대한 시간 제한을 지정합니다.	'vserver cifs security modify -vserver_vserver_name_-Kerberos-KDC -timeout_integer_in_seconds _' 기본 설정은 3초입니다.

2. Kerberos 보안 설정을 확인합니다.

   'vserver cifs security show -vserver_vserver_name_'

예

다음 예에서는 Kerberos 보안을 다음과 같이 변경합니다. ""Kerberos Clock Skew""는 3분으로 설정되고 ""Kerberos Ticket Age""는 SVM VS1 v1의 경우 8시간으로 설정됩니다.

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

cluster1::> vserver cifs security show -vserver 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
```

관련 정보

"CIFS 서버 보안 설정에 대한 정보를 표시합니다"

"지원되는 GPO"

"CIFS 서버에 그룹 정책 객체 적용"

SMB 서버 최소 인증 보안 수준을 설정합니다

SMB 클라이언트 액세스에 대한 비즈니스 보안 요구 사항을 충족하도록 SMB 서버에서 _LMCompatibilityLevel_이라고도 하는 SMB 서버 최소 보안 수준을 설정할 수 있습니다. 최소 보안 수준은 SMB 서버가 SMB 클라이언트에서 허용하는 최소 보안 토큰입니다.

이 작업에 대해

- 워크그룹 모드의 SMB 서버는 NTLM 인증만 지원합니다. Kerberos 인증은 지원되지 않습니다.
- LMCompatibilityLevel 관리자 인증이 아닌 SMB 클라이언트 인증에만 적용됩니다.

최소 인증 보안 수준을 지원되는 네 가지 보안 수준 중 하나로 설정할 수 있습니다.

값	설명
lm-NTLM-NTLMv2-KRB(기본값)	SVM(스토리지 가상 시스템)은 LM, NTLM, NTLMv2 및 Kerberos 인증 보안을 수락합니다.
NTLM-NTLMv2-KRB	SVM은 NTLM, NTLMv2 및 Kerberos 인증 보안을 수락합니다. SVM은 LM 인증을 거부합니다.
NTLMv2-KRB	SVM은 NTLMv2 및 Kerberos 인증 보안을 수락합니다. SVM은 LM 및 NTLM 인증을 거부합니다.
KRB	SVM은 Kerberos 인증 보안만 수락합니다. SVM은 LM, NTLM 및 NTLMv2 인증을 거부합니다.

단계

1. 최소 인증 보안 수준을 설정합니다. 'vserver cifs security modify -vserver_vserver_name_-lm -compatibility -level{lm-NTLM-NTLMv2-KRB | NTLM-NTLMv2-KRB | NTLMv2-KRB | KRB | KRB}'
2. 인증 보안 수준이 원하는 수준('vserver cifs security show -vserver_vserver_name_')으로 설정되어 있는지 확인합니다

관련 정보

Kerberos 기반 통신을 위한 AES 암호화 활성화 또는 비활성화

AES 암호화를 사용하여 Kerberos 기반 통신을 위한 강력한 보안을 구성합니다

Kerberos 기반 통신을 사용하여 보안을 강화하기 위해 SMB 서버에서 AES-256 및 AES-128 암호화를 활성화할 수 있습니다. 기본적으로 SVM에서 SMB 서버를 생성할 때 AES(고급 암호화 표준) 암호화가 사용되지 않습니다. AES 암호화로 제공되는 강력한 보안을 활용하려면 이 기능을 활성화해야 합니다.

SMB를 위한 Kerberos 관련 통신은 SVM에서 SMB 서버를 생성하는 동안이나 SMB 세션 설정 단계에서 사용됩니다. SMB 서버는 Kerberos 통신을 위해 다음과 같은 암호화 유형을 지원합니다.

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

Kerberos 통신에 가장 높은 보안 암호화 유형을 사용하려면 SVM에서 Kerberos 통신에 AES 암호화를 사용하도록 설정해야 합니다.

SMB 서버가 생성되면 도메인 컨트롤러는 Active Directory에 컴퓨터 시스템 계정을 만듭니다. 이때 KDC는 특정 컴퓨터 계정의 암호화 기능을 인식합니다. 그런 다음 인증 중에 클라이언트가 서버에 제공하는 서비스 티켓을 암호화하기 위해 특정 암호화 유형을 선택합니다.

ONTAP 9.12.1부터 Active Directory(AD) KDC에 알릴 암호화 유형을 지정할 수 있습니다. 를 사용할 수 있습니다 `-advertised-enc-types` 권장 암호화 유형을 활성화하는 옵션으로, 약한 암호화 유형을 비활성화하는 데 사용할 수 있습니다. 자세한 내용을 알아보십시오 "Kerberos 기반 통신을 위한 암호화 유형을 활성화 및 비활성화합니다".

> 인텔 AES 새 명령어(인텔 AES NI)는 SMB 3.0에서 사용할 수 있으며, AES 알고리즘을 개선하고 지원되는 프로세서 제품군에서 데이터 암호화를 가속화합니다. SMB 3.1.1부터 AES-128-GCM은 SMB 암호화에 사용되는 해시 알고리즘으로 AES-128-CCM을 대체합니다.

관련 정보

CIFS 서버 Kerberos 보안 설정을 수정합니다

Kerberos 기반 통신을 위해 AES 암호화를 사용하거나 사용하지 않도록 설정합니다

Kerberos 기반 통신에서 가장 강력한 보안을 활용하려면 SMB 서버에서 AES-256 및 AES-128 암호화를 사용해야 합니다. ONTAP 9.13.1부터 AES 암호화는 기본적으로 사용하도록 설정됩니다. SMB 서버가 AD(Active Directory) KDC와 Kerberos 기반 통신을 위해 AES 암호화 유형을 선택하지 않도록 하려면 AES 암호화를 사용하지 않도록 설정할 수 있습니다.

AES 암호화가 기본적으로 사용되는지 여부와 암호화 유형을 지정하는 옵션이 있는지 여부는 ONTAP 버전에 따라 다릅니다.

ONTAP 버전입니다	**AES** 암호화 사용...	암호화 유형을 지정할 수 있습니까**?**
9.13.1 이상	기본적으로 사용됩니다	예
9.12.1	수동	예
9.11.1 이하	수동	아니요

ONTAP 9.12.1부터 AES 암호화는 을 사용하여 활성화 및 비활성화됩니다 `-advertised-enc-types` 옵션: AD KDC에 보급된 암호화 유형을 지정할 수 있습니다. 기본 설정은 입니다 `rc4` 및 `des`그러나 `AES` 유형이 지정되면 `AES` 암호화가 활성화됩니다. 이 옵션을 사용하여 약한 `RC4` 및 `DES` 암호화 유형을 명시적으로 비활성화할 수도 있습니다. `ONTAP 9.11.1` 이하 버전에서는 을 사용해야 합니다 `-is-aes-encryption-enabled` AES 암호화를 활성화 및 비활성화하는 옵션과 암호화 유형을 지정할 수 없습니다.

보안을 강화하기 위해 SVM(Storage Virtual Machine)은 AES 보안 옵션을 수정할 때마다 AD에서 시스템 계정 암호를 변경합니다. 암호를 변경하려면 컴퓨터 계정이 포함된 OU(조직 구성 단위)에 대한 관리 AD 자격 증명이 필요할 수

있습니다.

SVM이 ID가 보존되지 않는 재해 복구 대상으로 구성된 경우(`-identity-preserve` 옵션이 로 설정되어 있습니다 `false` SnapMirror 구성에서 기본 SMB 서버가 아닌 보안 설정은 대상에 복제되지 않습니다. 소스 SVM에서 AES 암호화를 사용하도록 설정한 경우 수동으로 활성화해야 합니다.

예 **1.** 단계

ONTAP 9.12.1 이상

1. 다음 작업 중 하나를 수행합니다.

Kerberos 통신을 위한 **AES** 암호화 유형을 원하는 경우…	명령 입력…
활성화됨	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
사용 안 함	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   - 참고: * `-is-aes-encryption-enabled` 옵션은 ONTAP 9.12.1에서 사용되지 않으며 이후 릴리스에서 제거될 수 있습니다.

2. AES 암호화가 필요에 따라 활성화 또는 비활성화되었는지 확인합니다. `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

예

다음 예에서는 SVM VS1 기반 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다.

```
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
```

다음 예에서는 SVM VS2에서 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다. 관리자는 SMB 서버가 포함된 OU에 대한 관리 AD 자격 증명을 입력하라는 메시지가 표시됩니다.

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

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

ONTAP 9.11.1 이전 버전

1. 다음 작업 중 하나를 수행합니다.

Kerberos 통신을 위한 **AES** 암호화 유형을 원하는 경우...	명령 입력...
활성화됨	'vserver cifs security modify -vserver vserver_name -is-aes-encryption-enabled true'
사용 안 함	'vserver cifs security modify -vserver vserver_name -is-aes-encryption-enabled false'

2. AES 암호화가 원하는 대로 설정되거나 비활성화되었는지 확인합니다. 'vserver cifs security show -vserver vserver_name -fields is -aes-encryption-enabled'

   AES 암호화가 활성화된 경우 is-aes-encryption-enabled 필드가 true로 표시되고, 비활성화된 경우 false로 표시됩니다.

예

다음 예에서는 SVM VS1 기반 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다.

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

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

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

다음 예에서는 SVM VS2에서 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다. 관리자는 SMB 서버가 포함된 OU에 대한 관리 AD 자격 증명을 입력하라는 메시지가 표시됩니다.

```
cluster1::> vserver cifs security modify -vserver 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::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

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

관련 정보

"도메인 사용자가 Domain-Tunnel을 사용하여 클러스터에 로그인하지 못했습니다"

SMB 서명을 사용하여 네트워크 보안을 강화합니다

SMB 서명을 사용하여 네트워크 보안 개요를 개선합니다

SMB 서명을 사용하면 SMB 서버와 클라이언트 사이의 네트워크 트래픽이 손상되지 않도록 할 수 있으며, 재생 공격을 차단하여 이 작업을 수행합니다. 기본적으로 ONTAP는 클라이언트가 요청할 때 SMB 서명을 지원합니다. 필요에 따라 스토리지 관리자는 SMB 서명이 필요하도록 SMB 서버를 구성할 수 있습니다.

SMB 서명 정책이 CIFS 서버와의 통신에 미치는 영향

CIFS 서버 SMB 서명 보안 설정 외에도 Windows 클라이언트의 두 SMB 서명 정책은 클라이언트와 CIFS 서버 간의 디지털 통신 서명을 제어합니다. 비즈니스 요구 사항에 맞게 설정을 구성할 수 있습니다.

클라이언트 SMB 정책은 MMC(Microsoft Management Console) 또는 Active Directory GPO를 사용하여 구성되는 Windows 로컬 보안 정책 설정을 통해 제어됩니다. 클라이언트 SMB 서명 및 보안 문제에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

다음은 Microsoft 클라이언트에 대한 두 가지 SMB 서명 정책에 대한 설명입니다.

- 'Microsoft 네트워크 클라이언트: 디지털 서명 통신(서버에서 동의한 경우)'

  이 설정은 클라이언트의 SMB 서명 기능이 설정되었는지 여부를 제어합니다. 기본적으로 활성화되어 있습니다. 클라이언트에서 이 설정을 비활성화하면 CIFS 서버와의 클라이언트 통신은 CIFS 서버의 SMB 서명 설정에 따라 달라집니다.

- 마이크로네트워크 클라이언트: 디지털 서명 통신(항상)

  이 설정은 클라이언트가 서버와 통신하기 위해 SMB 서명을 필요로 하는지 제어합니다. 기본적으로 비활성화되어 있습니다. 클라이언트에서 이 설정을 비활성화하면 SMB 서명 동작은 'Microsoft 네트워크 클라이언트: 디지털 서명 통신(서버에서 동의한 경우)' 및 CIFS 서버의 설정에 대한 정책 설정을 기반으로 합니다.

> 환경에 SMB 서명이 필요하도록 구성된 Windows 클라이언트가 포함된 경우 CIFS 서버에서 SMB 서명을 설정해야 합니다. 그렇지 않으면 CIFS 서버가 이러한 시스템에 데이터를 제공할 수 없습니다.

클라이언트 및 CIFS 서버 SMB 서명 설정의 효과적인 결과는 SMB 세션이 SMB 1.0 또는 SMB 2.x 이상을 사용하는지 여부에 따라 달라집니다.

다음 표에는 세션이 SMB 1.0을 사용하는 경우 효과적인 SMB 서명 동작이 요약되어 있습니다.

클라이언트	**ONTAP —** 서명이 필요하지 않습니다	**ONTAP —** 서명이 필요합니다
서명이 비활성화되었으며 필요하지 않습니다	서명되지 않았습니다	서명됨
서명이 활성화되었으며 필요하지 않습니다	서명되지 않았습니다	서명됨
서명이 비활성화되었으며 필수입니다	서명됨	서명됨
서명이 설정되어 있어야 합니다	서명됨	서명됨

> 클라이언트에서 서명이 비활성화되었지만 CIFS 서버에서 필요한 경우 이전 Windows SMB 1 클라이언트와 일부 비 Windows SMB 1 클라이언트가 연결되지 않을 수 있습니다.

다음 표에는 세션에서 SMB 2.x 또는 SMB 3.0을 사용하는 경우 효과적인 SMB 서명 동작이 요약되어 있습니다.

SMB 2.x 및 SMB 3.0 클라이언트의 경우 SMB 서명이 항상 사용하도록 설정됩니다. 비활성화할 수 없습니다.

클라이언트	**ONTAP —** 서명이 필요하지 않습니다	**ONTAP —** 서명이 필요합니다
서명이 필요하지 않습니다	서명되지 않았습니다	서명됨
서명이 필요합니다	서명됨	서명됨

다음 표에는 기본 Microsoft 클라이언트 및 서버 SMB 서명 동작이 요약되어 있습니다.

프로토콜	해시 알고리즘입니다	활성화/비활성화할 수 있습니다	필요/필요하지 않습니다	클라이언트 기본값입니다	서버 기본값	**DC** 기본값
SMB 1.0	MD5	예	예	활성화됨(필요하지 않음)	사용 안 함(필수 아님)	필수 요소입니다
SMB 2.x	HMAC SHA-256	아니요	예	필요하지 않습니다	필요하지 않습니다	필수 요소입니다
SMB 3.0	AES-CMAC	아니요	예	필요하지 않습니다	필요하지 않습니다	필수 요소입니다

Microsoft는 더 이상 '고유 서명 통신(클라이언트에서 동의한 경우)' 또는 '고유 서명 통신(서버에서 동의한 경우)' 그룹 정책 설정을 사용할 것을 권장하지 않습니다. Microsoft는 또한 "EnableSecuritySignature" 레지스트리 설정을 더 이상 사용하지 않을 것을 권장합니다. 이러한 옵션은 SMB 1 동작에만 영향을 미치며 Digitally sign communications (Always)(항상 서명 통신) 그룹 정책 설정 또는 RequireSecuritySignature(요구 보안 서명) 레지스트리 설정으로 대체할 수 있습니다. 또한 Microsoft 블로그에서 자세한 정보를 얻을 수 있습니다. The SMB 서명의 기본 사항(SMB1 및 SMB2 모두 포함)

SMB 서명의 성능 영향

SMB 세션에서 SMB 서명을 사용하면 Windows 클라이언트와 주고 받는 모든 SMB 통신이 성능에 영향을 미치며, 이는 클라이언트와 서버(즉, SMB 서버가 포함된 SVM을 실행하는 클러스터의 노드) 모두에 영향을 미칩니다.

네트워크 트래픽의 양은 변하지 않지만, 클라이언트와 서버 모두에서 CPU 사용량이 증가하면 성능에 미치는 영향이 나타납니다.

성능에 미치는 영향은 실행 중인 ONTAP 9 버전에 따라 달라집니다. ONTAP 9.7부터 새로운 암호화 오프 로드 알고리즘을 통해 서명된 SMB 트래픽의 성능을 향상시킬 수 있습니다. SMB 서명 오프로드는 SMB 서명이 설정된 경우 기본적으로 설정됩니다.

향상된 SMB 서명 성능을 위해서는 AES-NI 오프로드 기능이 필요합니다. 해당 플랫폼에서 AES-NI 오프로드가 지원되는지 확인하려면 HWU(Hardware Universe)를 참조하십시오.

훨씬 빠른 GCM 알고리즘을 지원하는 SMB 버전 3.11을 사용할 수 있다면 더욱 향상된 성능을 얻을 수 있습니다.

네트워크, ONTAP 9 버전, SMB 버전 및 SVM 구축에 따라 SMB 서명의 성능에 미치는 영향은 매우 다양할 수 있으며 네트워크 환경에서 테스트를 통해서만 확인할 수 있습니다.

대부분의 Windows 클라이언트는 서버에서 SMB 서명을 사용하는 경우 기본적으로 협상합니다. 일부 Windows 클라이언트에 대해 SMB 보호가 필요하고 SMB 서명으로 인해 성능 문제가 발생하는 경우 재생 공격에 대한 보호가 필요하지 않은 Windows 클라이언트에서 SMB 서명을 사용하지 않도록 설정할 수 있습니다. Windows 클라이언트에서 SMB 서명을 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

SMB 서명 구성을 위한 권장 사항입니다

SMB 클라이언트와 CIFS 서버 간에 SMB 서명 동작을 구성하여 보안 요구 사항을 충족할 수 있습니다. CIFS 서버에서 SMB 서명을 구성할 때 선택하는 설정은 보안 요구 사항에 따라 다릅니다.

클라이언트 또는 CIFS 서버에서 SMB 서명을 구성할 수 있습니다. SMB 서명을 구성할 때 다음 권장 사항을 고려하십시오.

만약...	권장 사항...
클라이언트와 서버 간의 통신 보안을 강화하려는 경우	클라이언트에서 'Require Option(Sign Always)' 보안 설정을 활성화하여 클라이언트에서 SMB 서명이 필요하도록 합니다.
모든 SMB 트래픽이 특정 SVM(스토리지 가상 머신)에 서명하기를 원합니다	SMB 서명이 필요하도록 보안 설정을 구성하여 CIFS 서버에 SMB 서명이 필요합니다.

Windows 클라이언트 보안 설정 구성에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

여러 데이터 **LIF**가 구성된 경우 **SMB** 서명을 위한 지침입니다

SMB 서버에서 필요한 SMB 서명을 설정하거나 해제하는 경우 SVM에 대한 여러 데이터 LIF 구성에 대한 지침을 숙지해야 합니다.

SMB 서버를 구성할 때 여러 데이터 LIF가 구성되어 있을 수 있습니다. 이 경우 DNS 서버에 동일한 SMB 서버 호스트 이름을 사용하는 CIFS 서버에 대한 여러 개의 "A" 레코드 항목이 포함되어 있고 각 항목은 고유한 IP 주소를 사용합니다. 예를 들어, 두 개의 데이터 LIF가 구성된 SMB 서버의 DNS 'A' 레코드 항목은 다음과 같습니다.

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

일반적으로 필요한 SMB 서명 설정을 변경하면 클라이언트의 새 연결만 SMB 서명 설정의 변경 사항에 영향을 받습니다. 그러나 이 동작에 대한 예외는 있습니다. 클라이언트가 공유에 대한 기존 연결을 가지고 있고, 원래 연결을 유지하면서 설정을 변경한 후 클라이언트가 동일한 공유에 대한 새 연결을 생성하는 경우가 있습니다. 이 경우 새로운 SMB 연결과 기존 SMB 연결이 모두 새로운 SMB 서명 요구 사항을 적용합니다.

다음 예제를 고려해 보십시오.

1. CLIENT1은 'O:\' 경로를 사용하여 SMB 서명이 필요 없이 공유에 연결합니다.
2. 스토리지 관리자는 SMB 서명이 필요하도록 SMB 서버 구성을 수정합니다.
3. CLIENT1은 ':\' 경로를 사용하여('O:\' 경로를 사용하여 연결을 유지하면서) 필요한 SMB 서명과 동일한 공유에 연결합니다.
4. 그 결과, "O:\"와 "s:\" 드라이브 모두에서 데이터에 액세스할 때 SMB 서명이 사용됩니다.

수신 **SMB** 트래픽에 필요한 **SMB** 서명을 설정하거나 해제합니다

필요한 SMB 서명을 설정하여 클라이언트가 SMB 메시지에 서명하도록 요구 사항을 적용할 수 있습니다. 활성화된 경우 ONTAP는 유효한 서명이 있는 경우에만 SMB 메시지를 수락합니다. SMB 서명을 허용하되 SMB 서명이 필요하지 않은 경우 필요한 SMB 서명을 사용하지 않도록 설정할 수 있습니다.

이 작업에 대해

기본적으로 필요한 SMB 서명은 사용되지 않습니다. 필요한 SMB 서명을 언제든지 설정하거나 해제할 수 있습니다.

> 다음과 같은 상황에서는 SMB 서명이 기본적으로 비활성화되어 있지 않습니다.
>
> 1. 필요한 SMB 서명이 설정되어 있고 클러스터가 SMB 서명을 지원하지 않는 ONTAP 버전으로 되돌려집니다.
> 2. 이후 클러스터는 SMB 서명을 지원하는 ONTAP 버전으로 업그레이드됩니다.
>
> 이러한 경우 지원되는 ONTAP 버전에 원래 구성된 SMB 서명 구성은 재버전과 후속 업그레이드를 통해 유지됩니다.

SVM(Storage Virtual Machine) 재해 복구 관계를 설정할 때 'napMirror create' 명령의 '-identity-preserve' 옵션에 선택한 값에 따라 타겟 SVM에 복제된 구성 세부 정보가 결정됩니다.

만약 '-identity-preserve' 옵션을 'true'(ID-preserve)로 설정하면 SMB 서명 보안 설정이 대상에 복제됩니다.

'-identity-preserve' 옵션을 false(non-ID-preserve)로 설정하면 SMB 서명 보안 설정이 대상에 복제되지 않습니다. 이 경우 대상의 CIFS 서버 보안 설정이 기본값으로 설정됩니다. 소스 SVM에서 필요한 SMB 서명을 사용하도록 설정한 경우, 대상 SVM에서 필요한 SMB 서명을 수동으로 활성화해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

SMB 서명이 필요한 경우	명령 입력...
활성화됨	'vserver cifs security modify -vserver_vserver_name_-is-signing-required true'
사용 안 함	'vserver cifs security modify -vserver_vserver_name_-is-signing-required false'

2. 다음 명령의 출력에서 "is signing required" 필드의 값이 원하는 값으로 설정되어 있는지 확인하여 필요한 SMB 서명이 활성화되어 있는지 또는 비활성화되어 있는지 확인합니다. 'vserver cifs security show

-vserver_vserver_name_-fields is-signing-required'

예

다음 예에서는 SVM VS1 에 필요한 SMB 서명을 활성화합니다.

```
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
```

암호화 설정에 대한 변경 사항은 새 연결에 적용됩니다. 기존 연결은 영향을 받지 않습니다.

SMB 세션이 서명되었는지 확인합니다

CIFS 서버에서 연결된 SMB 세션에 대한 정보를 표시할 수 있습니다. 이 정보를 사용하여 SMB 세션이 서명되었는지 확인할 수 있습니다. 이 방법은 SMB 클라이언트 세션이 원하는 보안 설정과 연결되어 있는지 여부를 확인하는 데 유용합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 표시하려면...	명령 입력...
지정된 스토리지 가상 시스템(SVM)에서 서명된 모든 세션	'vserver cifs session show -vserver_vserver_name_ -is-session-signed true'
SVM에서 특정 세션 ID와 서명된 세션의 세부 정보	'vserver cifs session show -vserver_vserver_name_ -session-id integer-instance'

예

다음 명령을 실행하면 SVM VS1 에서 서명된 세션에 대한 세션 정보가 표시됩니다. 기본 요약 출력에는 ""세션 서명됨" 출력 필드가 표시되지 않습니다.

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

다음 명령을 실행하면 세션 ID가 2인 SMB 세션에서 세션의 서명 여부를 비롯한 자세한 세션 정보가 표시됩니다.

```
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
```

관련 정보

SMB 서명 세션 통계 모니터링

SMB 서명 세션 통계를 모니터링합니다

SMB 세션 통계를 모니터링하고 서명된 설정된 세션과 그렇지 않은 세션을 확인할 수 있습니다.

이 작업에 대해

고급 권한 레벨의 '통계' 명령은 서명된 SMB 세션 수를 모니터링하는 데 사용할 수 있는 'signed_sessions' 카운터를 제공합니다. 'Signed_sessions' 카운터는 다음과 같은 통계 객체와 함께 사용할 수 있습니다.

- 'CIFS'를 사용하면 모든 SMB 세션에 대해 SMB 서명을 모니터링할 수 있습니다.
- 'MB1'을 사용하면 SMB 1.0 세션에 대한 SMB 서명을 모니터링할 수 있습니다.
- 'MB2'를 사용하면 SMB 2.x 및 SMB 3.0 세션에 대한 SMB 서명을 모니터링할 수 있습니다.

  SMB 3.0 통계는 'MB2' 객체의 출력에 포함됩니다.

서명된 세션의 수를 총 세션 수와 비교하려면 'signed_sessions' 카운터의 출력을 '설정된_sessions' 카운터의 출력과 비교할 수 있습니다.

결과 데이터를 보려면 먼저 통계 샘플 수집을 시작해야 합니다. 데이터 수집을 중지하지 않으면 샘플의 데이터를 볼 수

있습니다. 데이터 수집을 중지하면 고정된 샘플이 제공됩니다. 데이터 수집을 중지하지 않으면 이전 쿼리와 비교하는 데 사용할 수 있는 업데이트된 데이터를 가져올 수 있습니다. 비교를 통해 추세를 파악할 수 있습니다.

단계

1. 권한 수준을 advanced:+'et-Privilege advanced로 설정합니다
2. 데이터 수집 시작:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

   '-sample-id' 매개 변수를 지정하지 않으면 명령이 샘플 식별자를 생성하고 이 샘플을 CLI 세션의 기본 샘플로 정의합니다. '-sample-id'의 값은 텍스트 문자열입니다. 동일한 CLI 세션에서 이 명령을 실행하고 '-sample-id' 매개 변수를 지정하지 않으면 명령이 이전 기본 샘플을 덮어씁니다.

   선택적으로 통계를 수집할 노드를 지정할 수 있습니다. 노드를 지정하지 않으면 이 샘플에서 클러스터의 모든 노드에 대한 통계를 수집합니다.
3. 'tortistics stop' 명령어를 이용하여 시료에 대한 데이터 수집을 중단한다.
4. SMB 서명 통계 보기:

에 대한 정보를 보려면...	입력...
서명된 세션	shope-sample-id sample_ID-counter signed_sessions
node_name[-node_node_name_]'	서명된 세션 및 설정된 세션
shope-sample-id_sample_ID_-counter signed_sessions	ESTANCE_SECURIONS

   단일 노드에 대한 정보만 표시하려면 옵션 '-node' 매개 변수를 지정합니다.
5. 관리자 권한 수준으로 돌아가기: + 'Set-Privilege admin

예

다음 예에서는 SVM(Storage Virtual Machine) VS1 에서 SMB 2.x 및 SMB 3.0 서명 통계를 모니터링하는 방법을 보여 줍니다.

다음 명령을 실행하면 고급 권한 레벨로 이동합니다.

```
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
```

다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

다음 명령을 실행하면 샘플의 데이터 수집이 중지됩니다.

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

다음 명령을 실행하면 서명된 SMB 세션과 샘플의 노드별 설정된 SMB 세션이 표시됩니다.

```
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
```

다음 명령을 실행하면 샘플에서 노드 2에 대해 서명된 SMB 세션이 표시됩니다.

```
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
```

다음 명령을 실행하면 admin 권한 레벨로 다시 이동됩니다.

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

관련 정보

SMB 세션이 서명되었는지 확인

"성능 모니터링 및 관리 개요"

SMB를 통한 데이터 전송을 위해 SMB 서버에서 필요한 SMB 암호화를 구성합니다

SMB 암호화 개요

SMB를 통한 데이터 전송을 위한 SMB 암호화는 SMB 서버에서 활성화 또는 비활성화할 수 있는 향상된 보안 기능입니다. 공유 속성 설정을 통해 공유별로 원하는 SMB 암호화 설정을 구성할 수도 있습니다.

기본적으로 SVM(스토리지 가상 머신)에 SMB 서버를 생성할 때 SMB 암호화는 사용하지 않도록 설정됩니다. SMB 암호화를 통해 제공되는 향상된 보안을 활용하려면 이 기능을 활성화해야 합니다.

암호화된 SMB 세션을 생성하려면 SMB 클라이언트가 SMB 암호화를 지원해야 합니다. Windows Server 2012 및 Windows 8부터 시작되는 Windows 클라이언트는 SMB 암호화를 지원합니다.

SVM의 SMB 암호화는 두 가지 설정을 통해 제어됩니다.

- SVM에서 기능을 활성화하는 SMB 서버 보안 옵션
- 공유 단위로 SMB 암호화 설정을 구성하는 SMB 공유 속성입니다

SVM의 모든 데이터에 액세스하려면 암호화를 사용할지, 선택한 공유에서만 데이터에 액세스하려면 SMB 암호화가 필요한지 여부를 결정할 수 있습니다. SVM 레벨 설정이 공유 레벨 설정보다 우선합니다.

효과적인 SMB 암호화 구성은 두 가지 설정의 조합에 따라 달라지며 다음 표에 설명되어 있습니다.

SMB 서버 **SMB** 암호화가 활성화되었습니다	공유 암호화 데이터 설정이 활성화되었습니다	서버측 암호화 동작
참	거짓	SVM의 모든 공유에 대해 서버 레벨 암호화가 활성화됩니다. 이 구성을 사용하면 전체 SMB 세션에 대해 암호화가 수행됩니다.
참	참	공유 레벨 암호화와 관계없이 SVM의 모든 공유에 대해 서버 레벨 암호화가 활성화됩니다. 이 구성을 사용하면 전체 SMB 세션에 대해 암호화가 수행됩니다.
거짓	참	특정 공유에 대해 공유 수준 암호화가 설정됩니다. 이 구성을 사용하면 트리 연결로부터 암호화가 수행됩니다.

SMB 서버 **SMB** 암호화가 활성화되었습니다	공유 암호화 데이터 설정이 활성화되었습니다	서버측 암호화 동작
거짓	거짓	암호화가 활성화되지 않았습니다.

암호화를 지원하지 않는 SMB 클라이언트는 암호화가 필요한 SMB 서버 또는 공유에 연결할 수 없습니다.

암호화 설정에 대한 변경 사항은 새 연결에 적용됩니다. 기존 연결은 영향을 받지 않습니다.

SMB 암호화가 성능에 미치는 영향

SMB 세션에서 SMB 암호화를 사용하면 Windows 클라이언트와 서버 간의 모든 SMB 통신이 성능에 영향을 미치며, 이는 클라이언트와 서버 모두에 영향을 미칩니다(즉, SMB 서버가 포함된 SVM을 실행하는 클러스터의 노드).

네트워크 트래픽의 양은 변하지 않지만, 클라이언트와 서버 모두에서 CPU 사용량이 증가하면 성능에 미치는 영향이 나타납니다.

성능에 미치는 영향은 실행 중인 ONTAP 9 버전에 따라 달라집니다. ONTAP 9.7부터 새로운 암호화 오프 로드 알고리즘을 통해 암호화된 SMB 트래픽에서 성능을 향상시킬 수 있습니다. SMB 암호화 오프로드는 SMB 암호화가 활성화된 경우 기본적으로 활성화됩니다.

향상된 SMB 암호화 성능을 위해서는 AES-NI 오프로드 기능이 필요합니다. 해당 플랫폼에서 AES-NI 오프로드가 지원되는지 확인하려면 HWU(Hardware Universe)를 참조하십시오.

훨씬 빠른 GCM 알고리즘을 지원하는 SMB 버전 3.11을 사용할 수 있다면 더욱 향상된 성능을 얻을 수 있습니다.

네트워크, ONTAP 9 버전, SMB 버전 및 SVM 구축에 따라 SMB 암호화가 성능에 미치는 영향은 매우 다양할 수 있으며 네트워크 환경의 테스트를 통해서만 확인할 수 있습니다.

SMB 서버에서 SMB 암호화는 기본적으로 비활성화되어 있습니다. 암호화가 필요한 SMB 공유 또는 SMB 서버에서만 SMB 암호화를 활성화해야 합니다. SMB 암호화를 통해 ONTAP는 요청을 암호 해독하고 모든 요청에 대한 응답을 암호화하는 추가 처리를 수행합니다. 따라서 필요한 경우에만 SMB 암호화를 활성화해야 합니다.

수신 **SMB** 트래픽에 필요한 **SMB** 암호화를 설정하거나 해제합니다

수신 SMB 트래픽에 SMB 암호화가 필요한 경우 CIFS 서버 또는 공유 레벨에서 설정할 수 있습니다. 기본적으로 SMB 암호화는 필요하지 않습니다.

이 작업에 대해

CIFS 서버에서 SMB 암호화를 설정하면 CIFS 서버의 모든 공유에 적용됩니다. CIFS 서버의 모든 공유에 대해 SMB 암호화가 필요하지 않거나 공유 단위로 수신 SMB 트래픽에 대해 필요한 SMB 암호화를 설정하려는 경우 CIFS 서버에서 필요한 SMB 암호화를 해제할 수 있습니다.

SVM(Storage Virtual Machine) 재해 복구 관계를 설정할 때 'napmirror create' 명령의 '-identity-preserve' 옵션에 선택한 값에 따라 타겟 SVM에 복제된 구성 세부 정보가 결정됩니다.

만약 '-identity-preserve' 옵션을 'true'(ID-preserve)로 설정하면 SMB 암호화 보안 설정이 대상에 복제됩니다.

'-identity-preserve' 옵션을 false(non-ID-preserve)로 설정하면 SMB 암호화 보안 설정이 대상에 복제되지 않습니다.

이 경우 대상의 CIFS 서버 보안 설정이 기본값으로 설정됩니다. 소스 SVM에서 SMB 암호화를 사용하도록 설정한 경우 대상에서 CIFS 서버 SMB 암호화를 수동으로 설정해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

CIFS 서버에서 들어오는 **SMB** 트래픽에 대해 **SMB** 암호화가 필요한 경우	명령 입력...
활성화됨	'vserver cifs security modify -vserver_vserver_name_-is-smb-encryption -required true'
사용 안 함	'vserver cifs security modify -vserver_vserver_name_-is-smb-encryption -required false'

2. CIFS 서버에서 필요한 SMB 암호화가 원하는 대로 설정되거나 비활성화되었는지 확인합니다. 'vserver cifs security show -vserver_vserver_name_-fields is-smb-encryption-required'

   CIFS 서버에 필요한 SMB 암호화가 설정되어 있으면 is-smb-encryption-required 필드에 true가 표시되고, 비활성화된 경우에는 false가 표시됩니다.

예

다음 예에서는 SVM VS1에서 CIFS 서버에 대해 수신 SMB 트래픽에 필요한 SMB 암호화를 설정합니다.

```
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
```

클라이언트가 암호화된 **SMB** 세션을 사용하여 연결되어 있는지 확인합니다

연결된 SMB 세션에 대한 정보를 표시하여 클라이언트가 암호화된 SMB 연결을 사용하는지 여부를 확인할 수 있습니다. 이 방법은 SMB 클라이언트 세션이 원하는 보안 설정과 연결되어 있는지 여부를 확인하는 데 유용합니다.

이 작업에 대해

SMB 클라이언트 세션은 다음 세 가지 암호화 수준 중 하나를 가질 수 있습니다.

- "암호화되지 않음"

  SMB 세션이 암호화되지 않았습니다. SVM(스토리지 가상 시스템) 레벨 또는 공유 레벨 암호화가 구성되지

않았습니다.

- 부분적으로 암호화되었습니다

  트리 연결이 발생하면 암호화가 시작됩니다. 공유 수준 암호화가 구성됩니다. SVM 레벨 암호화가 활성화되지 않았습니다.

- '암호화됨'

  SMB 세션이 완전히 암호화됩니다. SVM 레벨 암호화가 활성화됩니다. 공유 수준 암호화가 활성화되어 있거나 활성화되어 있지 않을 수 있습니다. SVM 레벨 암호화 설정이 공유 레벨 암호화 설정보다 우선합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 표시하려면...	명령 입력...
지정된 SVM의 세션에 대해 지정된 암호화 설정을 갖는 세션	'vserver cifs session show -vserver_vserver_name_{encrypted
sPartially-encrypted	encrypted}-instance'
지정된 SVM에서 특정 세션 ID의 암호화 설정입니다	'vserver cifs session show -vserver_vserver_name_ -session-id_integer_-instance'

예

다음 명령을 실행하면 세션 ID가 2인 SMB 세션에서 암호화 설정을 비롯한 자세한 세션 정보가 표시됩니다.

```
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
```

SMB 암호화 통계를 모니터링합니다

SMB 암호화 통계를 모니터링하고 설정된 세션 및 공유 연결이 암호화되고 암호화되지 않은 세션을 확인할 수 있습니다.

이 작업에 대해

고급 권한 레벨의 '통계' 명령은 다음 카운터를 제공하며, 이 카운터를 사용하여 암호화된 SMB 세션 수를 모니터링하고 연결을 공유할 수 있습니다.

카운터 이름	설명
'암호화 세션'	암호화된 SMB 3.0 세션의 수를 제공합니다
'암호화_공유_연결'	트리 연결이 발생한 암호화된 공유 수를 제공합니다
"암호화되지 않은 세션"이 끼어들었습니다	에서는 클라이언트 암호화 기능이 부족하여 거부된 세션 설정 수를 제공합니다
"암호화되지 않은_공유"가 있습니다	에서는 클라이언트 암호화 기능이 없어 거부된 공유 매핑 수를 제공합니다

이러한 카운터는 다음 통계 개체에서 사용할 수 있습니다.

- 'CIFS'를 사용하면 모든 SMB 3.0 세션에 대해 SMB 암호화를 모니터링할 수 있습니다.

  SMB 3.0 통계는 'CIFS' 객체의 출력에 포함됩니다. 암호화된 세션의 수를 총 세션 수와 비교하려면 "encrypted_sessions" 카운터의 출력과 "encrypted_sessions" 카운터의 출력을 비교할 수 있습니다.

  암호화된 공유 연결 수와 총 공유 연결 수를 비교하려면 에 대한 출력을 비교할 수 있습니다 `encrypted_share_connections` 에 대한 출력이 있는 카운터 `connected_shares` 카운터.

- reped_cencrypted_sessions는 SMB 암호화를 지원하지 않는 클라이언트로부터 암호화를 요구하는 SMB 세션을 설정하려고 시도한 횟수를 제공합니다.
- refened_cencrypted_share는 SMB 암호화를 지원하지 않는 클라이언트의 암호화가 필요한 SMB 공유에 연결하려고 시도한 횟수를 제공합니다.

결과 데이터를 보려면 먼저 통계 샘플 수집을 시작해야 합니다. 데이터 수집을 중지하지 않으면 샘플의 데이터를 볼 수 있습니다. 데이터 수집을 중지하면 고정된 샘플이 제공됩니다. 데이터 수집을 중지하지 않으면 이전 쿼리와 비교하는 데 사용할 수 있는 업데이트된 데이터를 가져올 수 있습니다. 비교를 통해 추세를 파악할 수 있습니다.

단계

1. 권한 수준을 advanced:+'et-Privilege advanced로 설정합니다
2. 데이터 수집 시작:
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   '-sample-id' 매개 변수를 지정하지 않으면 명령이 샘플 식별자를 생성하고 이 샘플을 CLI 세션의 기본 샘플로 정의합니다. '-sample-id'의 값은 텍스트 문자열입니다. 동일한 CLI 세션에서 이 명령을 실행하고 '-sample-id' 매개 변수를 지정하지 않으면 명령이 이전 기본 샘플을 덮어씁니다.

   선택적으로 통계를 수집할 노드를 지정할 수 있습니다. 노드를 지정하지 않으면 이 샘플에서 클러스터의 모든 노드에 대한 통계를 수집합니다.

3. 'tortistics stop' 명령어를 이용하여 시료에 대한 데이터 수집을 중단한다.
4. SMB 암호화 통계 보기:

에 대한 정보를 보려면...	입력...
암호화된 세션	'shope-sample-id_sample_ID_-counter encrypted_sessions
node_name[-node_node_name_]'	암호화된 세션 및 설정된 세션
shope-sample-id_sample_ID_-counter encrypted_sessions	encrypted_sessions
node_name[-node_node_name_]'	암호화된 공유 연결
'shope-sample-id_sample_ID_-counter encrypted_share_connections	*node_name*[-node_node_name_]'

에 대한 정보를 보려면...	입력...
암호화된 공유 연결 및 연결된 공유	'sHow-sample-id_sample_ID_-counter encrypted_share_connections
Connected_share	*node_name*[-node_node_name_]'
암호화되지 않은 세션이 거부되었습니다	shope-sample-id_sample_ID_-counter rejected_sencrypted_sessions
node_name[-node_node_name_]'	암호화되지 않은 공유 연결이 거부되었습니다
'shd-sample-id_sample_ID_-counter rejected_sencrypted_share	*node_name*[-node_node_name_]'

단일 노드에 대해서만 정보를 표시하려면 옵션 '-node' 매개 변수를 지정합니다.

5. 관리자 권한 수준으로 돌아가기: + 'Set-Privilege admin

예

다음 예에서는 SVM(Storage Virtual Machine) VS1 에서 SMB 3.0 암호화 통계를 모니터링하는 방법을 보여줍니다.

다음 명령을 실행하면 고급 권한 레벨로 이동합니다.

```
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
```

다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

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

다음 명령을 실행하면 해당 샘플의 데이터 수집이 중지됩니다.

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

다음 명령을 실행하면 암호화된 SMB 세션 및 샘플의 노드에 의해 설정된 SMB 세션이 표시됩니다.

```
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
```

다음 명령을 실행하면 샘플에서 노드에서 암호화되지 않은 암호화되지 않은 SMB 세션이 거부된 수가 표시됩니다.

```
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.
```

다음 명령을 실행하면 샘플의 노드에 의해 연결된 SMB 공유 및 암호화된 SMB 공유의 수가 표시됩니다.

```
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.
```

다음 명령을 실행하면 샘플에서 노드에서 암호화되지 않은 암호화되지 않은 SMB 공유 연결이 거부된 수가 표시됩니다.

```
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.
```

관련 정보

사용할 수 있는 통계 개체 및 카운터 결정

"성능 모니터링 및 관리 개요"

보안 LDAP 세션 통신

LDAP 서명 및 봉인 개념

ONTAP 9부터는 AD(Active Directory) 서버에 대한 쿼리에 대해 LDAP 세션 보안을 사용하도록 서명과 봉인을 구성할 수 있습니다. SVM(스토리지 가상 시스템)의 CIFS 서버 보안 설정을 LDAP 서버의 보안 설정에 맞게 구성해야 합니다.

서명은 비밀 키 기술을 사용하여 LDAP 페이로드 데이터의 무결성을 확인합니다. 봉인은 LDAP 페이로드 데이터를 암호화하여 중요한 정보를 일반 텍스트로 전송하지 않도록 합니다. LDAP 보안 수준_ 옵션은 LDAP 트래픽의 서명, 서명 및 봉인 여부를 나타냅니다. 기본값은 '없음'입니다.

SVM에서 SVM CIFS 보안 수정 명령에 대한 '-session-security-for-ad-ldap' 옵션을 사용하여 CIFS 트래픽에 대한 LDAP 서명 및 봉인을 사용할 수 있습니다.

CIFS 서버에서 LDAP 서명 및 봉인을 설정합니다

CIFS 서버가 Active Directory LDAP 서버와의 보안 통신을 위해 서명 및 봉인을 사용하려면 먼저 CIFS 서버 보안 설정을 수정하여 LDAP 서명 및 봉인을 설정해야 합니다.

시작하기 전에

적절한 보안 구성 값을 확인하려면 AD 서버 관리자에게 문의해야 합니다.

단계

1. Active Directory LDAP 서버에서 서명되고 봉인된 트래픽을 사용할 수 있도록 CIFS 서버 보안 설정을 구성합니다. 'vserver cifs security modify -vserver_vserver_name_-session-security-for-ad-ldap{none|sign|seal}'

   서명('사인', 데이터 무결성), 서명 및 봉인('씰', 데이터 무결성 및 암호화) 또는 둘 다('없음', 서명 또는 봉인 없음)을 사용할 수 있습니다. 기본값은 '없음'입니다.

2. LDAP 서명 및 봉인 보안 설정이 올바르게 설정되었는지 확인합니다. 'vserver cifs security show -vserver_vserver_name_'

   SVM이 이름 매핑 또는 사용자, 그룹, 넷그룹과 같은 기타 UNIX 정보를 쿼리하기 위해 동일한 LDAP 서버를 사용하는 경우 'vserver services name-service ldap client modify' 명령의 '-session-security' 옵션을 사용하여 해당 설정을 활성화해야 합니다.

TLS를 통해 LDAP를 구성합니다

자체 서명된 루트 CA 인증서의 복사본을 내보냅니다

Active Directory 통신을 보호하기 위해 SSL/TLS를 통한 LDAP를 사용하려면 먼저 Active Directory 인증서 서비스의 자체 서명 루트 CA 인증서 복사본을 인증서 파일로 내보내고 ASCII 텍스트 파일로 변환해야 합니다. 이 텍스트 파일은 ONTAP에서 SVM(스토리지 가상 머신)에 인증서를 설치하는 데 사용됩니다.

시작하기 전에

CIFS 서버가 속한 도메인에 대해 Active Directory 인증서 서비스가 이미 설치 및 구성되어 있어야 합니다. Active Director 인증서 서비스 설치 및 구성에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

"Microsoft TechNet 라이브러리: technet.microsoft.com"

단계

1. '.pem' 텍스트 형식인 도메인 컨트롤러의 루트 CA 인증서를 얻습니다.

   "Microsoft TechNet 라이브러리: technet.microsoft.com"

작업을 마친 후

SVM에 인증서를 설치합니다.

관련 정보

"Microsoft TechNet 라이브러리"

SVM에 자체 서명된 루트 **CA** 인증서를 설치합니다

LDAP 서버에 바인딩할 때 TLS를 사용한 LDAP 인증이 필요한 경우 먼저 SVM에 자체 서명된 루트 CA 인증서를 설치해야 합니다.

이 작업에 대해

TLS를 통한 LDAP가 활성화된 경우 SVM의 ONTAP LDAP 클라이언트는 ONTAP 9.0 및 9.1에서 해지된 인증서를 지원하지 않습니다.

ONTAP 9.2부터 TLS 통신을 사용하는 ONTAP 내의 모든 응용 프로그램은 OCSP(온라인 인증서 상태 프로토콜)를 사용하여 디지털 인증서 상태를 확인할 수 있습니다. OCSP가 TLS를 통해 LDAP에 대해 활성화된 경우 해지된 인증서가 거부되고 연결이 실패합니다.

단계

1. 자체 서명된 루트 CA 인증서 설치:

   a. 인증서 설치를 시작합니다. 'Security certificate install - vserver vserver_name -type server -ca'

      콘솔 출력에는 'Please enter Certificate: press <Enter> when done(인증서를 입력하십시오. 완료되면 <Enter> 키를 누르십시오)' 메시지가 표시됩니다

   b. 텍스트 편집기로 인증서 '.pem' 파일을 열고 '-----'로 시작하는 줄을 포함하여 인증서를 복사합니다. 인증서 시작 ---- '----'로 끝나는 종료 인증서 ---- 그런 다음 명령 프롬프트 뒤에 인증서를 붙여 넣습니다.

   c. 인증서가 올바르게 표시되는지 확인합니다.

   d. Enter 키를 눌러 설치를 완료합니다.

2. 인증서가 설치되어 있는지 확인합니다. 'Security certificate show -vserver_vserver_name_'

서버에서 **TLS**를 통해 **LDAP**를 활성화합니다

SMB 서버가 Active Directory LDAP 서버와의 보안 통신에 TLS를 사용하려면 먼저 SMB 서버 보안 설정을 수정하여 TLS를 통한 LDAP를 활성화해야 합니다.

ONTAP 9.10.1부터 LDAP 채널 바인딩은 AD(Active Directory) 및 이름 서비스 LDAP 연결에 대해 기본적으로 지원됩니다. ONTAP는 시작 TLS 또는 LDAPS가 활성화되고 세션 보안이 서명 또는 봉인으로 설정된 경우에만 LDAP 연결을 사용하여 채널 바인딩을 시도합니다. AD 서버에서 LDAP 채널 바인딩을 비활성화하거나 다시 설정하려면 ' vserver cifs security modify ' 명령을 사용하여 '-try-channel-binding-for-ad-ldap' 매개 변수를 사용합니다.

자세한 내용은 다음을 참조하십시오.

- "LDAP 개요"
- "Windows의 2020 LDAP 채널 바인딩 및 LDAP 서명 요구 사항".

단계

1. Active Directory LDAP 서버와 보안 LDAP 통신을 허용하는 SMB 서버 보안 설정을 구성합니다. 'vserver cifs security modify -vserver_vserver_name_-use-start-tls-for-ad-ldap true'
2. TLS를 통한 LDAP 보안 설정이 "true"로 설정되어 있는지 확인합니다. vserver cifs security show -vserver_vserver_name_

> SVM이 이름 매핑 또는 기타 UNIX 정보(예: 사용자, 그룹 및 넷그룹)를 쿼리하기 위해 동일한 LDAP 서버를 사용하는 경우 'vserver services name-service ldap client modify' 명령을 사용하여 '-use-start-tls' 옵션도 수정해야 합니다.