



Frequently asked questions about Cloud Manager SaaS

Cloud Manager

Ben Cammett
November 19, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/faq_saas.html on February 28, 2021.
Always check docs.netapp.com for the latest.

Table of Contents

- Frequently asked questions about Cloud Manager SaaS 1
 - What capabilities were introduced with the Cloud Manager SaaS release on Aug 3, 2020? 1
 - What will happen to the Cloud Manager instance deployed in my VPC/VNet? 1
 - Can I remove the Connector now that I am using the SaaS platform? 1
 - Can I still use my Cloud Manager the same way that I did before (locally through the instance deployed in my VPC)? 2
 - Is a migration or any specific action required to move to Cloud Manager SaaS? 2
 - Did Cloud Volumes ONTAP or the data that it stores change or move anywhere? 2
 - Where is the endpoint for the Cloud Manager SaaS platform? 2
 - What kind of data or metadata is stored in the Cloud Manager SaaS service layer? 2
 - What data or metadata is stored by the Connector that's deployed in the VPC/VNet? 2
 - What are the data and metadata paths? 2
 - Is there a GDPR impact when using the Cloud Compliance service through the SaaS endpoint? 3
 - What kind of network direction access is used for the SaaS-based UI and API to access the Connector? .. 3
 - Has the login flow changed? 3
 - Is the SaaS-based Cloud Manager compliant (SOC2, FedRAMP, etc.)? 3

Frequently asked questions about Cloud Manager SaaS

This FAQ answers key questions associated with the new Cloud Manager SaaS release.

What capabilities were introduced with the Cloud Manager SaaS release on Aug 3, 2020?

- **A unified API and UI**

A unified and centralized API control plane for all NetApp ONTAP-based storage solutions, providing customers with management and control of the following:

- Azure NetApp Files
- Cloud Volumes Service for AWS
- Cloud Volumes Service for Google Cloud
- Cloud Volumes ONTAP

- **Seamless integration with NetApp data services**

For smooth integration, storage solutions come built-in with data services that can be easily integrated.

- **Centralized management of multiple environments**

Deployment and management of multiple environments is now simplified. With previous releases, a customer had to deploy Cloud Manager instances in every desirable location. With the new release, the Cloud Manager agent is now renamed to *Connector*.

Users with multiple NetApp Cloud Central Accounts or Connectors can easily switch between different accounts and environments.

- **Public endpoint for API and UI**

With the new release you can access the API and GUI for your Cloud Manager securely via <https://cloudmanager.netapp.com>.

What will happen to the Cloud Manager instance deployed in my VPC/VNet?

As mentioned, the Cloud Manager instance deployed in a customer's network is now called a *Connector*.

The role of the Connector hasn't changed. It has the same purpose as before—to manage resources and processes within the customer's public cloud network.

Can I remove the Connector now that I am using the SaaS platform?

No, you should not. The Connector is the same software that was used to manage resources and processes

within your public cloud environments, such as deploying and managing Cloud Volumes ONTAP, enabling Cloud Backup Service, deploying Cloud Compliance, and more.

Can I still use my Cloud Manager the same way that I did before (locally through the instance deployed in my VPC)?

Yes, you can do that by clicking the **Connector** menu and clicking **Go to local UI** or by entering the Connector's IP address directly into your web browser.

Is a migration or any specific action required to move to Cloud Manager SaaS?

Nothing is needed. Just browse to <https://cloudmanager.netapp.com> and start working. Obviously, access to Cloud Manager is only granted to authorized users.

Did Cloud Volumes ONTAP or the data that it stores change or move anywhere?

No. It's where it's always been—in your VPC or VNet, under your management.

Where is the endpoint for the Cloud Manager SaaS platform?

It's operated securely by NetApp in the public cloud.

What kind of data or metadata is stored in the Cloud Manager SaaS service layer?

No data is stored in the Cloud Manager SaaS service layer.

The SaaS platform is used as a secure pipeline for API calls (HTTPS with a NetApp-signed certificate) between the user's web browser and the local Connector or the different NetApp services integrated into Cloud Manager.

What data or metadata is stored by the Connector that's deployed in the VPC/VNet?

The Connector/Cloud Manager has not changed. It's storing the same data that it did in the previous release. It only holds metadata required to manage resources and processes within your public cloud environments, such as deploying and managing Cloud Volumes ONTAP, enabling Cloud Backup Service, deploying and using Cloud Compliance, and more (see the [Learn about Connectors](#) page for the complete list of services).

What are the data and metadata paths?

Data from the Connector to the customer is transported via HTTPS, encrypted and signed by a NetApp certificate. The SaaS-based UI serves as a secure pipeline between the client web browser and the Connector. That means the data from the Connector can be accessed only by authorized users.

For customers utilizing the Cloud Compliance service, it is now encrypted end-to-end. The key exchange takes place between the web browser and the Connector, so NetApp can't read any of the data. [Learn more about Cloud Compliance](#).

Is there a GDPR impact when using the Cloud Compliance service through the SaaS endpoint?

The data is encrypted end-to-end. The key exchange takes place between the web browser and the Connector, so NetApp can't read any of the data.

What kind of network direction access is used for the SaaS-based UI and API to access the Connector?

- Communication from the customer's VPC/VNet to the SaaS-based UI is only *outbound*, which means it's only initiated by the Connector.
- The Connector polls for updates from the SaaS-based service tier on a secure channel.
- All API calls use authentication and authorization to ensure that access is secure.

This means that no additional ports/endpoints in your network need to be opened.

- Communication between the user's browser client and the SaaS-based UI uses HTTPS with a NetApp-signed certificate.

Has the login flow changed?

No, the login flow has stayed the same as the previous release. When a user logs in (SSO or credentials), they are authenticated against Auth0, just like before.

Note the following:

- If SSO or Federation is in place, the same security procedures that were being used are still in place. Access is federation at your company's facility. When utilizing federated access, you can add MFA (at your company's discretion) for heightened security.
- There are no changes to roles or permissions. Only users who are registered with the Cloud Central account can access the SaaS-based endpoints.
- Usage of Incognito Mode or a configuration where 3rd party cookies are not allowed in your client browser is currently not supported.

Is the SaaS-based Cloud Manager compliant (SOC2, FedRAMP, etc.)?

Cloud Manager is in the process of obtaining SOC2 certification.

To comply with FedRAMP certification, the SaaS-based UI is not enabled for customers who deploy a Cloud Manager Connector in Gov Cloud regions.

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.