



Information and Region

Cloud Insights

Tony Lavoie
April 02, 2021

This PDF was generated from https://docs.netapp.com/us-en/cloudinsights/security_information_and_region.html on October 26, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Information and Region 1
 - What information does Cloud Insights store? 1
 - Where is my information stored? 2
- More Information 2

Information and Region

NetApp takes the security of customer information very seriously. Here is how and where Cloud Insights stores your information.

What information does Cloud Insights store?

Cloud Insights stores the following information:

- Performance data

Performance data is time-series data providing information about the performance of the monitored device/source. This includes, for example, the number of IOs delivered by a storage system, the throughput of a FibreChannel port, the number of pages delivered by a web server, the response time of a database, and more.

- Inventory data

Inventory data consists of metadata describing the monitored device/source and how it is configured. This includes, for example, hardware and software versions installed, disks and LUNs in a storage system, CPU cores, RAM and disks of a virtual machine, the tablespaces of a database, the number and type of ports on a SAN switch, directory/file names (if Cloud Secure is enabled), etc.

- Configuration data

This summarizes customer-provided configuration data used to manage customer inventory and operations, e.g. hostnames or IP addresses of the monitored devices, polling intervals, timeout values, etc.

- Secrets

Secrets consist of the credentials used by the Cloud Insights Acquisition Unit to access customer devices and services. These credentials are encrypted using AES-256, and the private keys are stored only on the Acquisition Units and never leave the customer environment. Even privileged Cloud Insights SREs are unable to access customer secrets in plain-text due to this design.

- Functional Data

This is data generated as a result of NetApp providing the Cloud Data Service, which informs NetApp in the development, deployment, operations, maintenance, and securing of the Cloud Data Service. Functional Data does not contain Customer Information or Personal Information.

- User Access data

Authentication and access information that allows NetApp Cloud Central to communicate with regional Cloud Insights sites, including data related to user Authorization.

- Cloud Secure User Directory Data

In cases where the Cloud Secure functionality is enabled AND the customer chooses to enable the User Directory collector, the system will store user display names, corporate email addresses, and other information collected from Active Directory.



User Directory data refers to user directory information collected by the Cloud Secure User Directory data collector, not to data about the users of Cloud Insights/Cloud Secure themselves.

No explicit personal data is collected from infrastructure and services resources. Collected information consists of performance metrics, configuration information and infrastructure metadata only, much like many vendor phone-homes, including NetApp auto-support and ActiveIQ. However, depending on a customer's naming conventions, data for shares, volumes, VMs, qtrees, applications, etc. may contain personally identifiable information.

If Cloud Secure is enabled, the system additionally looks at file and directory names on SMB or other shares, which may contain personally identifiable information. Where customers enable the Cloud Secure User Directory Collector (which essentially maps Windows SIDs to usernames through Active Directory), the display name, corporate email address and any additional attributes selected will be collected and stored by Cloud Insights.

Additionally, access logs to Cloud Insights are maintained and contain users' IP and email addresses used to log into the service.

Where is my information stored?

Cloud Insights stores information according to the region in which your environment is created.

The following information is stored in the host region:

- Telemetry and asset/object information, including counters and performance metrics
- Acquisition Unit information
- Functional data
- Audit information on user activities inside Cloud Insights
- Cloud Secure Active Directory information
- Cloud Secure Audit information

The following information resides in the United States, regardless of the region hosting your Cloud Insights environment:

- Environment site (sometimes called "tenant") information such as site/account owner.
- Information that allows NetApp Cloud Central to communicate with regional Cloud Insights sites, including anything to do with user Authorization.
- Information related to the relation between the Cloud Insights user and the tenant.

More Information

You can read more about NetApp's privacy and security at the following links:

- [Trust Center](#)
- [Cross-Border Data Transfers](#)
- [Binding Corporate Rules](#)
- [Responding to Third-Party Data Requests](#)
- [NetApp Privacy Principles](#)

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.