



Configure credentials for an individual SQL Server resource

SnapCenter Software

Nirupama Sriram, Soumik Das, Archana
August 02, 2021

Table of Contents

Configure credentials for an individual SQL Server resource 1

Configure credentials for an individual SQL Server resource

You can configure credentials to perform data protection jobs on individual SQL Server resource for each user. While you can configure the credentials globally, you might want to do this only for a particular resource.

About this task

- If you are using Windows credentials for authentication, you must set up your credential before installing plug-ins.

However, if you are using an SQL Server instance for authentication, you must add the credential after installing plug-ins.

- If you have enabled SQL authentication while setting up the credentials, the discovered instance or database is shown with a red color padlock icon.

If the padlock icon appears, you must specify the instance or database credentials to successfully add the instance or database to a resource group.

- You must assign the credential to a role-based access control (RBAC) user without sysadmin access when the following conditions are met:
 - The credential is assigned to an SQL instance.
 - The SQL instance or host is assigned to an RBAC user.



The user must have both the resource group and backup privileges

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Credential**.
3. To add a new credential, click **New**.
4. In the **Credential** page, configure the credentials:

For this field...	Do this...
Credential name	Enter a name for the credentials.

For this field...	Do this...
Username	<p>Enter the user name used for SQL Server authentication.</p> <ul style="list-style-type: none"> • Domain administrator or any member of the administrator group Specify the domain administrator or any member of the administrator group on the system on which you are installing the SnapCenter plug-in. Valid formats for the Username field are: <ul style="list-style-type: none"> ◦ <i>NetBIOS\UserName</i> ◦ <i>Domain FQDN\UserName</i> • Local administrator (for workgroups only) For systems that belong to a workgroup, specify the built-in local administrator on the system on which you are installing the SnapCenter plug-in. You can specify a local user account that belongs to the local administrators group if the user account has elevated privileges or the User Access control feature is disabled on the host system. The valid format for the Username field is: <i>UserName</i>
Password	Enter the password used for authentication.
Authentication mode	Select the SQL Server authentication mode. You can also choose Windows authentication if the Windows user has sysadmin privileges on the SQL server.
Host	Select the host.
SQL Server Instance	Select the SQL Server instance.

5. Click **OK** to add the credential.
6. In the left navigation pane, click **Resources**.
7. In the **Resources** page, select **Instance** from the **View** list.
 - a. Click , and then select the host name to filter the instances.
 - b. Click  to close the filter pane.
8. In the **Instance Protect** page, protect the instance, and if required, click **Configure Credentials**.

If the user who is logged in to the SnapCenter Server does not have access to SnapCenter Plugin for Microsoft SQL Server, then the user has to configure the credentials.



The credential option does not apply to databases and availability groups.

9. Click **Refresh Resources**.

Copyright Information

Copyright © 2021 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.