



参考

NetApp Data Classification

NetApp

January 14, 2026

This PDF was generated from <https://docs.netapp.com/zh-cn/data-services-data-classification/reference-instance-types.html> on January 14, 2026. Always check docs.netapp.com for the latest.

目录

- 参考 1
 - 支持的NetApp Data Classification实例类型 1
 - AWS 实例类型 1
 - Azure 实例类型 1
 - GCP 实例类型 1
 - 从NetApp Data Classification中的数据源收集的元数据 2
 - 上次访问时间时间戳 2
 - 登录NetApp Data Classification系统 3
 - NetApp Data ClassificationAPI 3
 - 概述 4
 - 访问 Swagger API 参考 4
 - 使用 API 的示例 4

参考

支持的NetApp Data Classification实例类型

NetApp Data Classification软件必须在满足特定操作系统要求、RAM 要求、软件要求等的主机上运行。在云中部署数据分类时，我们建议您使用具有“大型”特性的系统以实现全部功能。

您可以在具有较少 CPU 和较少 RAM 的系统上部署数据分类，但在使用这些功能较弱的系统时会受到一些限制。[了解这些限制](#)。

在下表中，如果标记为“默认”的系统在您安装数据分类的区域中不可用，则将部署表中的下一个系统。

AWS 实例类型

系统大小	规格	实例类型
特大号	32 个 CPU、128 GB RAM、1 TiB gp3 SSD	"m6i.8xlarge" （默认）
大型	16 个 CPU、64 GB RAM、500 GiB SSD	"m6i.4xlarge" （默认） m6a.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
中	8 个 CPU、32 GB RAM、200 GiB SSD	"m6i.2xlarge" （默认） m6a.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
小型	8 个 CPU、16 GB RAM、100 GiB SSD	"c6a.2xlarge" （默认） c5a.2xlarge c5.2xlarge c4.2xlarge

Azure 实例类型

系统大小	规格	实例类型
特大号	32 个 CPU、128 GB RAM、OS 磁盘（2,048 GiB，最小吞吐量 250 MB/s）和数据磁盘（1 TiB SSD，最小吞吐量 750 MB/s）	"Standard_D32_v3" （默认）
大型	16 个 CPU、64 GB RAM、500 GiB SSD	"Standard_D16s_v3" （默认）

GCP 实例类型

系统大小	规格	实例类型
大型	16 个 CPU、64 GB RAM、500 GiB SSD	"n2-标准-16" （默认） n2d-standard-16 n1-standard-16

从NetApp Data Classification中的数据源收集的元数据

NetApp Data Classification在对来自数据源和系统的数据执行分类扫描时收集某些元数据。数据分类可以访问我们对数据进行分类所需的大部分元数据，但有些来源我们无法访问所需的数据。

	元数据	CIFS	NFS
时间戳	创建时间	可用	不可用（Linux 不支持）
	上次访问时间	可用	可用
	上次修改时间	可用	可用
权限	开放权限	如果“EVERYONE”组有权访问该文件，则视为“对组织开放”	如果“其他人”有权访问该文件，则视为“对组织开放”
	用户/组访问	用户和组信息取自 LDAP	不可用（NFS 用户通常在服务器本地进行管理，因此同一个人每个服务器上可以有不同的 UID）



- 数据分类不会从数据库数据源中提取“上次访问时间”。
- 旧版本的 Windows 操作系统（例如 Windows 7 和 Windows 8）默认禁用“上次访问时间”属性的收集，因为它会影响系统性能。当未收集此属性时，基于“上次访问时间”的数据分类分析将受到影响。如果需要，您可以在这些较旧的 Windows 系统上启用上次访问时间的收集。

上次访问时间时间戳

当数据分类从文件共享中提取数据时，操作系统会将其视为访问数据，并相应地更改“上次访问时间”。扫描后，数据分类会尝试将上次访问时间恢复为原始时间戳。如果数据分类在 CIFS 中没有写入属性权限，或者在 NFS 中没有写入权限，则系统无法将上次访问时间恢复为原始时间戳。配置了 SnapLock 的 ONTAP 卷具有只读权限，并且无法将上次访问时间恢复为原始时间戳。

默认情况下，如果数据分类没有这些权限，系统将不会扫描卷中的这些文件，因为数据分类无法将“上次访问时间”恢复为原始时间戳。但是，如果您不介意文件中的最后访问时间是否重置为原始时间，则可以选择配置页面底部的*缺少“写入属性”权限时扫描*开关，以便数据分类无论权限如何都会扫描卷。

SMB_Shares Scan Configuration

2 Shares selected

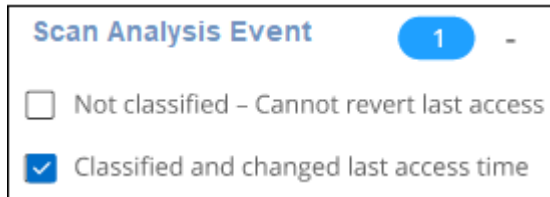
Scan when missing "write" permissions ☐

+ Add Shares Edit CIFS Credentials

Scan	Storage Repository (Share)	Protocol	Access	Scan Status	Required Action
Map Map & Classify	\\10.1.7.16\CIFS_LABS_SHARE6	CIFS	Continuously Scanning	Mapped: 5.8K Classified: 5.8K	...
Map Map & Classify	\\10.1.7.16\CIFS_LABS_SHARE7	CIFS	Continuously Scanning	Mapped: 5.8K Classified: 5.8K	...

此功能适用于本地 ONTAP 系统、Cloud Volumes ONTAP、Azure NetApp Files、Amazon FSx for NetApp ONTAP 管理和第三方文件共享。

调查页面中有一个名为“扫描分析事件”的过滤器，它使您能够显示未分类的文件（因为数据分类无法恢复上次访问时间），或者即使数据分类无法恢复上次访问时间也已分类的文件。

A UI element for the 'Scan Analysis Event' filter. It has a title 'Scan Analysis Event' followed by a blue circle containing the number '1' and a minus sign. Below the title are two checkboxes. The first checkbox is unchecked and labeled 'Not classified - Cannot revert last access'. The second checkbox is checked and labeled 'Classified and changed last access time'.

过滤器选择包括：

- “未分类 - 无法恢复上次访问时间” - 这显示由于缺少写入权限而未分类的文件。
- “已分类并更新的上次访问时间” - 这显示已分类的文件，并且数据分类无法将上次访问时间重置回原始日期。此过滤器仅与您打开*缺少“写入属性”权限时扫描*的环境相关。

如果需要，您可以将这些结果导出到报告中，以便查看哪些文件由于权限原因而被扫描，哪些文件未被扫描。[了解有关数据调查报告的更多信息](#)。”

登录NetApp Data Classification系统

您需要登录NetApp Data Classification系统，以便访问日志文件或编辑配置文件。

当数据分类安装在您本地的 Linux 机器上或在云中部署的 Linux 机器上时，您可以直接访问配置文件和脚本。

当数据分类部署在云中时，您需要通过 SSH 连接到数据分类实例。您可以通过输入用户和密码，或使用控制台代理安装期间提供的 SSH 密钥，通过 SSH 连接到系统。SSH 命令是：

```
ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
```

- <path_to_the_ssh_key>= ssh 身份验证密钥的位置
- <machine_user>:
 - 对于 AWS：使用 <ec2-user>
 - 对于 Azure：使用为控制台实例创建的用户
 - 对于 GCP：使用为控制台实例创建的用户
- <datasense_ip>= 虚拟机实例的 IP 地址

需要修改安全组入站规则才能访问云端的系统。有关详细信息，请参阅：

- ["AWS 中的安全组规则"](#)
- ["Azure 中的安全组规则"](#)
- ["Google Cloud 中的防火墙规则"](#)

NetApp Data ClassificationAPI

通过 Web UI 提供的NetApp Data Classification功能也可通过 REST API 提供。

数据分类中定义了四个类别，与 UI 中的选项卡相对应：

- 调查
- Compliance
- 治理
- 配置

Swagger 文档中的 API 允许您搜索、聚合数据、跟踪扫描以及执行复制、移动和删除等操作。

概述

该 API 使您能够执行以下功能：

- 导出信息
 - UI 中可用的所有内容都可以通过 API 导出（报告除外）
 - 数据以 JSON 格式导出（易于解析并推送到第三方应用程序，如 Splunk）
- 使用“AND”和“OR”语句创建查询，包括和排除信息等等。

例如，您可以找到没有特定个人身份信息 (PII) 的文件（UI 中不可用的功能）。您还可以排除导出操作的特定字段。

- 执行操作
 - 更新 CIFS 凭证
 - 查看和取消操作
 - 重新扫描目录
 - 导出数据

API 是安全的，它使用与 UI 相同的身份验证方法。您可以在["REST API 文档"](#)。

访问 Swagger API 参考

要进入 Swagger，您需要数据分类实例的 IP 地址。对于云部署，您将使用公共 IP 地址。然后您需要进入这个端点：

`https://<classification_ip>/documentation`

使用 API 的示例

以下示例显示了复制文件的 API 调用。

API 请求

您最初需要获取系统的所有相关字段和选项，以查看调查选项卡中的所有过滤器。

```
curl -X GET "http://{classification_ip}/api/{classification_version}
/search/options?data_mode=ALL_EXTRACTABLE" -H "accept: application/json"
-H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR..... " -H "x-agent-id:
hOXsZNvnA5LsthwMILtjL9xZFyBQxAwMclients"
```

响应

```
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "string",
      "is_rulable": true,
      "name": "string",
      "operators": [
        "EQUALS"
      ],
      "optional_values": [
        {}
      ],
      "secondary": {},
      "server_data": false,
      "type": "TEXT"
    }
  ]
}
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "POLICIES",
      "name": "Policies",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "EXTRACTION_STATUS_RANGE",
```

```

    "name": "Scan Analysis Status",
    "operators": [
        "IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "SCAN_ANALYSIS_ERROR",
    "name": "Scan Analysis Event",
    "operators": [
        "IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "PUBLIC_ACCESS",
    "name": "Open Permissions",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": true,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "USERS_PERMISSIONS_COUNT_RANGE",
    "name": "Number of Users with Access",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": true,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "USER_GROUP_PERMISSIONS",

```

```

    "name": "User / Group Permissions",
    "operators": [
        "IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "FILE_OWNER",
    "name": "File Owner",
    "operators": [
        "EQUALS",
        "CONTAINS"
    ],
    "server_data": true,
    "type": "TEXT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "ENVIRONMENT_TYPE",
    "name": "system-type",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "ENVIRONMENT",
    "name": "system",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_SCANNED",

```

```

    "field": "SCAN_TASK",
    "name": "Storage Repository",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "FILE_PATH",
    "name": "File / Directory Path",
    "operators": [
        "MULTI_CONTAINS",
        "MULTI_EXCLUDE"
    ],
    "server_data": true,
    "type": "MULTI_TEXT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_DASHBOARD_EXTRACTABLE",
    "field": "CATEGORY",
    "name": "Category",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "PATTERN_SENSITIVITY_LEVEL",
    "name": "Sensitivity Level",
    "operators": [
        "IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,

```

```

    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "NUMBER_OF_IDENTIFIERS",
    "name": "Number of identifiers",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "PATTERN_PERSONAL",
    "name": "Personal Data",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "PATTERN_SENSITIVE",
    "name": "Sensitive Personal Data",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "DATA_SUBJECT",
    "name": "Data Subject",
    "operators": [
        "EQUALS",
        "CONTAINS"
    ],
    "server_data": true,
    "type": "TEXT"
},

```

```

{
  "active_directory_affected": false,
  "data_mode": "DIRECTORIES",
  "field": "DIRECTORY_TYPE",
  "name": "Directory Type",
  "operators": [
    "IN",
    "NOT_IN"
  ],
  "server_data": true,
  "type": "SELECT"
},
{
  "active_directory_affected": false,
  "data_mode": "ALL_EXTRACTABLE",
  "field": "FILE_TYPE",
  "name": "File Type",
  "operators": [
    "IN",
    "NOT_IN"
  ],
  "server_data": true,
  "type": "SELECT"
},
{
  "active_directory_affected": false,
  "data_mode": "ALL_EXTRACTABLE",
  "field": "FILE_SIZE_RANGE",
  "name": "File Size",
  "operators": [
    "IN",
    "NOT_IN"
  ],
  "server_data": true,
  "type": "SELECT"
},
{
  "active_directory_affected": false,
  "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
  "field": "FILE_CREATION_RANGE_RETENTION",
  "name": "Created Time",
  "operators": [
    "IN"
  ],
  "server_data": true,
  "type": "SELECT"
}

```

```

},
{
  "active_directory_affected": false,
  "data_mode": "ALL_EXTRACTABLE",
  "field": "DISCOVERED_TIME_RANGE",
  "name": "Discovered Time",
  "operators": [
    "IN"
  ],
  "server_data": true,
  "type": "SELECT"
},
{
  "active_directory_affected": false,
  "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
  "field": "FILE_LAST_MODIFICATION_RETENTION",
  "name": "Last Modified",
  "operators": [
    "IN"
  ],
  "server_data": true,
  "type": "SELECT"
},
{
  "active_directory_affected": false,
  "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
  "field": "FILE_LAST_ACCESS_RANGE_RETENTION",
  "name": "Last Accessed",
  "operators": [
    "IN"
  ],
  "server_data": true,
  "type": "SELECT"
},
{
  "active_directory_affected": false,
  "data_mode": "FILES",
  "field": "IS_DUPLICATE",
  "name": "Duplicates",
  "operators": [
    "EQUALS",
    "IN"
  ],
  "server_data": true,
  "type": "SELECT"
},

```

```

{
  "active_directory_affected": false,
  "data_mode": "FILES",
  "field": "FILE_HASH",
  "name": "File Hash",
  "operators": [
    "EQUALS",
    "IN"
  ],
  "server_data": true,
  "type": "TEXT"
},
{
  "active_directory_affected": false,
  "data_mode": "ALL_EXTRACTABLE",
  "field": "USER_DEFINED_STATUS",
  "name": "Tags",
  "operators": [
    "IN",
    "NOT_IN"
  ],
  "server_data": true,
  "type": "SELECT"
},
{
  "active_directory_affected": false,
  "data_mode": "ALL_EXTRACTABLE",
  "field": "ASSIGNED_TO",
  "name": "Assigned to",
  "operators": [
    "IN",
    "NOT_IN"
  ],
  "server_data": true,
  "type": "SELECT"
}
]
}

```

我们将在请求参数中使用该响应来过滤我们想要复制的文件。

您可以对多个项目应用一个操作。支持的操作类型包括：移动、删除和复制。

我们将创建复制动作：

API 请求

下一个 API 是操作 API，它允许您创建多个操作。

```
curl -X POST "http://
{classification_ip}/api/{classification_version}/actions" -H "accept:
application/json" -H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR..... "
-H "x-agent-id: hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients " -H "Content-
Type: application/json" -d "{ \"action_type\": \"COPY\", \"data_mode\":
\"FILES\", \"policy_id\": 0, \"request_params\": { destination_nfs_path:
\"{ontap_ip}/{share_name} \" },
\"requested_query\":{\"condition\":\"AND\",\"rules\":[{\"field\":\"ENVIRONMENT_TYPE
\",\"operator\":\"IN\",\"value\":[\"ONPREM\"]},{\"field\":\"CATEGORY\",\"operator\":\"IN\",
\"value\":[\"21\"]}]}}"
```

响应

响应将返回操作对象，因此您可以使用获取和删除 API 来获取有关操作的状态，或取消它。

```
{
  "action_type": "COPY",
  "creation_time": "2023-08-08T12:37:21.705Z",
  "data_mode": "FILES",
  "end_time": "2023-08-08T12:37:21.705Z",
  "estimated_time_to_complete": 0,
  "id": 0,
  "policy_id": 0,
  "policy_name": "string",
  "priority": 0,
  "request_params": {},
  "requested_query": {},
  "result": {
    "error_message": "string",
    "failed": 0,
    "in_progress": 0,
    "succeeded": 0,
    "total": 0
  },
  "start_time": "2023-08-08T12:37:21.705Z",
  "status": "QUEUED",
  "title": "string",
  "user_id": "string"
}
```

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。