StarWind Virtual SAN®
Challenge-Handshake Authentication Protocol (CHAP)
AUGUST, 2018
TECHNICAL PAPERS
Trademarks

“StarWind”, “StarWind Software” and the StarWind and the StarWind Software logos are registered trademarks of StarWind Software. “StarWind LSFS” is a trademark of StarWind Software which may be registered in some jurisdictions. All other trademarks are owned by their respective owners.

Changes

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, StarWind Software assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein. StarWind Software reserves the right to make changes in the product design without reservation and without notification to its users.

Technical Support and Services

If you have questions about installing or using this software, check this and other documents first - you will find answers to most of your questions on the Technical Papers webpage or in StarWind Forum. If you need further assistance, please contact us .

About StarWind

StarWind is a pioneer in virtualization and a company that participated in the development of this technology from its earliest days. Now the company is among the leading vendors of software and hardware hyper-converged solutions. The company’s core product is the years-proven StarWind Virtual SAN, which allows SMB and ROBO to benefit from cost-efficient hyperconverged IT infrastructure. Having earned a reputation of reliability, StarWind created a hardware product line and is actively tapping into hyperconverged and storage appliances market. In 2016, Gartner named StarWind “Cool Vendor for Compute Platforms” following the success and popularity of StarWind HyperConverged Appliance. StarWind partners with world-known companies: Microsoft, VMware, Veeam, Intel, Dell, Mellanox, Citrix, Western Digital, etc.

Copyright ©2009-2018 StarWind Software Inc.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of StarWind Software.
Introduction

StarWind implements and fully supports the Challenge-Handshake Authentication Protocol (CHAP) for the authentication of users. Challenge Handshake Authentication Protocol is a type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. Both sender and peer share a predefined secret. The peer concatenates the random value (or nonce), the ID and the secret, and calculates a one-way hash using MD5. The hash value is sent to the authenticator, which in turn builds that same string on its side, calculates the MD5 sum itself and compares the result with the value received from the peer. If the values match, the peer is authenticated. By transmitting the hash only, the secret can’t be reverse-engineered. The ID value is increased with each CHAP dialogue to protect against replay attacks. The access can be limited to all server targets at once or set permissions for each target separately. In case of limiting access to certain targets only and keep other targets shared with all, the permissions need to be set for those targets only. Otherwise, the access limitation for all targets may be done by setting permissions for connection. Also, the one-side authentication or mutual authentication can be used.

Configuring Chap Settings In Starwind Management Console

StarWind enables global and individual access CHAP restrictions to targets. Challenge-Handshake Authentication Protocol (CHAP) authenticates a user or network host to an authenticating entity. CHAP provides protection against replay attacks by the peer through the use of an incrementally changing identifier and a variable challenge value. CHAP requires that both client and server know the plain text of the secret, although it is never sent over the network.

NOTE: More information about CHAP can be found here.

Setting global permissions

1. Select one of the hosts in the StarWind Management Console tree.

2. Click the CHAP Permissions tab. Right-click the main tab area and select Add Permission from the shortcut menu.
3. In **New Permission Item**, specify the required settings:

- **Target CHAP name**: is a name used by CHAP for initiator authentication.
- **Target secret**: is a secret that is used by CHAP for initiator authentication.
- **Initiator CHAP name**: is a name for the CHAP mutual authentication.
- **Initiator secret**: is a secret for the CHAP mutual authentication.

4. Check the new **CHAP Permission** tab.

![New Permission Item](image)
NOTE: Repeat this step to add as many permissions as needed. Now all clients need to provide CHAP settings to access any target on this server.

NOTE: If the partner authentication settings are not changed, StarWind will not be able to synchronize HA devices to the partner node after the service restart.

Setting individual target permissions

1. Select the required target in the StarWind Management Console tree.

2. Click Add Permission in the CHAP Permissions area.

3. In the New Permission Item window, specify the required settings:
   - **Target CHAP name**: is a name used by CHAP for initiator authentication.
   - **Target secret**: is a secret that is used by CHAP for initiator authentication.
   - **Initiator CHAP name**: is a name for the CHAP mutual authentication.
   - **Initiator secret**: is a secret for the CHAP mutual authentication.
Click **OK**.

**NOTE:** Repeat this step to add as many permissions as needed. Now all clients need to provide CHAP settings to access target on this server.

![CHAP Permissions](image)

**NOTE:** If the partner authentication settings are not changed, StarWind will not be able to synchronize HA devices to the partner node after the service restart.

### Setting permissions for HA target

1. Open StarWind Management Console.

2. Choose partner device. Click **Change Partner Authentication Settings** or right-click the device and select **Change Partner Authentication Settings** from the shortcut menu.
3. Select CHAP in Authentication Type.

Partner Authentication Settings

Authentication Parameters

Partner: ign.2008-08.com.starwindsoftware-sw-sup-fs-01-ha-ds-main

Authentication Type: CHAP

<table>
<thead>
<tr>
<th>Local Name</th>
<th>Local Secret</th>
<th>Peer Name</th>
<th>Peer Secret</th>
</tr>
</thead>
</table>

4. Indicate Local Name and Local Secret. Click OK.
Selecting The Hypervisor

Please select the required option:

Configuring Chap Settings On Hyper-V

Setting target permissions

1. Open iSCSI Initiator.

2. Select Target in the Discovered targets area. Click Connect.
3. Click **Advance**
To enable CHAP, select the **Enable CHAP log on** checkbox.

5. Indicate **Name** and **Target secret**. Click **OK**.
6. Open Properties... in the iSCSI Initiator and check Authentication of the connected session.
7. Check **Favorite Target**
NOTE: Target will not be reconnected after the service restart in case it does not have CHAP Authentication.

Changing CHAP initiator configuration

1. Open iSCSI initiator and click **Configuration**.
NOTE: Click Change... to modify the initiator name. Click CHAP... to set the initiator CHAP secret.

**Configuring Chap Settings On Esxi**

1. Click **Add dynamic target** in Dynamic Targets. Click **Edit Settings**.
One Stop Virtualization Shop

StarWind Virtual SAN ® Challenge-Handshake Authentication Protocol (CHAP)

2. Uncheck *Inherit from parent*.

3. Write **Name** and **Secret** in the corresponding fields. Click **Save**.

4. Click the **Save configuration** button.

**NOTE:** Target will not be reconnected after the service restart if it does not have CHAP.
Configuring Chap Settings On Xen

1. Open XenCenter and click on the **Server** tab. Then select **Storage** tab and click **New SR...**.

2. Select **iSCSI** as **Virtual disk storage** and click **Next**.
3. Indicate **Name** in **New Storage Repository**. Click **Next** to proceed.

4. Indicate **Target host name/IP address** and check **Use CHAP**. Type username and password. Click **Finish**.
### Enter a path for your iSCSI storage

<table>
<thead>
<tr>
<th>Location</th>
<th>Provide a target host for your iSCSI storage, indicating your target IQN and your target LUN before proceeding.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target host name/IP address:</td>
<td>192.168.10.103 : 3260</td>
</tr>
<tr>
<td>CHAP username:</td>
<td>Target1</td>
</tr>
<tr>
<td>CHAP password:</td>
<td>************</td>
</tr>
</tbody>
</table>

**Scan Target Host**

**iSCSI target**

- Target IQN: [Dropdown]
- Target LUN: [Dropdown]
Contacts

<table>
<thead>
<tr>
<th>US Headquarters</th>
<th>EMEA and APAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-617-449-77 17</td>
<td>+44 203 769 18 57 (UK)</td>
</tr>
<tr>
<td>1-617-507-58 45</td>
<td>+34 629 03 07 17</td>
</tr>
<tr>
<td>1-866-790-26 46</td>
<td>(Spain and Portugal)</td>
</tr>
</tbody>
</table>

Customer Support Portal: [https://www.starwind.com/support](https://www.starwind.com/support)
Support Forum: [https://www.starwind.com/forums](https://www.starwind.com/forums)
Sales: sales@starwind.com
General Information: info@starwind.com

StarWind Software, Inc. 35 Village Rd., Suite 100, Middleton, MA 01949 USA
www.starwind.com

©2019, StarWind Software Inc. All rights reserved.