



SMB를 통한 데이터 전송을 위해 **SMB** 서버에서 필요한 **SMB** 암호화를 구성합니다 ONTAP 9

NetApp
September 12, 2024

목차

SMB를 통한 데이터 전송을 위해 SMB 서버에서 필요한 SMB 암호화를 구성합니다	1
SMB 암호화 개요	1
SMB 암호화가 성능에 미치는 영향	2
수신 SMB 트래픽에 필요한 SMB 암호화를 설정하거나 해제합니다	2
클라이언트가 암호화된 SMB 세션을 사용하여 연결되어 있는지 확인합니다	3
SMB 암호화 통계를 모니터링합니다	5

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.
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
<i>node_name</i> [-node_node_name_]	암호화된 세션 및 설정된 세션
shope-sample-id_sample_ID_-counter encrypted_sessions	encrypted_sessions
<i>node_name</i> [-node_node_name_]	암호화된 공유 연결
'shope-sample-id_sample_ID_-counter encrypted_share_connections	<i>node_name</i> [-node_node_name_]
암호화된 공유 연결 및 연결된 공유	'sHow-sample-id_sample_ID_-counter encrypted_share_connections
Connected_share	<i>node_name</i> [-node_node_name_]
암호화되지 않은 세션이 거부되었습니다	shope-sample-id_sample_ID_-counter rejected_sencrypted_sessions
<i>node_name</i> [-node_node_name_]	암호화되지 않은 공유 연결이 거부되었습니다
'shd-sample-id_sample_ID_-counter rejected_sencrypted_share	<i>node_name</i> [-node_node_name_]

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

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

다음 예에서는 SVM(Storage Virtual Machine) VS1 에서 SMB 3.0 암호화 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 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"](#)

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.