



RBAC permissions and roles

SnapCenter Software

Soumik Das, Archana
June 15, 2021

This PDF was generated from https://docs.netapp.com/us-en/snapcenter/concept/reference_role_based_access_control_permissions_and_roles.html on June 18, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- RBAC permissions and roles 1
 - SnapCenter roles 1
 - SnapCenter Plug-in for VMware vSphere roles 1
 - SnapCenter permissions 1

RBAC permissions and roles

SnapCenter role-based access control (RBAC) enables you to create roles and assign permissions to those roles, and then assign users or groups of users to the roles. This enables SnapCenter administrators to create a centrally managed environment, while application administrators can manage data protection jobs. SnapCenter ships with some predefined roles and permissions.

SnapCenter roles

SnapCenter ships with the following predefined roles. You can either assign users and groups to these roles or create new roles.

When you assign a role to a user, only jobs that are relevant to that user are visible in the Jobs page unless you assigned the SnapCenter Admin role.

- App Backup and Clone Admin
- Backup and Clone Viewer
- Infrastructure Admin
- SnapCenterAdmin

SnapCenter Plug-in for VMware vSphere roles

For managing VM-consistent data protection of VMs, VMDKs, and datastores, the following roles are created in vCenter by the SnapCenter Plug-in for VMware vSphere:

- SCV Administrator
- SCV View
- SCV Backup
- SCV Restore
- SCV Guest File Restore

For more information, see [Types of RBAC for SnapCenter Plug-in for VMware vSphere users](#)

Best Practice: NetApp recommends that you create one ONTAP role for SnapCenter Plug-in for VMware vSphere operations and assign it all the required privileges.

SnapCenter permissions

SnapCenter provides the following permissions:

- Resource Group
- Policy
- Backup
- Host

- Storage Connection
- Clone
- Provision (only for Microsoft SQL database)
- Dashboard
- Reports
- Restore
 - Full Volume Restore (only for Custom Plug-ins)
- Resource

Plug-in privileges are required from the administrator for non-administrators to perform resource discovery operation.

- Plug-in Install or Uninstall



When you enable Plug-in Installation permissions, you must also modify the Host permission to enable reads and updates.

- Migration
- Mount (only for Oracle database)
- Unmount (only for Oracle database)
- Job Monitor

Job Monitor permission enables members of different roles to see the operations on all the objects to which they are assigned.

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.