Secure client access with Kerberos

ONTAP System Manager

Amanda Stroman, Barb Einarsen, Thom Illingworth, Mark Forry
November 04, 2020

This PDF was generated from https://docs.netapp.com/us-en/ontap/task_nas_secure_client_access_with_kerberos.html on November 20, 2020. Always check docs.netapp.com for the latest.

NetApp®

Table of Contents

Secure client access with Kerberos 1

Secure client access with Kerberos

Enable Kerberos to secure storage access for NAS clients.

This procedure configures Kerberos on an existing storage VM enabled for NFS or SMB.

Before beginning you should have configured DNS, NTP, and LDAP on the storage system.

Steps

1. At the ONTAP command line, set UNIX permissions for the storage VM root volume.
   a. Display the relevant permissions on the storage VM root volume: `volume show -volume root_vol_name-fields user,group,unix-permissions`

      The root volume of the storage VM must have the following configuration:

Name...	Setting...
UID	root or ID 0
GID	root or ID 0
UNIX permissions	755

   b. If these values are not shown, use the `volume modify` command to update them.
2. Set user permissions for the storage VM root volume.
   a. Display the local UNIX users: `vserver services name-service unix-user show -vserver vserver_name`

      The storage VM should have the following UNIX users configured:

User name	User ID	Primary group ID
nfs	500	0
root	0	0

      Note: The NFS user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS client user; see step 5.

   b. If these values are not shown, use the `vserver services name-service unix-user modify` command to update them.
3. Set group permissions for the storage VM root volume.
   a. Display the local UNIX groups: `vserver services name-service unix-group show -vserver vserver_name`

The storage VM should have the following UNIX groups configured:

Group name	Group ID
daemon	1
root	0

b. If these values are not shown, use the `vserver services name-service unix-group modify` command to update them.

4. Switch to System Manager to configure Kerberos
5. In ONTAP System Manager, click **Storage** > **Storage VMs** and select the storage VM.
6. Click **Settings**.
7. Click → under Kerberos.
8. Click **Add** under Kerberos Realm, and complete the following sections:
   - Add Kerberos Realm

     Enter configuration details depending on KDC vendor.

   - Add Network Interface to Realm

     Click **Add** and select a network interface.

9. If desired, add mappings from Kerberos principal names to local user names.
   a. Click **Storage** > **Storage VMs** and select the storage VM.
   b. Click **Settings**, and then click → under **Name Mapping**.
   c. Under **Kerberos to UNIX**, add patterns and replacements using regular expressions.

Copyright Information

Copyright © 2020 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.