Additional REST considerations

Astra Automation

NetApp
September 13, 2021

This PDF was generated from https://docs.netapp.com/us-en/astra-automation/additional/security.html on September 13, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Additional REST considerations 1
Security 1
Working with collections 2
Diagnostics and support 2

Additional REST considerations

Security

The Astra REST API provides multiple layers of security.

All HTTP network traffic is protected using the transport layer security (TLS) standard.

Astra API tokens

To use the Astra REST API, you must provide an API token on every request in the `Authorization` request header. Note the following:

- You can generate an API token at the Astra web user interface.
- A token never expires after it is created.
- You can revoke a token at any time at the Astra web user interface.

See Get an API token for more information.

Revoking an API access token

You can revoke an API token at the Astra web interface when it is no longer needed.

Before you begin

You need an account for the Astra service. You should also identify the tokens you want to revoke.

About this task

After a token is revoked, it is immediately and permanently unusable.

Steps

1. Sign in to Astra using your account credentials.

   Access the following site for Astra Control Service: https://astra.netapp.io

2. Click the figure icon at the top right of the page and select **API access**.
3. Select the token or tokens you want to revoke.
4. Under the **Actions** drop-down box, click **Revoke tokens**.

Roles and access control

Each Astra user is assigned to a single role which determines the actions that can be performed. The roles are arranged in a hierarchy as described in the table below.

Role	Description
Owner	Has all the permissions of the Admin role and can also delete Astra accounts.
Admin	Has all the permissions of the Member role and can also invite users to join an account.
Member	Can fully manage the Astra application and compute resources.

Role	Description
Viewer	Restricted to only viewing resources.

Working with collections

The Astra REST API provides several different ways to access resource collections through the defined query parameters.

Selecting values

You can specify which key-value pairs should be returned for each resource instance using the `include` parameter. All of the instances are returned in the response body.

Filtering

Collection resource filtering allows an API user to specify conditions which determine if a resource is returned in the response body. The `filter` parameter is used to indicate the filtering condition.

Sorting

Collection resource sorting allows an API user to specify the order in which resources are returned in the response body. The `orderBy` parameter is used to indicate the filtering condition.

Pagination

You can enforce pagination by restricting the number of resource instances returned on a request using the `limit` parameter.

Count

If you include the Boolean parameter `count` set to `true`, the number of resources in the returned array for a given response is provided in the metadata section.

Diagnostics and support

There are several support features available with the Astra REST API that can be used for diagnostics and debugging.

API resources

There are several Astra features exposed through API resources that provide diagnostic information and support.

Type	Description
Event	System activities that are recorded as part of Astra processing.
Notification	A subset of the Events that are considered important enough to be presented to the user.
Unread notification	The notifications that have yet to be read or retrieved by the user.

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.