



Configure required SMB encryption on SMB servers for data transfers over SMB

ONTAP 9

NetApp
November 19, 2022

Table of Contents

- Configure required SMB encryption on SMB servers for data transfers over SMB 1
 - SMB encryption overview 1
 - Performance impact of SMB encryption. 2
 - Enable or disable required SMB encryption for incoming SMB traffic 2
 - Determine whether clients are connected using encrypted SMB sessions 3
 - Monitor SMB encryption statistics 5

Configure required SMB encryption on SMB servers for data transfers over SMB

SMB encryption overview

SMB encryption for data transfers over SMB is a security enhancement that you can enable or disable on SMB servers. You can also configure the desired SMB encryption setting on a share-by-share basis through a share property setting.

By default, when you create a SMB server on the storage virtual machine (SVM), SMB encryption is disabled. You must enable it to take advantage of the enhanced security provided by SMB encryption.

To create an encrypted SMB session, the SMB client must support SMB encryption. Windows clients beginning with Windows Server 2012 and Windows 8 support SMB encryption.

SMB encryption on the SVM is controlled through two settings:

- A SMB server security option that enables the functionality on the SVM
- A SMB share property that configures the SMB encryption setting on a share-by-share basis

You can decide whether to require encryption for access to all data on the SVM or to require SMB encryption to access data only in selected shares. SVM-level settings supersede share-level settings.

The effective SMB encryption configuration depends on the combination of the two settings and is described in the following table:

SMB server SMB encryption enabled	Share encrypt data setting enabled	Server-side encryption behavior
True	False	Server-level encryption is enabled for all of the shares in the SVM. With this configuration, encryption happens for the entire SMB session.
True	True	Server-level encryption is enabled for all of the shares in the SVM irrespective of share-level encryption. With this configuration, encryption happens for the entire SMB session.
False	True	Share-level encryption is enabled for the specific shares. With this configuration, encryption happens from the tree connect.
False	False	No encryption is enabled.

SMB clients that do not support encryption cannot connect to a SMB server or share that requires encryption.

Performance impact of SMB encryption

When SMB sessions use SMB encryption, all SMB communications to and from Windows clients experience a performance impact, which affects both the clients and the server (that is, the nodes on the cluster running the SVM that contains the SMB server).

The performance impact shows as increased CPU usage on both the clients and the server, although the amount of network traffic does not change.

The extent of the performance impact depends on the version of ONTAP 9 you are running. Beginning with ONTAP 9.7, a new encryption off-load algorithm can enable better performance in encrypted SMB traffic. SMB encryption offload is enabled by default when SMB encryption is enabled.

Enhanced SMB encryption performance requires AES-NI offload capability. See the Hardware Universe (HWU) to verify that AES-NI offload is supported for your platform.

Further performance improvements are also possible if you are able to use SMB version 3.11 (supported with Windows 10 and Windows Server 2016), which supports the much faster GCM algorithm.

Depending on your network, ONTAP 9 version, SMB version, and SVM implementation, the performance impact of SMB encryption can vary widely; you can verify it only through testing in your network environment.

SMB encryption is disabled by default on the SMB server. You should enable SMB encryption only on those SMB shares or SMB servers that require encryption. With SMB encryption, ONTAP performs additional processing of decrypting the requests and encrypting the responses for every request. SMB encryption should therefore be enabled only when necessary.

Enable or disable required SMB encryption for incoming SMB traffic

If you want to require SMB encryption for incoming SMB traffic you can enable it on the CIFS server or at the share level. By default, SMB encryption is not required.

About this task

You can enable SMB encryption on the CIFS server, which applies to all shares on the CIFS server. If you do not want required SMB encryption for all shares on the CIFS server or if you want to enable required SMB encryption for incoming SMB traffic on a share-by-share basis, you can disable required SMB encryption on the CIFS server.

When you set up a storage virtual machine (SVM) disaster recovery relationship, the value you select for the `-identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `-identity-preserve` option to `true` (ID-preserve), the SMB encryption security setting is replicated to the destination.

If you set the `-identity-preserve` option to `false` (non-ID-preserve), the SMB encryption security setting is not replicated to the destination. In this case, the CIFS server security settings on the destination are set to the default values. If you have enabled SMB encryption on the source SVM, you must manually enable CIFS server SMB encryption on the destination.

Steps

1. Perform one of the following actions:

If you want required SMB encryption for incoming SMB traffic on the CIFS server to be...	Enter the command...
Enabled	<pre>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true</pre>
Disabled	<pre>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false</pre>

2. Verify that required SMB encryption on the CIFS server is enabled or disabled as desired: `vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`

The `is-smb-encryption-required` field displays `true` if required SMB encryption is enabled on the CIFS server and `false` if it is disabled.

Example

The following example enables required SMB encryption for incoming SMB traffic for the CIFS server on 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
```

Determine whether clients are connected using encrypted SMB sessions

You can display information about connected SMB sessions to determine whether clients are using encrypted SMB connections. This can be helpful in determining whether SMB client sessions are connecting with the desired security settings.

About this task

SMB clients sessions can have one of three encryption levels:

- `unencrypted`

The SMB session is not encrypted. Neither storage virtual machine (SVM)-level or share-level encryption is

configured.

- `partially-encrypted`

Encryption is initiated when the tree-connect occurs. Share-level encryption is configured. SVM-level encryption is not enabled.

- `encrypted`

The SMB session is fully encrypted. SVM-level encryption is enabled. Share level encryption might or might not be enabled. The SVM-level encryption setting supersedes the share-level encryption setting.

Steps

1. Perform one of the following actions:

If you want display information about...	Enter the command...
Sessions with a specified encryption setting for sessions on a specified SVM	<code>vserver cifs session show -vserver <i>vserver_name</i> {unencrypted partially-encrypted encrypted} -instance</code>
The encryption setting for a specific session ID on a specified SVM	<code>vserver cifs session show -vserver <i>vserver_name</i> -session-id <i>integer</i> -instance</code>

Examples

The following command displays detailed session information, including the encryption setting, on an SMB session with a session ID of 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

```

Monitor SMB encryption statistics

You can monitor SMB encryption statistics and determine which established sessions and share connections are encrypted and which are not.

About this task

The `statistics` command at the advanced privilege level provides the following counters, which you can use to monitor the number of encrypted SMB sessions and share connections:

Counter name	Descriptions
<code>encrypted_sessions</code>	Gives the number of encrypted SMB 3.0 sessions
<code>encrypted_share_connections</code>	Gives the number of encrypted shares on which a tree connect has happened
<code>rejected_unencrypted_sessions</code>	Gives the number of session setups rejected due to a lack of client encryption capability
<code>rejected_unencrypted_shares</code>	Gives the number of share mappings rejected due to a lack of client encryption capability

These counters are available with the following statistics objects:

- `cifs` enables you to monitor SMB encryption for all SMB 3.0 sessions.

SMB 3.0 statistics are included in the output for the `cifs` object. If you want to compare the number of encrypted sessions to the total number of sessions, you can compare output for the `encrypted_sessions` counter with the output for the `established_sessions` counter.



If you want to compare the number of encrypted share connections to the total number of share connections, you can compare output for the ``encrypted_share_connections`` counter with the output for the ``connected_shares`` counter.

- `rejected_unencrypted_sessions` provides the number of times an attempt has been made to establish an SMB session that requires encryption from a client that does not support SMB encryption.
- `rejected_unencrypted_shares` provides the number of times an attempt has been made to connect to an SMB share that requires encryption from a client that does not support SMB encryption.

You must start a statistics sample collection before you can view the resultant data. You can view data from the sample if you do not stop the data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify trends.

Performance management

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Start a data collection: `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

If you do not specify the `-sample-id` parameter, the command generates a sample identifier for you and defines this sample as the default sample for the CLI session. The value for `-sample-id` is a text string. If you run this command during the same CLI session and do not specify the `-sample-id` parameter, the command overwrites the previous default sample.

You can optionally specify the node on which you want to collect statistics. If you do not specify the node, the sample collects statistics for all nodes in the cluster.

3. Use the `statistics stop` command to stop collecting data for the sample.
4. View SMB encryption statistics:

If you want to view information for...	Enter...
Encrypted sessions	<code>show -sample-id sample_ID -counter encrypted_sessions node_name [-node node_name]</code>

If you want to view information for...	Enter...
Encrypted sessions and established sessions	<code>show -sample-id <i>sample_ID</i> -counter encrypted_sessions established_sessions <i>node_name</i> [-node <i>node_name</i>]</code>
Encrypted share connections	<code>show -sample-id <i>sample_ID</i> -counter encrypted_share_connections <i>node_name</i> [-node <i>node_name</i>]</code>
Encrypted share connections and connected shares	<code>show -sample-id <i>sample_ID</i> -counter encrypted_share_connections connected_shares <i>node_name</i> [-node <i>node_name</i>]</code>
Rejected unencrypted sessions	<code>show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_sessions <i>node_name</i> [-node <i>node_name</i>]</code>
Rejected unencrypted share connections	<code>show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_share <i>node_name</i> [-node <i>node_name</i>]</code>

If you want to display information only for a single node, specify the optional `-node` parameter.

5. Return to the admin privilege level: `set -privilege admin`

Examples

The following example shows how you can monitor SMB 3.0 encryption statistics on storage virtual machine (SVM) `vs1`.

The following command moves to the advanced privilege level:

```
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

The following command starts data collection for a new sample:

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

The following command stops data collection for that sample:

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

The following command shows encrypted SMB sessions and established SMB sessions by the node from the sample:

```
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

The following command shows the number of rejected unencrypted SMB sessions by the node from the sample:

```
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.

The following command shows the number of connected SMB shares and encrypted SMB shares by the node from the sample:

```
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.

The following command shows the number of rejected unencrypted SMB share connections by the node from the sample:

```
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.

Related information

[Determining which statistics objects and counters are available](#)

[Performance monitoring express setup](#)

Copyright information

Copyright © 2022 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.