使用資料分類
NetApp Data Classification

NetApp
February 11, 2026

目錄

使用資料分類

使用NetApp Data Classification查看組織中儲存的資料的治理詳細信息

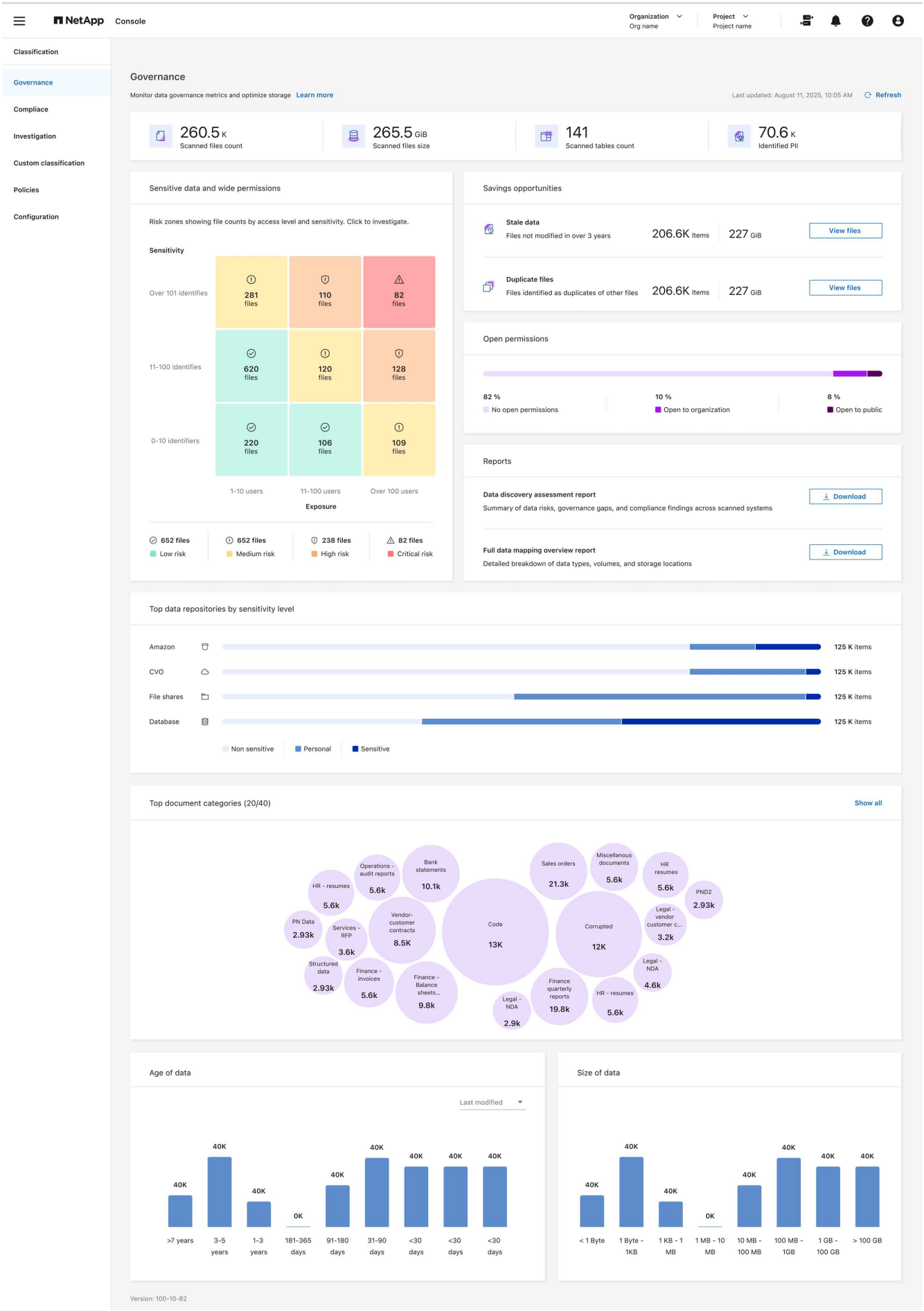
控制與組織儲存資源上的資料相關的成本。 NetApp Data Classification可識別系統中陳舊資料、重複檔案和超大檔案的數量，以便您可以決定是否要刪除某些檔案或將某些檔案分層到成本較低的物件儲存中。

您應該從這裡開始您的研究。從治理儀表板中，您可以選擇一個區域進行進一步調查。

此外，如果您打算將資料從本地位置遷移到雲端，則可以在移動資料之前查看資料的大小以及其中是否有任何資料包含敏感資訊。

查看治理儀表板

治理儀表板提供信息，以便您可以提高效率並控制與儲存在儲存資源上的資料相關的成本。


NetApp Console
Organization
Org name
Project
Project name
Classification
Governance
Compliace
Investigation
Custom classification
Policies
Configuration
Governance
Monitor data governance metrics and optimize storage Learn more
Last updated: August 11, 2025, 10:05 AM
Refresh
260.5 K
Scanned files count
265.5 GiB
Scanned files size
141
Scanned tables count
70.6 K
Identified PII
Sensitive data and wide permissions
Risk zones showing file counts by access level and sensitivity. Click to investigate.
Sensitivity
Over 101 identifies
11-100 identifies
0-10 identifiers
281 files
110 files
82 files
620 files
120 files
128 files
220 files
106 files
109 files
1-10 users
11-100 users
Over 100 users
Exposure
652 files
Low risk
652 files
Medium risk
238 files
High risk
82 files
Critical risk
Savings opportunities
Stale data
Files not modified in over 3 years
206.6K Items
227 GiB
View files
Duplicate files
Files identified as duplicates of other files
206.6K Items
227 GiB
View files
Open permissions
82 %
No open permissions
10 %
Open to organization
8 %
Open to public
Reports
Data discovery assessment report
Summary of data risks, governance gaps, and compliance findings across scanned systems
Download
Full data mapping overview report
Detailed breakdown of data types, volumes, and storage locations
Download
Top data repositories by sensitivity level
Amazon
CVO
File shares
Database
125 K items
Non sensitive
Personal
Sensitive
Top document categories (20/40)
Show all
Operations - audit reports 5.6k
Bank statements 10.1k
Sales orders 21.3k
Miscellanous documents 5.6k
HR resumes 5.6k
PND2 2.93k
HR - resumes 5.6k
PN Data 2.93k
Services - RFP 3.6k
Vendor-customer contracts 8.5K
Code 13K
Corrupted 12K
Legal - vendor customer c... 3.2k
Structured data 2.93k
Finance - invoices 5.6k
Finance - Balance sheets... 9.8k
Legal - NDA 2.9k
Finance quarterly reports 19.8k
HR - resumes 5.6k
Legal - NDA 4.6k
Age of data
Last modified
40K
>7 years
40K
3-5 years
40K
1-3 years
0K
181-365 days
40K
91-180 days
40K
31-90 days
40K
<30 days
40K
<30 days
40K
<30 days
Size of data
40K
< 1 Byte
40K
1 Byte - 1KB
40K
1 KB - 1 MB
0K
1 MB - 10 MB
40K
10 MB - 100 MB
40K
100 MB - 1GB
40K
1 GB - 100 GB
40K
> 100 GB
Version: 100-10-82

步驟

1. 從NetApp Console選單中，選擇 治理 **>** 分類。
2. 選擇*治理*。

   出現治理儀表板。

檢討節省機會

_節省機會_元件顯示您可以刪除或分層到較便宜的物件儲存的資料。 《節省機會》中的數據每 2 小時更新一次。您也可以手動更新資料。

步驟

1. 從資料分類選單中，選擇*治理*。
2. 在治理儀表板的每個節省機會圖塊中，選擇*最佳化儲存*以在調查頁面中查看過濾的結果。要發現您應該刪除或分層到較便宜的存儲的任何數據，請調查_節省機會_。
   - 過期資料 - 預設情況下，如果資料上次修改超過 3 年，則該資料視為過期資料。您可以[自訂過期資料的定義](task-stale-data.html)。
   - 重複檔案 - 您正在掃描的資料來源中其他位置重複的檔案。"查看顯示的重複檔案類型" 。

如果您的任何資料來源實現了資料分層，則可以在「陳舊資料」類別中識別已經駐留在物件儲存中的舊資料。

建立數據發現評估報告

數據發現評估報告對掃描環境進行了高級分析，以顯示關注區域和潛在的補救步驟。結果基於數據的映射和分類。本報告的目標是提高您對資料集三個重要面向的認識：

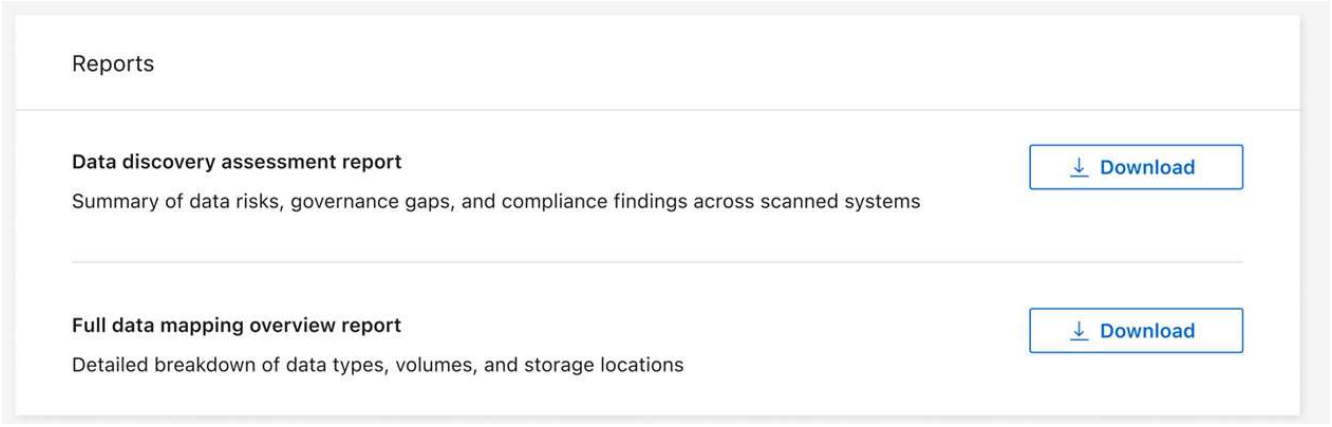
特徵	描述
資料治理問題	您擁有的所有數據以及可以減少數據量以節省成本的區域的詳細圖片。
資料安全風險	由於存取權限廣泛，您的資料可能受到內部或外部攻擊的區域。
數據合規性差距	您的個人或敏感個人資訊位於何處，以滿足安全和 DSAR（資料主體存取請求）。

透過該報告，您可以採取以下行動：

- 透過更改保留策略或移動或刪除某些資料（陳舊或重複的資料）來降低儲存成本。
- 透過修改全域群組管理策略來保護具有廣泛權限的資料。
- 透過將 PII 移至更安全的資料儲存來保護包含個人或敏感個人資訊的資料。

步驟

1. 從資料分類中，選擇*治理*。
2. 在報告圖塊中，選擇「資料發現評估報告」。



結果

資料分類會產生一份您可以檢視和分享的 PDF 報告。

建立資料映射概覽報告

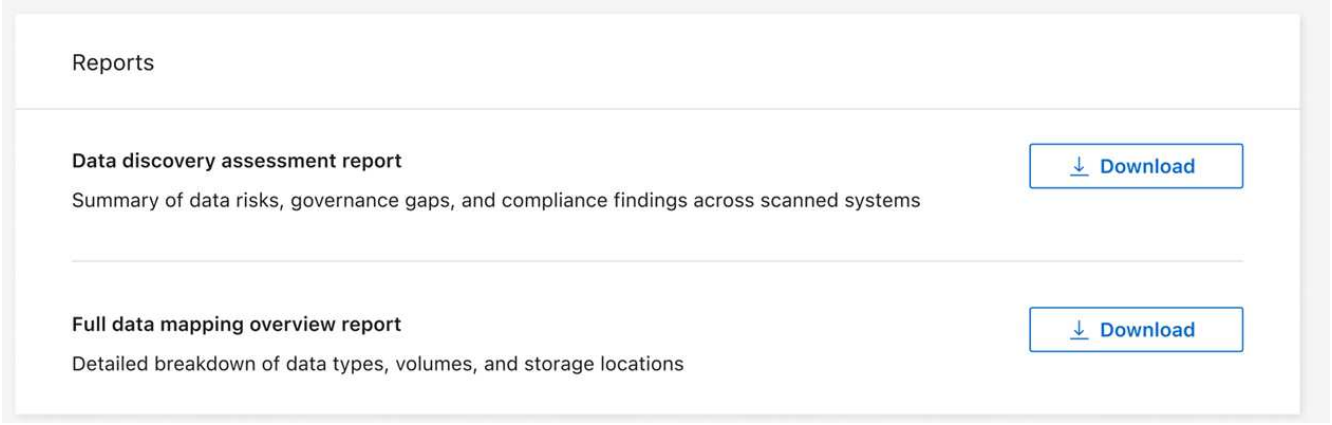
資料映射概覽報告提供了儲存在公司資料來源中的資料的概覽，以協助您做出遷移、備份、安全性和合規性流程的決策。該報告總結了所有系統和資料來源。它還為每個系統提供了分析。

該報告包含以下資訊：

類別	描述
使用容量	對於所有系統：列出每個系統的檔案數量和已使用容量。對於單一系統：列出使用最多容量的檔案。
數據時代	提供三個圖表和圖形，分別表示檔案的建立時間、上次修改時間或上次造訪時間。根據特定日期範圍列出文件數量及其已使用容量。
數據大小	列出系統中存在於特定大小範圍內的檔案數。

步驟

1. 從資料分類中，選擇*治理*。
2. 在報告圖塊中，選擇*完整資料映射概覽報告*。



結果

資料分類會產生一份 PDF 報告，您可以根據需要查看並傳送給其他群組。

如果報告大於 1 MB，則 PDF 檔案將保留在資料分類實例上，您將看到有關確切位置的彈出訊息。當資料分類安裝在您本機的 Linux 機器上或在雲端部署的 Linux 機器上時，您可以直接導覽至 PDF 檔案。當資料分類部署在雲端時，您需要使用 SSH 授權資料分類實例下載 PDF 檔案。

查看按資料敏感度列出的頂級資料儲存庫

資料映射概覽報告中的「按敏感度等級排列的頂級資料儲存庫」區域列出了包含最敏感項目的前四個資料儲存庫（系統和資料來源）。每個系統的長條圖分為：

- 非敏感數據
- 個人資料
- 敏感個人數據

數據每兩小時刷新一次，可以手動刷新。

步驟

1. 若要查看每個類別中的項目總數，請將遊標放在欄的每個部分上。
2. 若要過濾調查頁面中顯示的結果，請選擇欄中的每個區域並進一步調查。

審查敏感數據和廣泛的權限

治理儀表板的「敏感資料和廣泛權限」區域顯示包含敏感資料和具有廣泛權限的檔案的數量。此表顯示以下類型的權限：

- 從橫軸上最嚴格的權限到最寬鬆的限制。
- 縱軸上從最不敏感的資料到最敏感的資料。

步驟

1. 若要查看每個類別中的檔案總數，請將遊標放在每個方塊上。
2. 若要過濾調查頁面中顯示的結果，請選擇一個方塊並進一步調查。

查看按開放權限類型列出的數據

資料映射概覽報表的「開啟權限」區域顯示正在掃描的所有檔案中每種權限的百分比。此圖表顯示以下類型的權限：

- 無開放權限
- 向組織開放
- 對外開放
- 未知訪問

步驟

1. 若要查看每個類別中的檔案總數，請將遊標放在每個方塊上。
2. 若要過濾調查頁面中顯示的結果，請選擇一個方塊並進一步調查。

審查資料的年齡和大小

您可以調查資料對應概覽報表的「*Age*」和「*Size*」圖表中的項目，看看是否有任何資料應該刪除或分層到較便宜的物件儲存。

步驟

1. 在資料年齡圖表中，要查看有關資料年齡的詳細信息，請將遊標放在圖表中的某個點上。
2. 若要依年齡或尺寸範圍進行過濾，請選擇該年齡或尺寸。
   - 資料年齡圖 - 根據資料建立時間、上次造訪時間或上次修改時間對資料進行分類。
   - 資料大小圖 - 根據大小將資料分類。

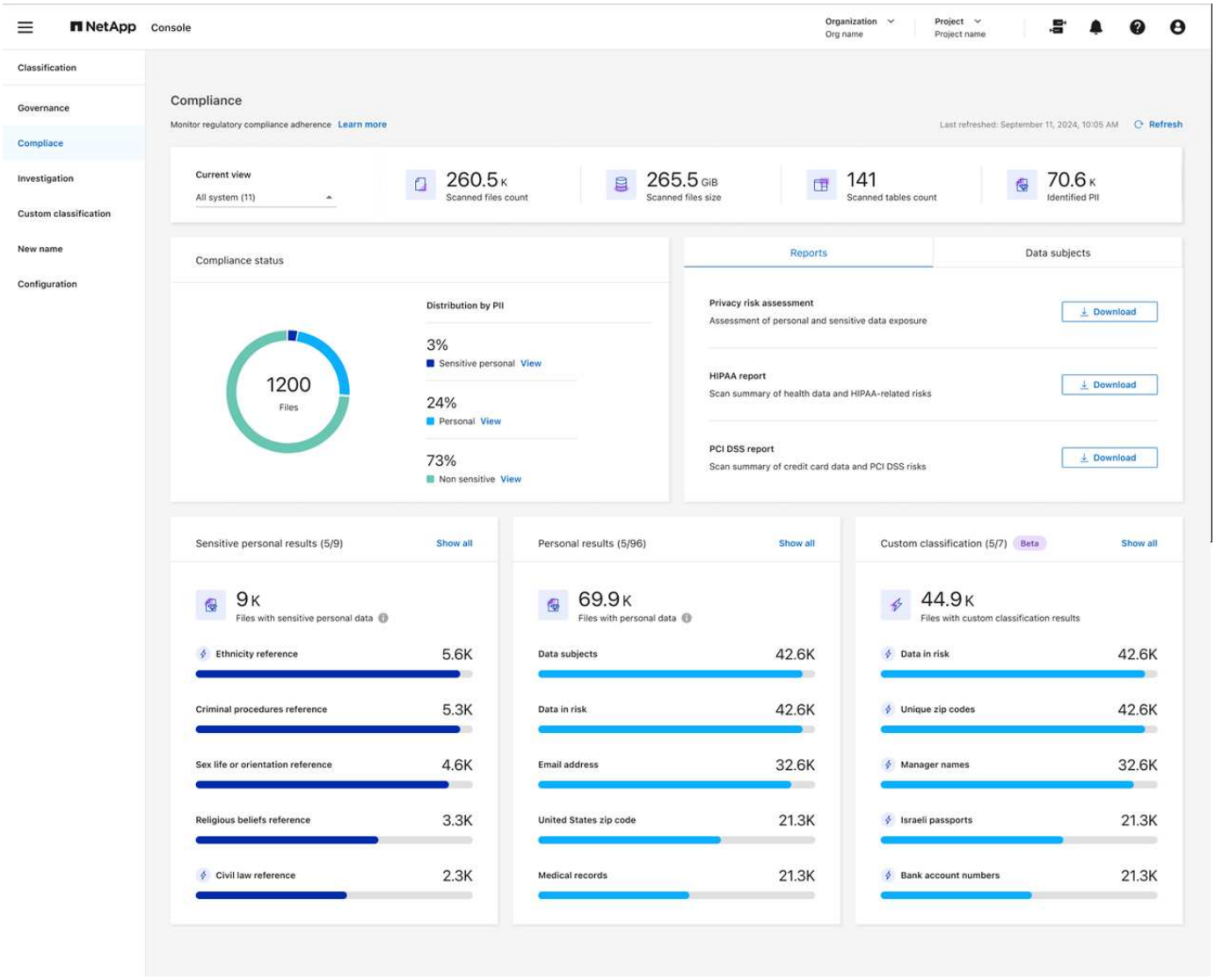
如果您的任何資料來源實現了資料分層，則已駐留在物件儲存中的舊資料可能會在「資料年齡」圖中被識別。

使用NetApp Data Classification查看組織中儲存的私人資料的合規性詳細信息

透過查看組織中的個人資料 (PII) 和敏感個人資料 (SPII) 的詳細資訊來控制您的私人資料。您也可以透過查看NetApp Data Classification在您的資料中找到的類別和檔案類型來獲得可見性。

只有當您執行完整分類掃描時，才可獲得文件級合規性詳細資訊。僅映射掃描不會產生文件級詳細資訊。

預設情況下，資料分類儀表板顯示所有系統和資料庫的合規性資料。若要僅查看部分系統的數據，請選擇它們。



您可以從資料調查頁面過濾結果，並將結果報告下載為 CSV 檔案。看"在資料調查頁面中過濾數據"了解詳情。

查看包含個人資料的文件

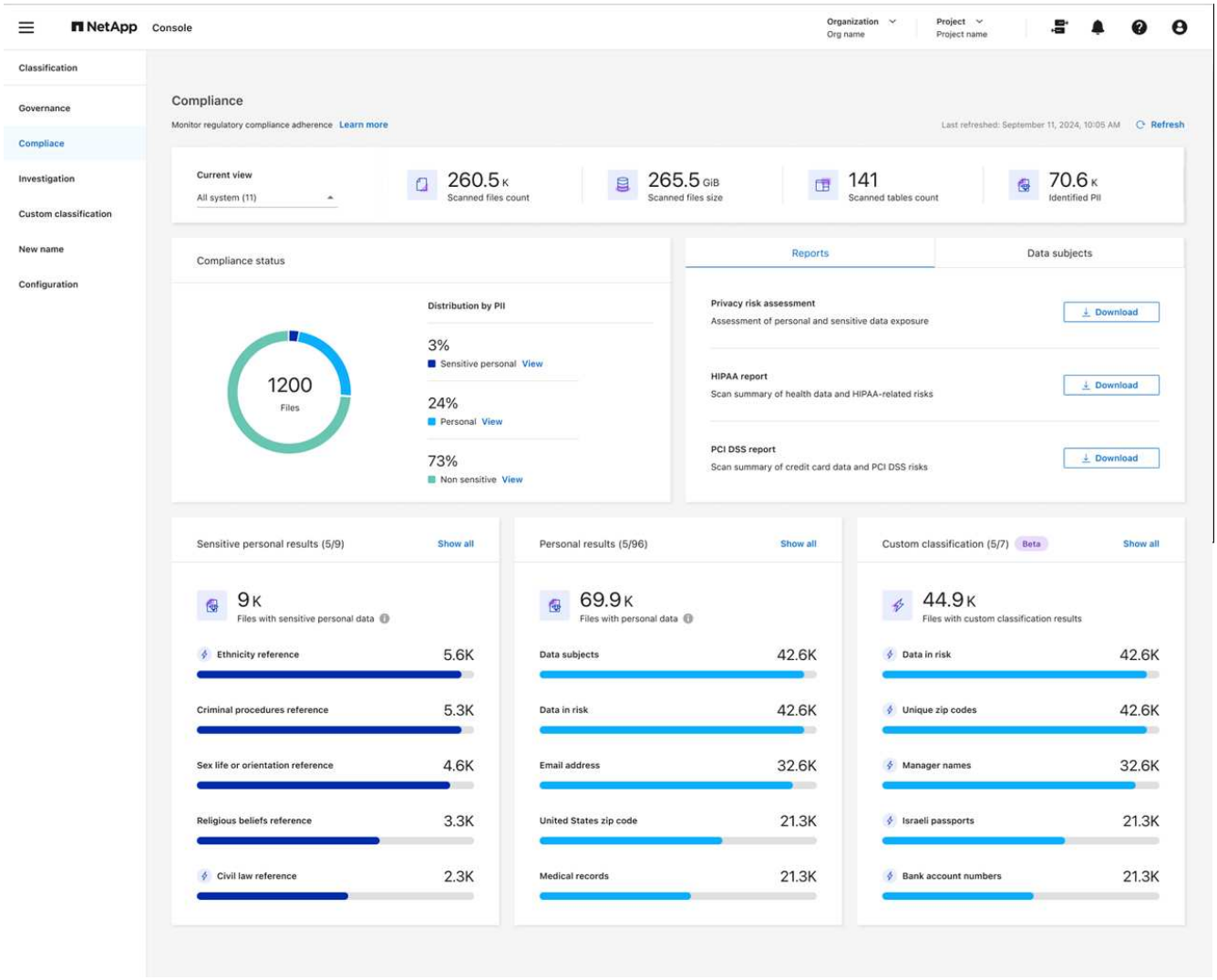
資料分類會自動識別資料中的特定單字、字串和模式（正規表示式）。"例如，信用卡號、社會安全號碼、銀行帳號、密碼等等。"資料分類可在單一檔案、目錄（共用和資料夾）內的檔案以及資料庫表中識別此類資訊。

您也可以建立自訂搜尋字詞來識別特定於您組織的個人資料。有關更多信息，請參閱"建立自訂分類" 。

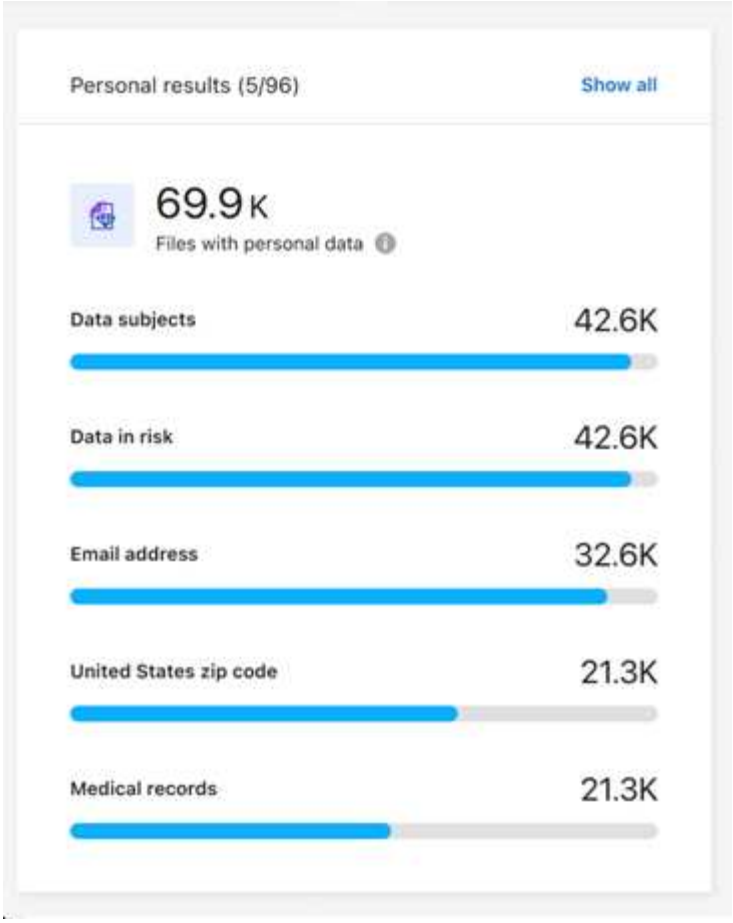
對於某些類型的個人數據，資料分類使用_鄰近驗證_來驗證其發現。透過尋找與找到的個人資料接近的一個或多個預定義關鍵字來進行驗證。例如，如果資料分類看到旁邊有一個近似詞（例如，*SSN* 或 *social security*），它就會將美國社會安全號碼 (SSN) 識別為 SSN。"個人資料表"顯示資料分類何時使用鄰近驗證。

步驟

1. 從資料分類選單中，選擇“合規性”標籤。
2. 要調查所有個人資料的詳細信息，請選擇個人資料百分比旁邊的圖示。

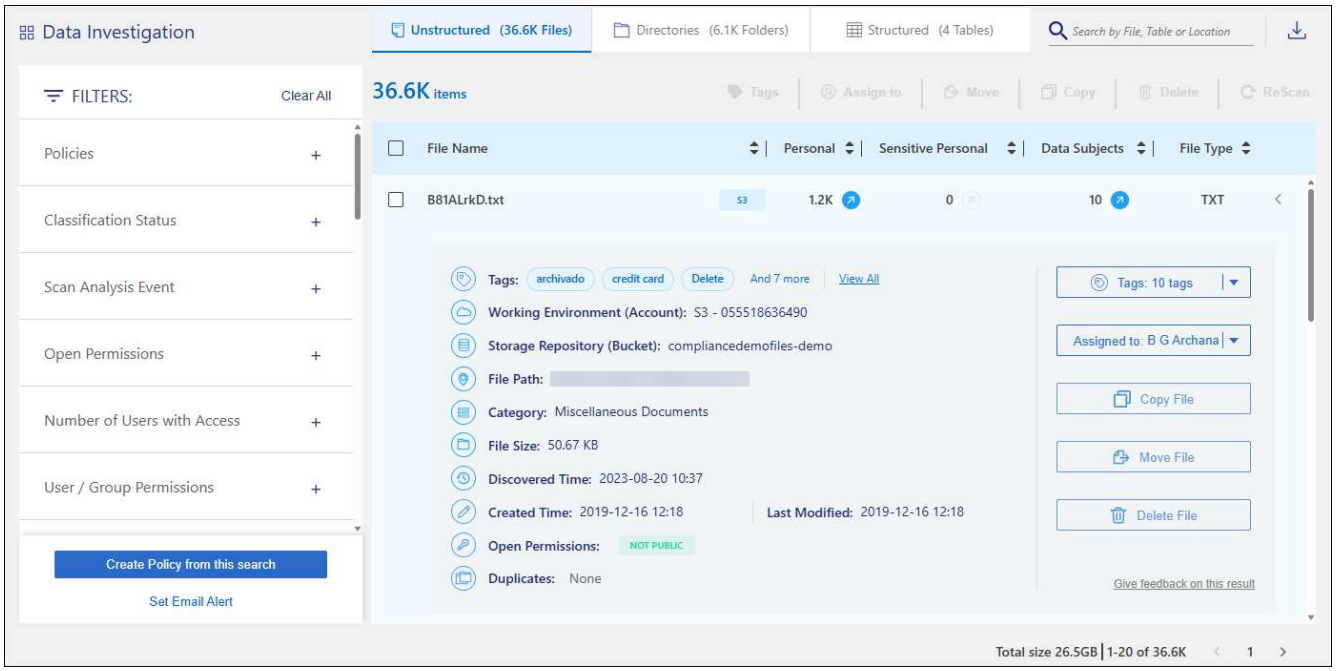


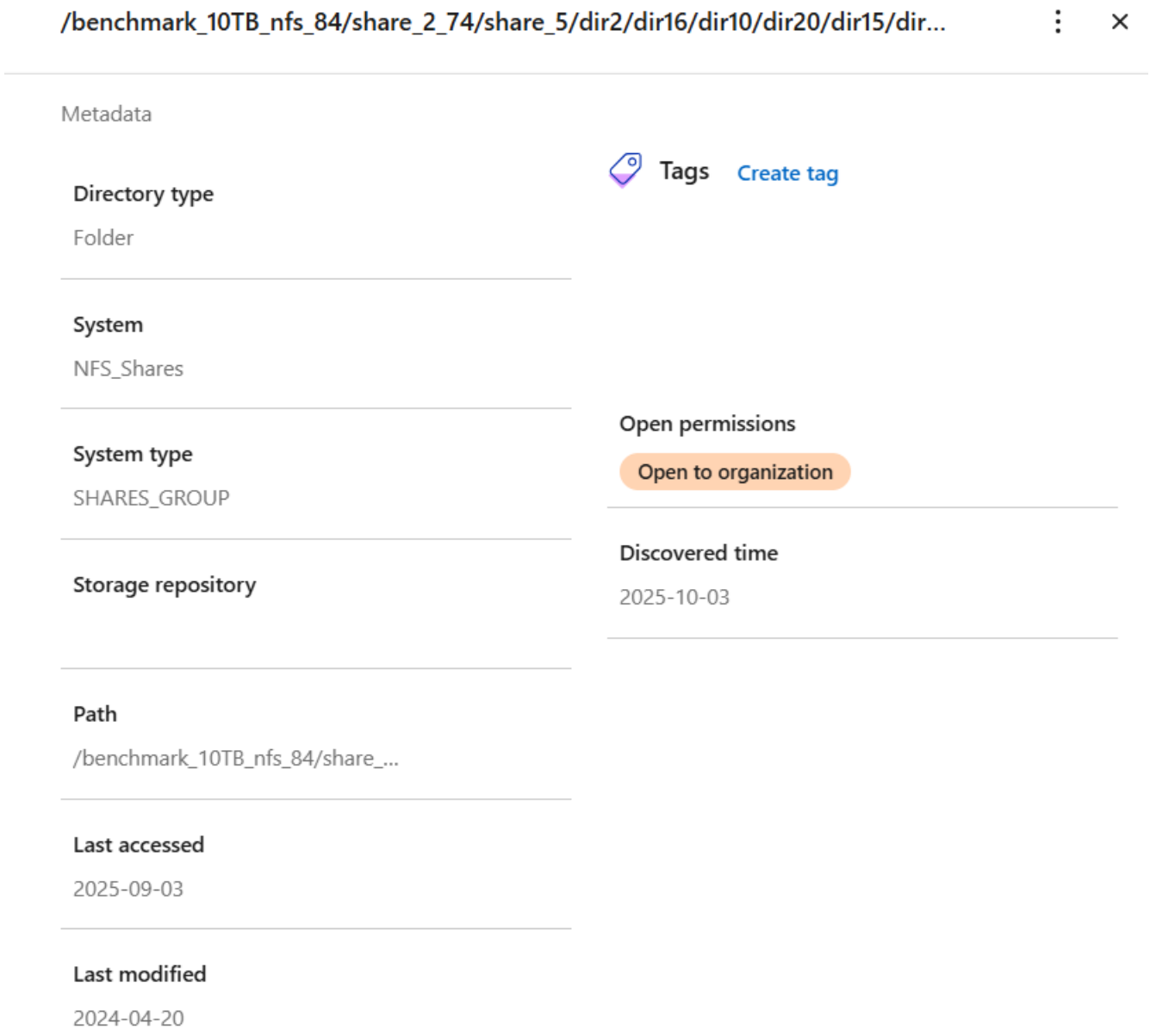
3. 要調查特定類型的個人資料的詳細信息，請選擇*查看全部*，然後選擇特定類型的個人資料（例如電子郵件地址）的*調查結果*箭頭圖示。



4. 透過搜尋、排序、擴展特定文件的詳細資訊、選擇「調查結果」箭頭查看屏蔽資訊或下載文件列表來調查資料。

   下圖顯示在目錄（共享和資料夾）中找到的個人資料。在「結構化」標籤中，您可以查看資料庫中的個人資料。在「非結構化」標籤中，您可以查看檔案層級資料。





查看包含敏感個人資料的文件

資料分類會自動識別隱私法規所定義的特殊類型的敏感個人資訊，例如 "GDPR 第 9 條和第 10 條"。例如，有關一個人的健康、種族或性取向的資訊。"查看完整列表" 。資料分類可在單一檔案、目錄（共用和資料夾）內的檔案以及資料庫表中識別此類資訊。

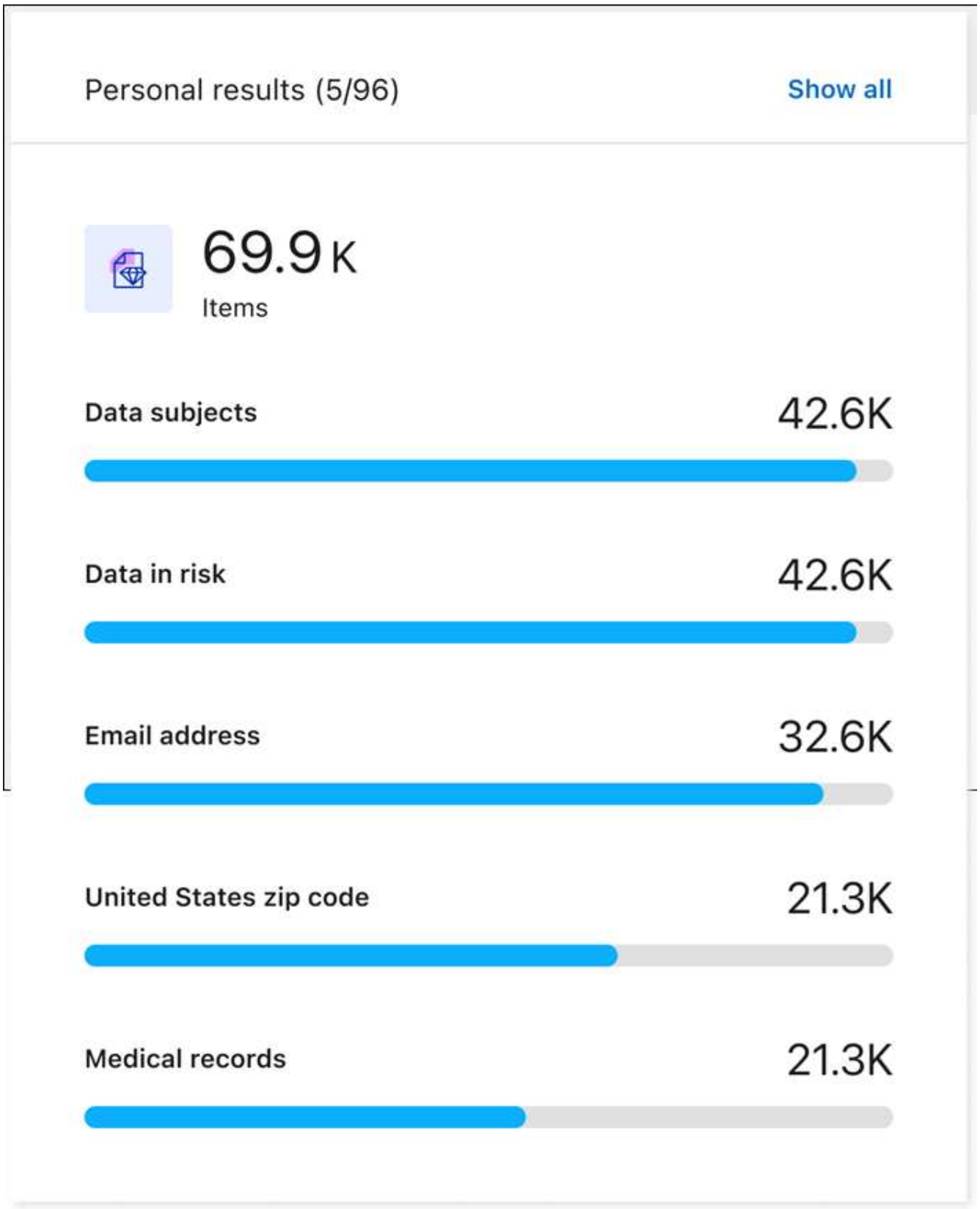
資料分類使用人工智慧、自然語言處理 (NLP)、機器學習 (ML) 和認知運算 (CC) 來理解其掃描的內容的含義，以便提取實體並對其進行相應的分類。

例如，GDPR 資料的一個敏感類別是種族來源。由於其 NLP 能力，資料分類可以區分「喬治是墨西哥人」（表示 GDPR 第 9 條規定的敏感資料）和「喬治正在吃墨西哥食物」之間的區別。

掃描敏感個人資料時僅支援英文。稍後將添加對更多語言的支援。

步驟

1. 從資料分類選單中，選擇*合規性*。
2. 要調查所有敏感個人資料的詳細信息，請找到敏感個人資訊結果卡，然後選擇顯示全部。



。

3. 要調查特定類型的敏感個人資料的詳細信息，請選擇“查看全部”，然後選擇特定類型的敏感個人資料的“調查結果”箭頭圖示。
4. 透過搜尋、排序、擴展特定文件的詳細資訊、點擊「調查結果」查看封鎖資訊或下載文件清單來調查資料。

NetApp Data Classification中的私有資料類別

NetApp Data Classification可在您的磁碟區和資料庫中識別多種類型的私有資料。

資料分類識別兩種類型的個人資料：

- 個人識別資訊（**PII**）
- 敏感個人資訊（**SPII**）

如果您需要資料分類來識別其他私人資料類型，例如額外的國民身分證號碼或醫療保健識別符，請聯絡您的客戶經理。

個人資料的類型

文件中的個人資料或_個人識別資訊_（PII）可以是一般個人資料或國家識別碼。下表第三列標識資料分類是否使用"接近度驗證"驗證其對標識符的發現。

表中標明了可以辨識這些項目的語言。

類型	識別符	接近度驗證？	英語	德文	西班牙語	法語	日本人
一般的	信用卡號碼	是的	✓	✓	✓		✓
	資料主體	不	✓	✓	✓		
	電子郵件	不	✓	✓	✓		✓
	IBAN 號碼（國際銀行帳號）	不	✓	✓	✓		✓
	IP 位址	不	✓	✓	✓		✓
	密碼	是的	✓	✓	✓		✓

類型	識別符	接近度驗證？	英語	德文	西班牙語	法語	日本人
國家識別符							

類型	識別符	接近度驗證？	英語	德文	西班牙語	法語	日本人

類型	識別符	接近度驗證的	英語	德文	西班牙語	法語	日本人
	希臘身分證	是的	✓	✓	✓		
	匈牙利稅務識別號	是的	✓	✓	✓		
	愛爾蘭身分證 (PPS)	是的	✓	✓			
	以色列身分證	是的	✓	✓	✓		
	義大利稅務識別號	是的	✓	✓	✓		
	日本個人身份證號碼（個人和公司）	是的	✓	✓	✓		✓
	拉脫維亞身分證	是的	✓	✓	✓		
	立陶宛身分證	是的	✓	✓	✓		
	盧森堡身分證	是的	✓	✓	✓		
	馬爾他身分證	是的	✓	✓	✓		
	國家醫療服務體系 (NHS) 號碼	是的	✓	✓	✓		
	紐西蘭銀行帳戶	是的	✓	✓	✓		
	紐西蘭駕駛執照	是的	✓	✓	✓		
	紐西蘭稅務局 (IRD) 號碼（稅號）	是的	✓	✓	✓		
	紐西蘭 NHI（國民健康指數）號碼	是的	✓	✓	✓		
	紐西蘭護照號碼	是的	✓	✓	✓		
	波蘭身分證 (PESEL)	是的	✓	✓	✓		
	葡萄牙稅務識別號碼（NIF）	是的	✓	✓	✓		
	羅馬尼亞身分證 (CNP)	是的	✓	✓	✓		
	新加坡國民登記身分證（NRIC）	是的	✓	✓	✓		
	斯洛維尼亞身分證 (EMSO)	是的	✓	✓	✓		
	南非身分證	是的	✓	✓	✓		
	西班牙稅務識別號	是的	✓	✓	✓		
	瑞典身分證	是的	✓	✓	✓		
	英國身分證（NINO）	是的	✓	✓	✓		
	美國加州駕駛執照	是的	✓	✓	✓		
	美國印第安納州駕照	是的	✓	✓	✓		
	美國紐約州駕駛執照	是的	✓	✓	✓		
	美國德州駕駛執照	是的	✓	✓	✓		
	美國社會安全號碼（SSN）	是的	✓	✓	✓		

敏感個人資料的類型

資料分類可以在文件中找到以下敏感個人資訊（SPII）。

以下 SPII 目前僅能以英文辨識：

- 刑事訴訟參考：有關自然人的刑事定罪和犯罪的數據。

- 種族參考：有關自然人的種族或民族血統的資料。
- 健康參考：有關自然人健康的數據。
- **ICD-9-CM** 醫療代碼：醫療保健產業使用的代碼。
- **ICD-10-CM** 醫療代碼：醫療保健產業使用的代碼。
- 哲學信仰參考：有關自然人的哲學信念的數據。
- 政治觀點參考：有關自然人政治觀點的數據。
- 宗教信仰參考：有關自然人的宗教信仰的資料。
- 性生活或性取向參考：自然人的性生活或性取向的資料。

類別類型

資料分類將您的資料分類如下。

大多數類別都可以用英語、德語和西班牙語識別。

類別	類型	英語	德文	西班牙語
金融	資產負債表	✓	✓	✓
	採購訂單	✓	✓	✓
	發票	✓	✓	✓
	季度報告	✓	✓	✓
人力資源	背景調查	✓		✓
	薪酬計劃	✓	✓	✓
	員工合約	✓		✓
	員工評價	✓		✓
	健康	✓		✓
	履歷	✓	✓	✓
合法的	保密協議	✓	✓	✓
	供應商-客戶合約	✓	✓	✓
行銷	活動	✓	✓	✓
	會議	✓	✓	✓
營運	審計報告	✓	✓	✓
銷售量	銷售訂單	✓	✓	
服務	射頻幹擾	✓		✓
	徵求建議書	✓		✓
	母豬	✓	✓	✓
	訓練	✓	✓	✓
支援	投訴和票務	✓	✓	✓

以下元資料也使用相同的支援語言進行分類和識別：

- 應用程式數據
- 存檔文件
- 聲音的
- 資料分類業務應用資料中的麵包屑
- CAD 檔案
- 程式碼
- 腐敗
- 資料庫和索引文件
- 設計文件
- 電子郵件應用程式數據
- 加密（具有高熵值的文件）
- 執行檔
- 財務應用數據
- 健康應用數據
- 圖片
- 紀錄
- 雜項文件
- 雜項演示
- 雜項電子表格
- 雜項“未知”
- 受密碼保護的文件
- 結構化資料
- 影片
- 零位元組文件

文件類型

資料分類掃描所有文件的類別和元資料洞察，並在儀表板的文件類型部分顯示所有文件類型。當資料分類偵測個人識別資訊 (PII) 或執行 DSAR 搜尋時，僅支援以下文件格式：

```
.CSV, .DCM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX, Docs,
Sheets, and Slides
```

所發現資訊的準確性

NetApp無法保證資料分類識別的個人資料和敏感個人資料 100% 的準確性。您應該始終透過查看數據來驗證資訊。

根據我們的測試，下表顯示了資料分類發現的資訊的準確性。我們根據_精確度_和_召回率_來細分它：

精確

資料分類發現的內容被正確識別的機率。例如，個人資料的準確率為 90%，表示在被識別為包含個人資訊的 10 個文件中，有 9 個實際上包含個人資訊。 10 個文件中會有 1 個是誤報。

記起

資料分類找到其應有內容的機率。例如，個人資料的召回率為 70%，意味著資料分類可以識別出組織中 10 個文件中實際包含個人資訊的 7 個。數據分類會遺漏 30% 的數據，而這些數據不會出現在儀表板中。

我們正在不斷提高結果的準確性。這些改進將在未來的資料分類版本中自動提供。

類型	精確	記起
個人資料 - 一般	90%-95%	60%-80%
個人資料 - 國家識別符	30%-60%	40%-60%
敏感個人數據	80%-95%	20%-30%
類別	90%-97%	60%-80%

在NetApp Data Classification中建立自訂分類

NetApp Data Classification可讓您建立自訂類別或個人識別符，以識別特定於您組織監管和合規要求的資料。

資料分類支援兩種類型的自訂分類器：類別和個人識別碼。自訂類別是根據您上傳的一組檔案建立的，資料分類功能會根據這些檔案建立一個 AI 模型，以識別您組織中的類似資料（例如，一家健康研究公司可能會建立一個臨床分析類別）。使用關鍵字清單或正規表示式 (regex) 建立自訂個人識別符，以識別貴組織特有的、可能構成合規風險的資訊。

所有自訂分類都可以在自訂分類控制面板中找到。

建立自訂個人標識符

資料分類功能可讓您使用上下文關鍵字或正規表示式建立自訂個人識別符，以識別貴組織特有的資料。

關鍵字要求

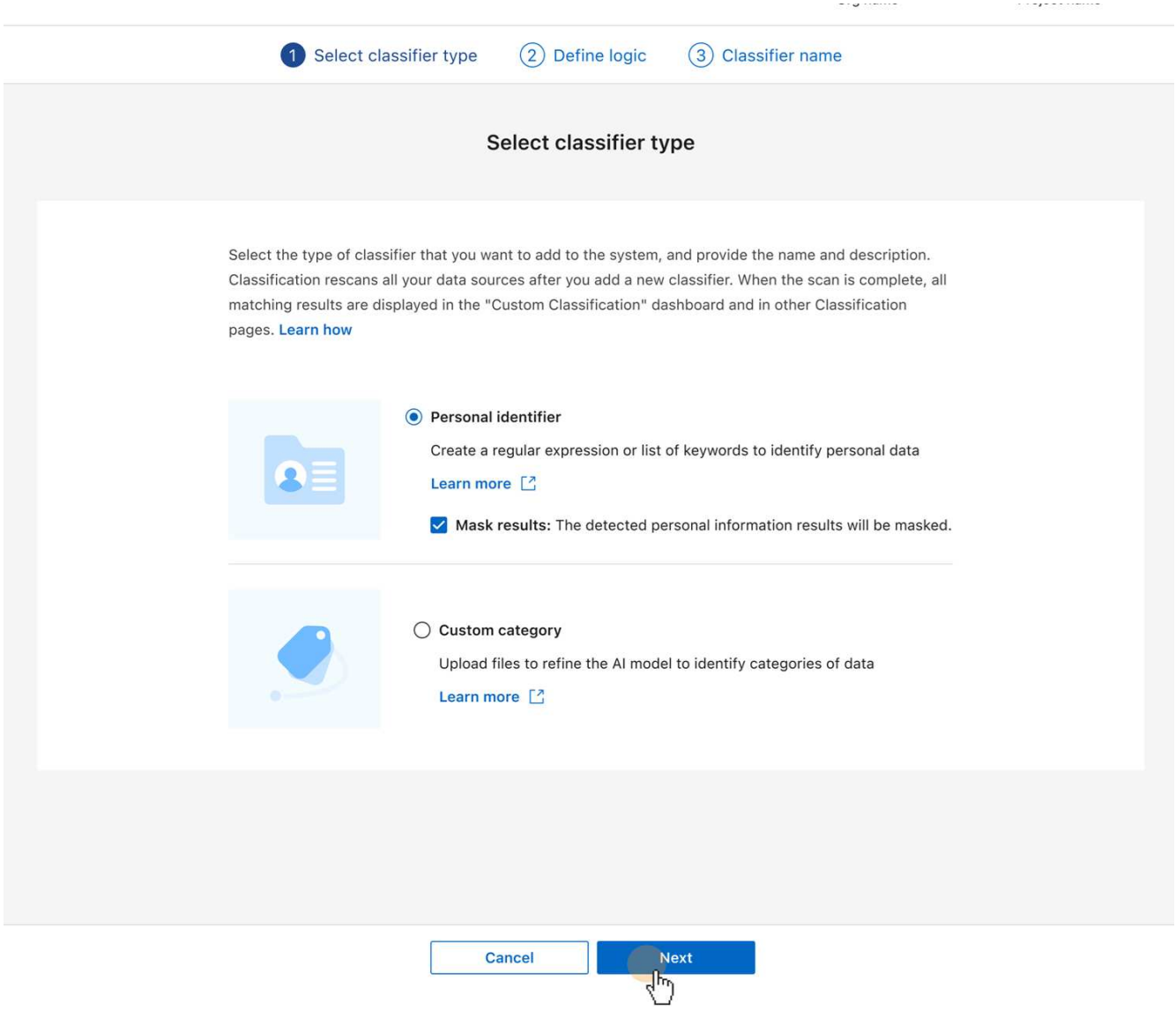
如果您使用關鍵字清單建立個人標識符，則該清單必須滿足以下要求：

- 關鍵字輸入不區分大小寫。
- 關鍵字必須至少包含三個字元。長度少於三個字元的單字將被忽略。
- 重複的字詞只會加一次。
- 關鍵字總數不能超過 50 萬個字元。清單中必須至少包含一個關鍵字。

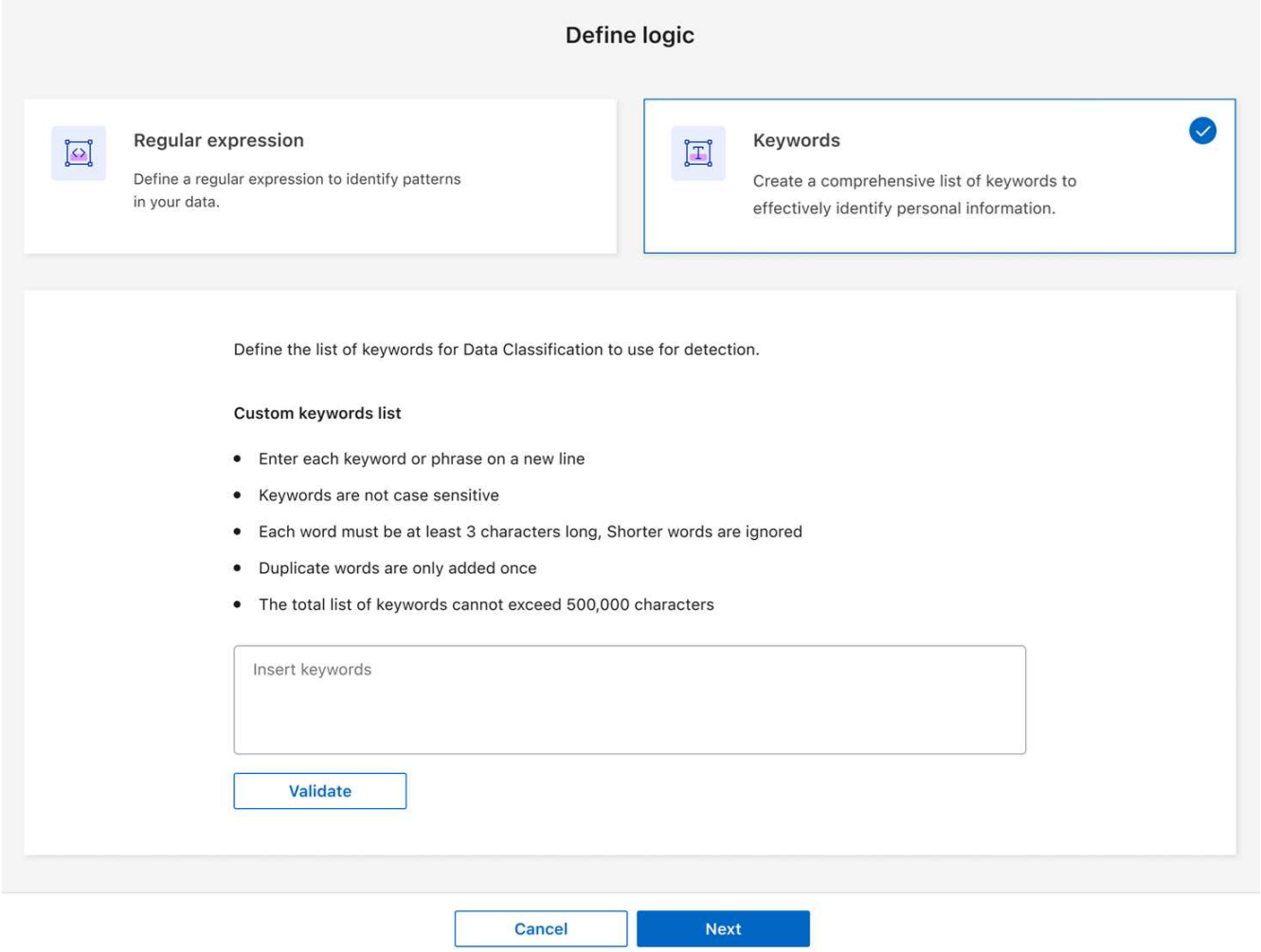
步驟

1. 選擇自訂分類選項卡。
2. 選擇**+** 新分類器以建立自訂分類器。

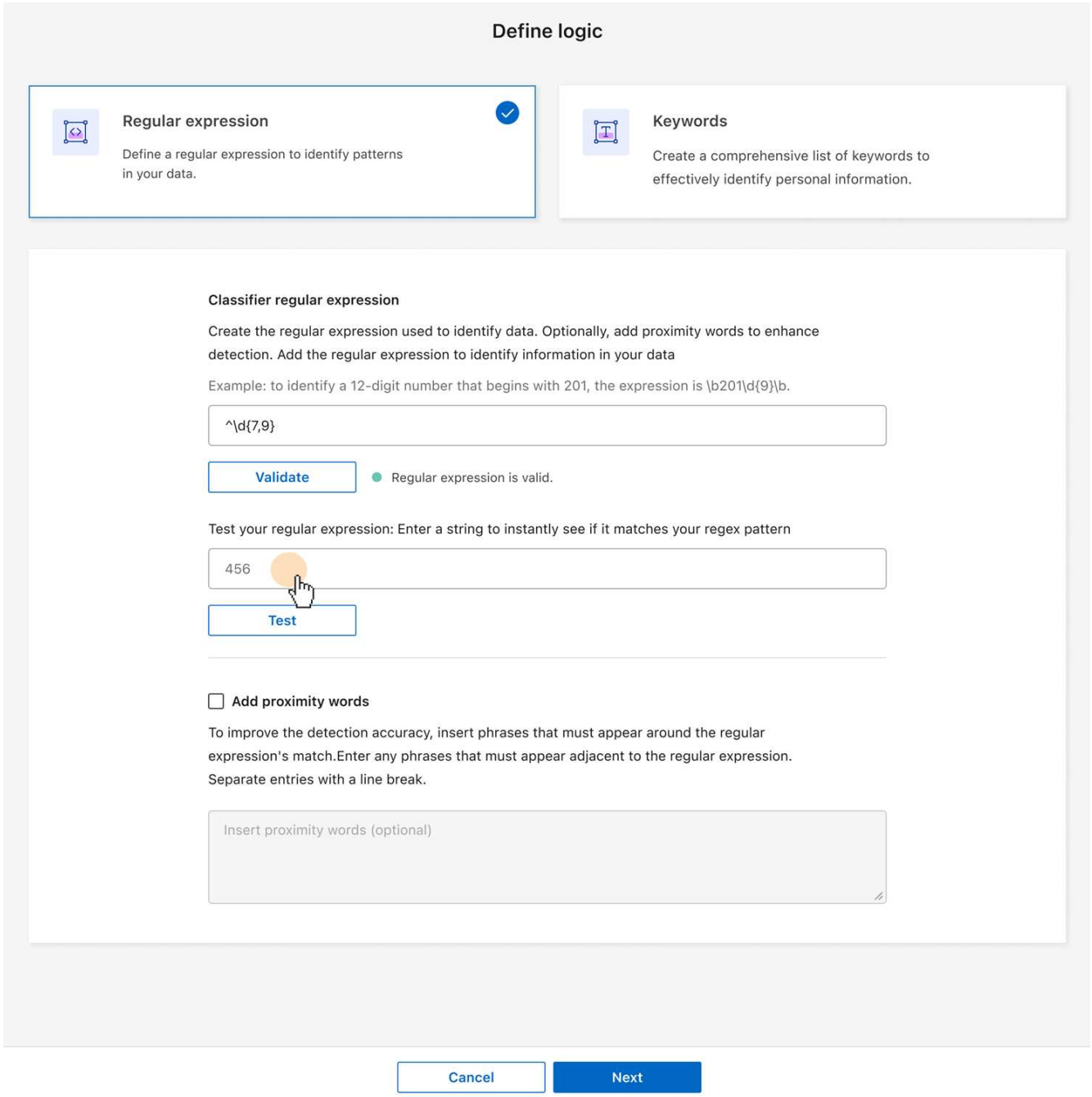
3. 請選擇*個人識別碼*。（可選）選擇「屏蔽結果」以封鎖偵測到的個人資料。
4. 選擇下一步。



5. 若要新增帶有關鍵字的分類器，請選擇關鍵字。請輸入關鍵字列表，每個關鍵字佔一行。請確保關鍵字符合要求。



若要將分類器新增為正規表示式，請選擇正規表示式，然後新增模式來偵測資料的特定資訊。選擇驗證以確認您輸入的語法正確。



a. （可選）輸入一個應該與正規表示式模式相符的範例字串，然後選擇測試進行檢查。

b. （可選）添加鄰近詞。如果新增鄰近詞，則資料分類僅在鄰近詞與匹配字串相鄰時才標記正規表示式模式。

6. 選擇下一步。
7. 輸入分類器名稱和描述，以便在儀表板中識別自訂類別。
8. 選擇儲存以建立自訂個人識別碼。

建立自訂個人標識符後，其結果將在下次計劃掃描中捕獲。為了更快地取得結果，請執行按需掃描。若要查看結果，請參閱 產生合規性報告。

建立自訂類別

透過自訂類別，您可以對特定於您組織的資料進行分類。自訂類別是根據您上傳的文字檔案建立的，資料分類功能會根據這些檔案建立一個人工智慧模型，以識別其他檔案中的類似資訊。

訓練資料要求

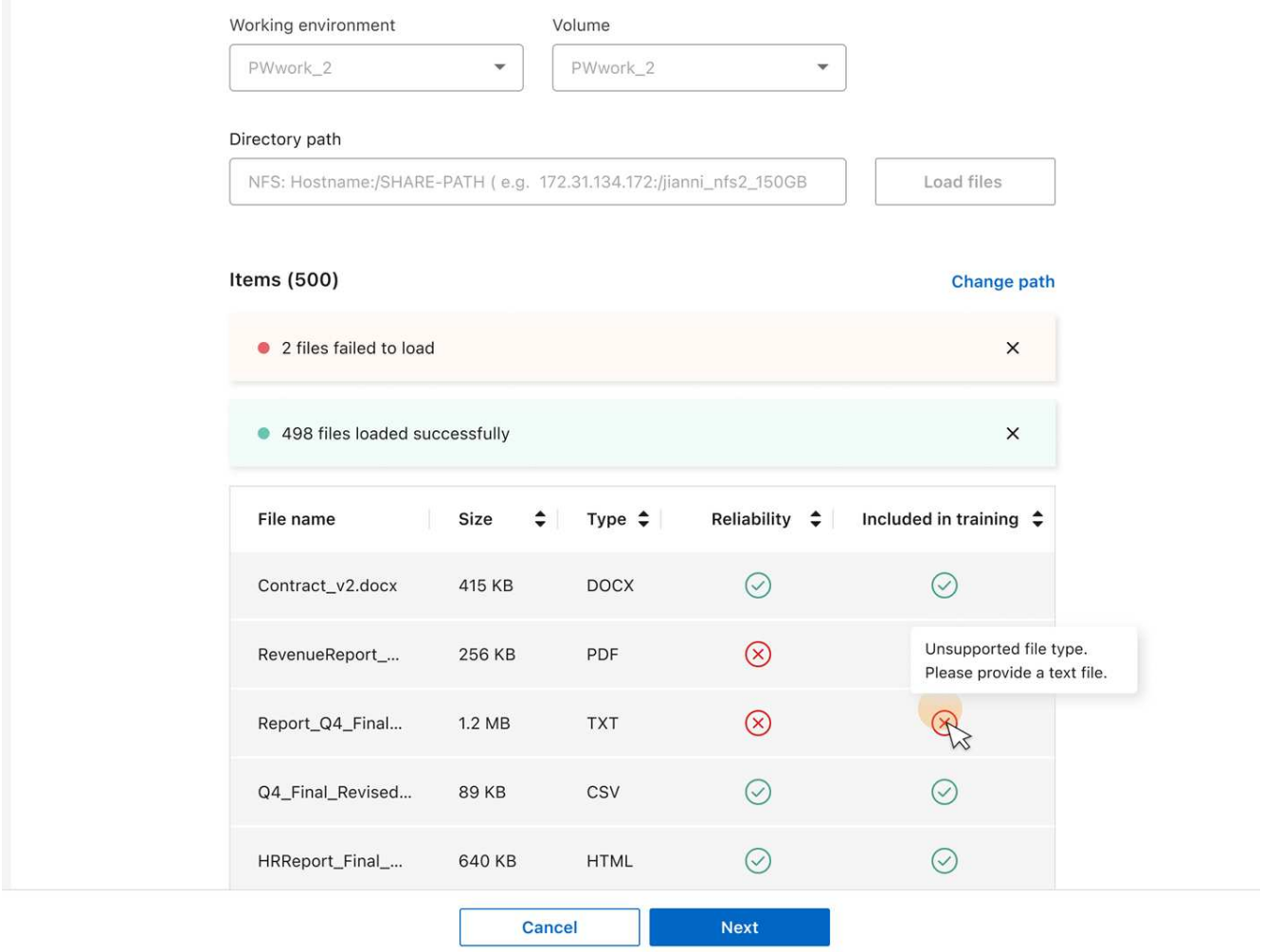
- 訓練資料集必須至少包含 25 個檔案。最大文件數為 1,000。
- 所有文件必須直接位於您提供的文件路徑中。
- 所有檔案必須大於 100 位元組。
- 資料分類訓練資料必須是下列檔案類型之一：CSV、DOCX、DOC、GZ、JSON、PDF、PPTX、TXT、RTT、XLS 或 XLSX。您可以上傳所有支援的文件類型的組合。

步驟

1. 在NetApp Data Classification中，選擇「自訂分類」。
2. 選擇 **+** 新分類器。
3. 選擇“自訂類別”作為分類器類型，然後下一步。
4. 使用一系列基於文字的文件來定義自訂類別的邏輯。請提供*工作位址*的IP位址，然後從下拉式選單中選擇*音量*。

   輸入包含訓練資料的目錄的目錄路徑。

5. 選擇“載入檔案”進行資料分類，以執行檔案檢查。您可以查看文件摘要，其中列出了文件名稱、大小、類型和備註（如果該文件被認為適合用於培訓）。



資料分類會顯示資料訓練的預計完成時間。..若要變更檔案路徑或重新上傳檔案，請選取 **Change path** ，然後輸入資料並再次載入檔案。

6. 當您對上傳的文件滿意後，請選擇下一步。
7. 輸入分類器名稱和描述，以便在儀表板中識別自訂類別。
8. 選擇儲存以建立自訂類別。

結果

建立自訂類別後，其結果將在下次計畫掃描中擷取。為了更快地取得結果，請手動啟動掃描。

編輯自訂分類器

建立個人識別碼後，您可以修改其邏輯。您無法變更個人識別碼的類型或邏輯類型；例如，您無法將自訂類別變更為自訂個人識別碼。您也不能將基於關鍵字的自訂識別碼變更為基於正規表示式的自訂識別碼。

步驟

1. 在NetApp Data Classification中，選擇「自訂分類」。
2. 確定要刪除的分類器，然後選擇操作選單 ... 在它那一行的末尾。
3. 選擇編輯邏輯。

4. 如果要修改關鍵字，請新增、刪除或編輯對應的關鍵字。如果要修改正規表示式，請輸入新的正規表示式並進行驗證。（可選）加入鄰近關鍵字。
5. 選擇“儲存”以套用變更。

刪除自訂分類器

1. 在NetApp Data Classification中，選擇「自訂分類」。
2. 確定要刪除的分類器，然後選擇操作選單 ... 在它那一行的末尾。
3. 選擇刪除分類器。

下一步

- 產生合規性報告

使用NetApp Data Classification調查組織中儲存的數據

資料調查儀表板顯示文件和目錄層級的資料洞察，使您能夠對結果進行排序和過濾。數據調查頁面提供有關文件和目錄元數據和權限的見解以及識別重複文件。透過文件、目錄和資料庫層級的洞察，您可以採取措施來提高組織的合規性並節省儲存空間。資料調查頁面還支援移動、複製和刪除檔案。

要從調查頁面獲得見解，您必須對資料來源執行完整的分類掃描。僅進行過映射掃描的資料來源不會顯示檔案層級的詳細資訊。

資料調查結構

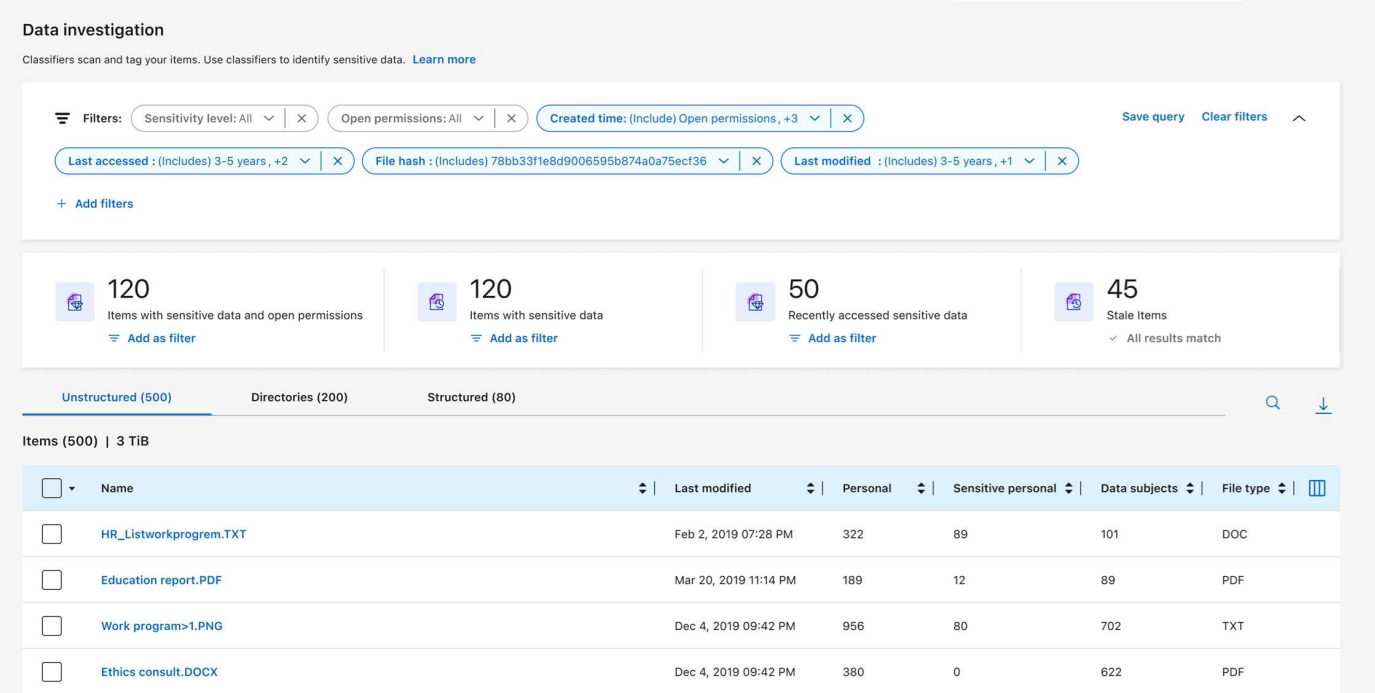
數據調查頁面將數據分類到三個選項卡：

- 非結構化資料：文件數據
- 目錄：資料夾和檔案共享
- 結構化：資料庫

數據過濾器

資料調查頁面提供了許多過濾器來對您的資料進行分類，以便您可以找到所需的資料。您可以同時使用多個過濾器。

若要新增過濾器，請選擇新增過濾器按鈕。



過濾敏感度和內容

使用以下過濾器查看您的資料包含多少敏感資訊。

篩選	細節
類別	選擇"類別類型"。
敏感度等級	選擇敏感度等級：個人、敏感個人或非敏感。
識別符數量	選擇每個檔案偵測到的敏感標識符的範圍。包括個人資料和敏感個人資料。在目錄中過濾時，資料分類會將每個資料夾（和子資料夾）中所有檔案的匹配結果匯總。注意：2023 年 12 月（版本 1.26.6）版本刪除了按目錄計算個人識別資訊 (PII) 資料數量的選項。
個人資料	選擇"個人資料的類型"。
敏感個人資訊	選擇"敏感個人資料的類型"。
資料主體	輸入資料主體的全名或已知標識符。"在此處了解有關數據主體的更多信息" 。

過濾使用者擁有者和使用者權限

使用下列過濾器查看文件擁有者和存取資料的權限。

篩選	細節
開放權限	選擇資料和資料夾/共享內的權限類型。
使用者/群組權限	選擇一個或多個使用者名稱和/或群組名，或輸入部分名稱。
文件所有者	輸入檔案所有者名稱。
有存取權限的使用者數	選擇一個或多個類別範圍以顯示哪些檔案和資料夾對一定數量的使用者開放。

按時間順序過濾

使用以下過濾器根據時間標準查看資料。

篩選	細節
創建時間	選擇文件建立的時間範圍。您也可以指定自訂時間範圍來進一步最佳化搜尋結果。
發現時間	選擇資料分類發現檔案的時間範圍。您也可以指定自訂時間範圍來進一步最佳化搜尋結果。
上次修改	選擇檔案最後修改的時間範圍。您也可以指定自訂時間範圍來進一步最佳化搜尋結果。
上次訪問	選擇檔案或目錄*上次被存取的時間範圍。您也可以指定自訂時間範圍來進一步最佳化搜尋結果。對於資料分類掃描的檔案類型，這是資料分類最後一次掃描該檔案的時間。

{星號} 目錄的上次存取時間僅適用於 NFS 或 CIFS 共用。

過濾元資料

使用下列篩選器根據位置、大小和目錄或檔案類型檢視資料。

篩選	細節
文件路徑	輸入最多 20 個要在查詢中包含或排除的部分或完整路徑。如果同時輸入包含路徑和排除路徑，資料分類會先在包含路徑中找到所有文件，然後從排除路徑中刪除文件，然後顯示結果。請注意，在此過濾器中使用“*”沒有任何效果，並且您無法從掃描中排除特定資料夾 - 配置共用下的所有目錄和檔案都將被掃描。
目錄類型	選擇目錄類型；“共享”或“資料夾”。
文件類型	選擇"文件類型"。
文件大小	選擇檔案大小範圍。
文件哈希	輸入文件的雜湊值即可找到特定文件，即使名稱不同。

過濾器儲存類型

使用以下過濾器按儲存類型查看資料。

篩選	細節
系統類型	選擇系統類型。
系統環境名稱	選擇特定係統。
儲存庫	選擇儲存庫，例如磁碟區或模式。

過濾查詢

使用下列篩選器按已儲存的查詢查看資料。

篩選	細節
已儲存的查詢	選擇一個或多個已儲存的查詢。前往"已儲存的查詢選項卡"查看現有已儲存查詢的清單並建立新查詢。
標籤	選擇"一個或多個標籤"分配給您的文件。

過濾分析狀態

使用以下過濾器按資料分類掃描狀態查看資料。

篩選	細節
分析狀態	選擇一個選項來顯示「等待首次掃描」、「已完成掃描」、「等待重新掃描」或「掃描失敗」的檔案清單。
掃描分析事件	選擇是否要查看由於資料分類無法恢復上次存取時間而未分類的文件，或即使資料分類無法恢復上次存取時間但已分類的文件。

"查看有關"上次訪問時間"時間戳的詳細信息"有關使用掃描分析事件進行過濾時調查頁面中出現的項目的詳細資訊。

按重複項過濾資料

使用以下過濾器查看儲存中重複的檔案。

篩選	細節
重複項	選擇檔案是否在儲存庫中重複。

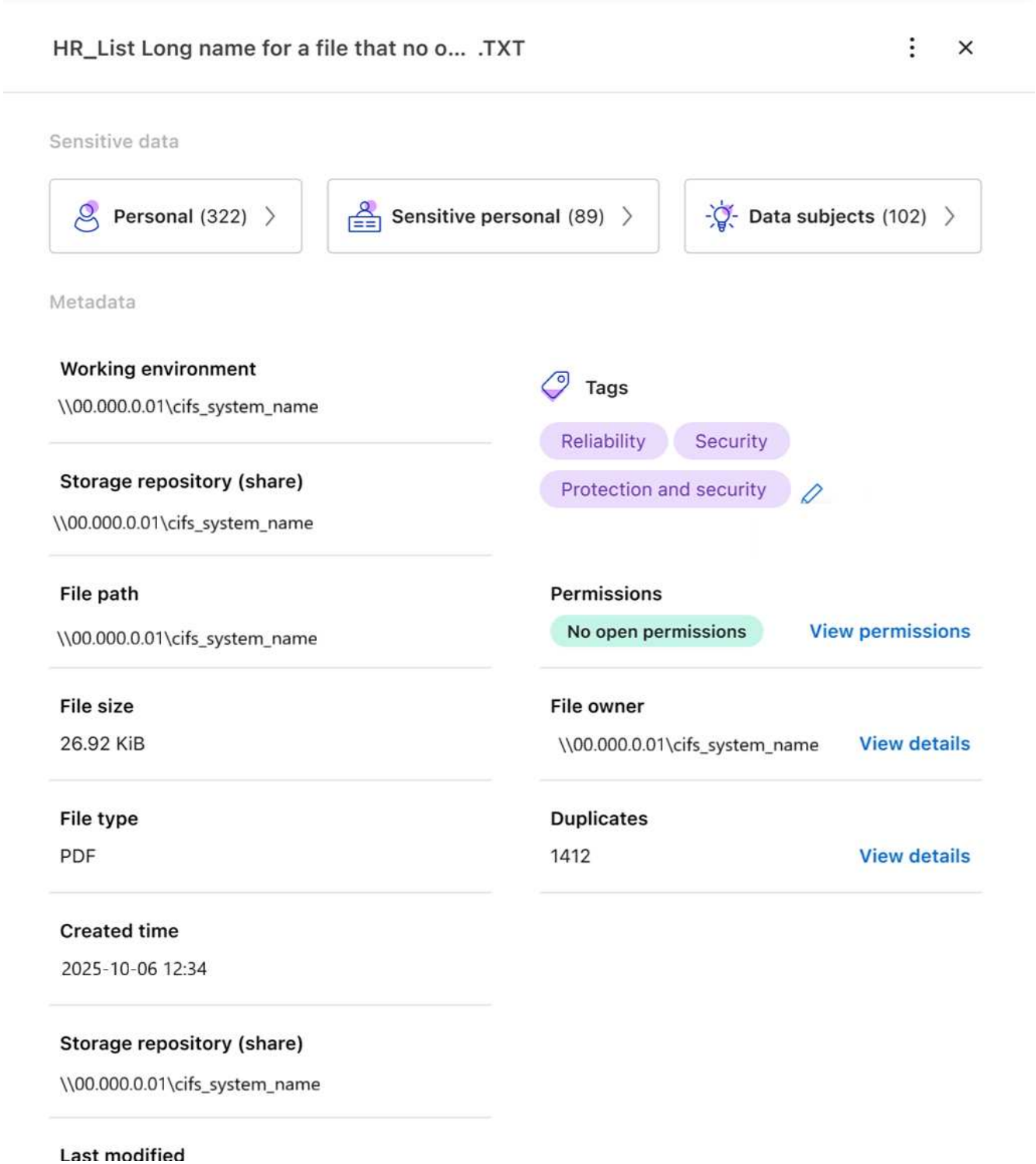
查看檔案元數據

除了顯示文件所在的系統和磁碟區之外，元資料還顯示更多信息，包括文件權限、文件擁有者以及該文件是否有重複。如果您打算"建立已儲存的查詢"因為您可以看到可用於過濾資料的所有資訊。

資訊的可用性取決於資料來源。例如，資料庫檔案的磁碟區名稱和權限不共用。

步驟

1. 從資料分類選單中，選擇*調查*。
2. 在右側的資料調查清單中，選擇向下插入符號 在任意單一文件的右側查看文件元資料。



3. 或者，您可以使用*建立標籤*按鈕為檔案建立或新增標籤。從下拉式選單中選擇一個現有標籤或使用 + 新增按鈕新增一個新標籤。標籤可用於過濾資料。

查看檔案和目錄的使用者權限

若要查看有權存取檔案或目錄的所有使用者或群組的清單以及他們擁有的權限類型，請選擇「查看所有權限」。此選項僅適用於 CIFS 共享中的資料。

如果您使用安全性識別碼 (SID) 而不是使用者名稱和群組名，則應該將 Active Directory 整合到資料分類中。有

關更多信息，請參閱"將 Active Directory 新增至資料分類" 。

步驟

1. 從資料分類選單中，選擇*調查*。
2. 在右側的資料調查清單中，選擇向下插入符號在任意單一文件的右側查看文件元資料。
3. 若要查看有權存取檔案或目錄的所有使用者或群組的清單以及他們擁有的權限類型，請在「開啟權限」欄位中選擇「查看所有權限」。

   資料分類在清單中顯示最多 100 個使用者。

4. 選擇向下插入符號任何群組的按鈕即可查看屬於該群組的使用者清單。

   您可以展開該群組的某個層級來查看屬於該群組的使用者。

5. 選擇使用者或群組的名稱以重新整理調查頁面，以便您可以看到該使用者或群組有權存取的所有檔案和目錄。

檢查儲存系統中的重複文件

您可以檢查儲存系統中是否儲存了重複的檔案。如果您想確定可以節省儲存空間的區域，這將非常有用。確保具有特定權限或敏感資訊的某些檔案不會在儲存系統中不必要地重複也是很好的。

資料分類會比較所有檔案（資料庫除外）是否有重複項，如果存在重複項，則進行以下操作：

- 1 MB 或更大
- 或包含個人資訊或敏感個人資訊

資料分類使用雜湊技術來確定重複檔案。如果一個檔案的雜湊碼與另一個檔案相同，即使檔案名稱不同，這兩個檔案也是完全相同的副本。

步驟

1. 從資料分類選單中，選擇*調查*。
2. 在「篩選器」窗格中，選擇「檔案大小」以及「重複」（「有重複」）以查看您的環境中哪些特定大小範圍的檔案是重複的。
3. 或者，下載重複檔案的清單並將其發送給儲存管理員，以便他們可以決定可以刪除哪些檔案（如果有）。
4. 您可以選擇刪除、標記或移動重複的檔案。選擇您想要執行操作的文件，然後選擇適當的操作。

查看特定檔案是否重複

您可以查看單一文件是否有重複。

步驟

1. 從資料分類選單中，選擇*調查*。
2. 在資料調查清單中，選擇在任意單一文件的右側查看文件元資料。

   如果檔案存在重複，則此資訊將顯示在「*Duplicates*」欄位旁邊。

3. 若要查看重複檔案的清單及其位置，請選擇「查看詳細資料」*。
4. 在下一頁中選擇「查看重複項」以查看調查頁面中的文件。
5. 您可以選擇刪除、標記或移動重複的檔案。選擇您想要執行操作的文件，然後選擇適當的操作。

您可以使用此頁面提供的「檔案雜湊」值並將其直接輸入到調查頁面中，以便隨時搜尋特定的重複檔案 - 或者您可以在已儲存的查詢中使用它。

下載您的報告

您可以以 CSV 或 JSON 格式下載過濾結果。

如果資料分類正在掃描檔案（非結構化資料）、目錄（資料夾和檔案共用）和資料庫（結構化資料），則最多可以下載三個報表檔案。

檔案被分割成具有固定行數或記錄數的檔案：

- JSON：每份報告 100,000 筆記錄，產生大約需要 5 分鐘
- CSV：每份報告 200,000 筆記錄，產生大約需要 4 分鐘

您可以下載 CSV 檔案的版本以在此瀏覽器中查看。此版本限制為 10,000 筆記錄。

可下載報告所包含的內容

*非結構化文件資料報告*包含有關您的文件的以下資訊：

- 檔案名稱
- 位置類型
- 系統名稱
- 儲存庫（例如，磁碟區、儲存桶、共用）
- 儲存庫類型
- 文件路徑
- 文件類型
- 文件大小（單位：MB）
- 創建時間
- 上次修改時間
- 上次訪問
- 文件所有者
    - 設定 Active Directory 時，檔案擁有者資料包含帳戶名稱、SAM 帳戶名稱和電子郵件地址。
- 類別
- 個人資訊
- 敏感個人資訊

- 開放權限
- 掃描分析錯誤
- 刪除檢測日期

  刪除檢測日期標識檔案被刪除或移動的日期。這使您能夠識別敏感文件何時被移動。已刪除的文件不會計入儀表板或調查頁面上顯示的文件數量。這些文件僅出現在 CSV 報告中。

*非結構化目錄資料報告*包括有關您的資料夾和檔案共享的以下資訊：

- 系統類型
- 系統名稱
- 目錄名稱
- 儲存庫（例如資料夾或檔案共用）
- 目錄所有者
- 創建時間
- 發現時間
- 上次修改時間
- 上次訪問
- 開放權限
- 目錄類型

*結構化資料報告*包含有關資料庫表的以下資訊：

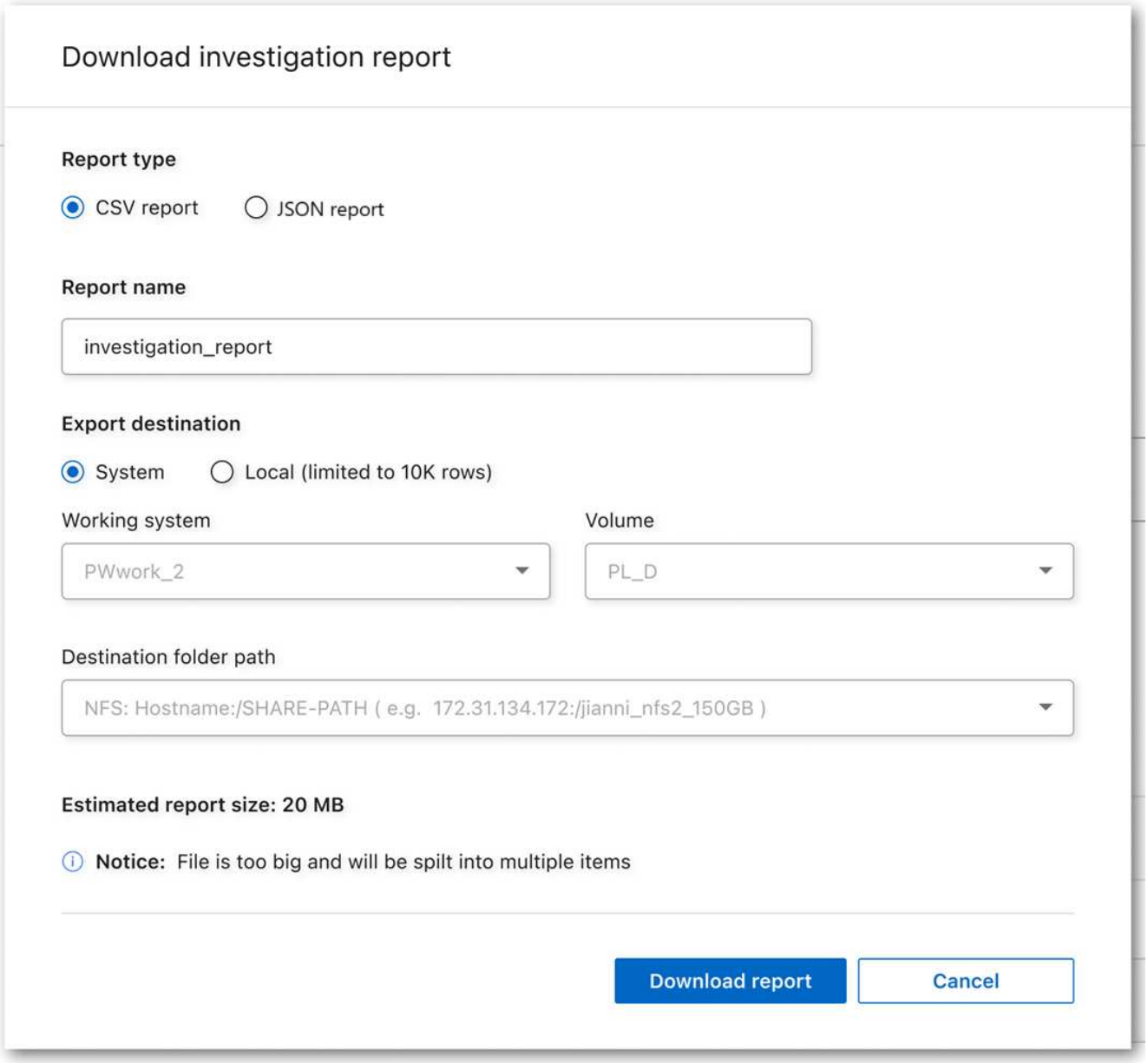
- 資料庫表名稱
- 位置類型
- 系統名稱
- 儲存庫（例如，架構）
- 列數
- 行數
- 個人資訊
- 敏感個人資訊

產生報告的步驟

1. 從資料調查頁面中，選擇  頁面右上方的按鈕。
2. 選擇報告類型：CSV 或 JSON。
3. 輸入報告名稱。
4. 若要下載完整的報告，請選擇系統，然後從對應的下拉式選單中選擇系統和磁碟區。提供目標資料夾路徑。

   若要在瀏覽器中下載報告，請選擇本機。請注意，此選項將報表限制為前 10,000 行，並且僅限於 **CSV** 格式。如果您選擇本機，則無需填寫任何其他欄位。

5. 選擇下載報告。



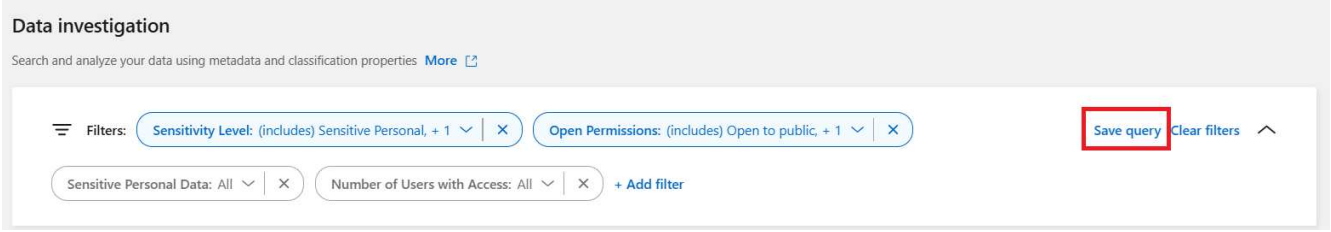
結果

對話方塊中將顯示一則訊息，提示正在下載報告。

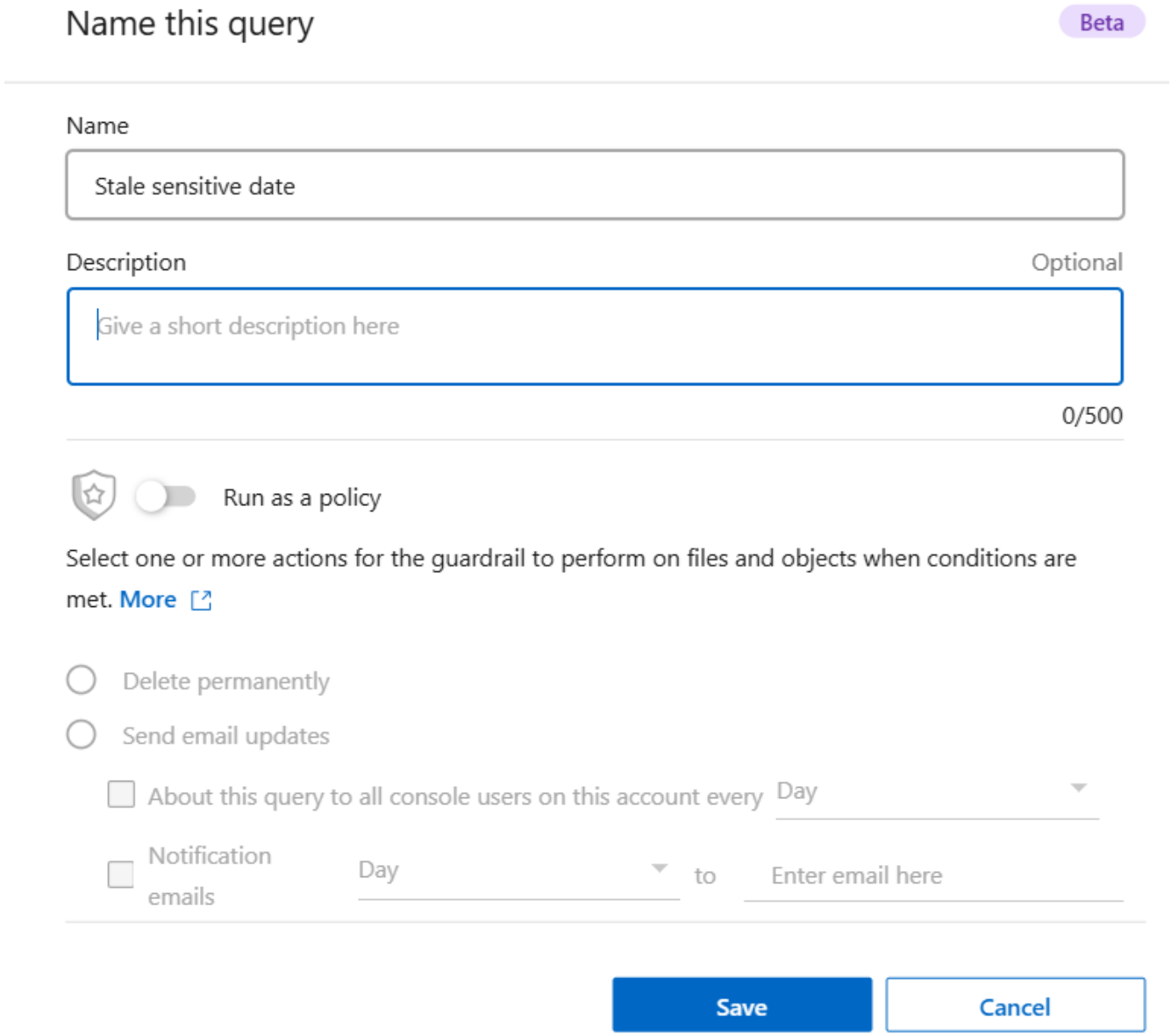
根據選定的篩選器建立已儲存的查詢

步驟

1. 在調查標籤中，透過選擇要使用的篩選器來定義搜尋。看"在調查頁面中過濾數據"了解詳情。
2. 一旦您根據自己的喜好設定了所有過濾器特性，請選擇*儲存查詢*。



3. 為已儲存的查詢命名並新增描述。該名稱必須是唯一的。
4. 您可以選擇將查詢儲存為策略：
   a. 若要將查詢儲存為策略，請切換*作為策略執行*開關。
   b. 選擇*永久刪除*或*發送電子郵件更新*。如果您選擇電子郵件更新，您可以每天、每週或每月透過電子郵件將查詢結果傳送給所有控制台使用者。或者，您可以以相同的頻率將通知傳送到特定的電子郵件地址。
5. 選擇*儲存*。



建立搜尋或策略後，您可以在已儲存的查詢標籤中查看它。

結果可能需要最多 15 分鐘才會顯示在「已儲存的查詢」頁面上。

使用NetApp Data Classification管理已儲存的查詢

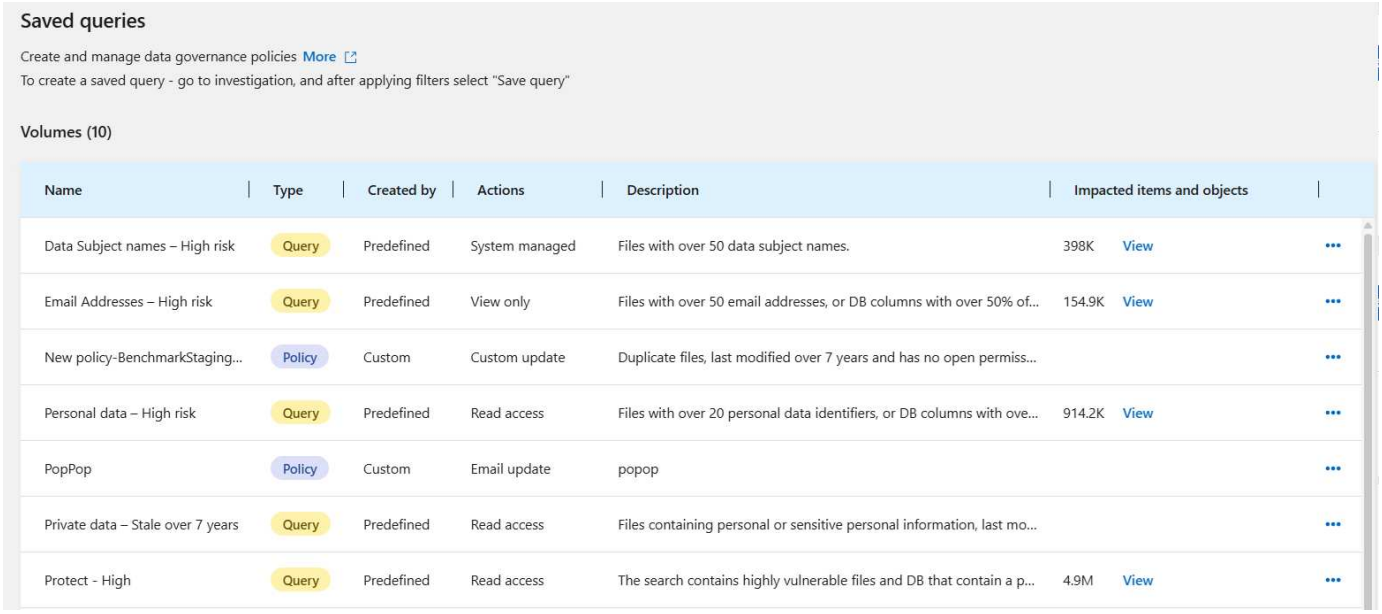
NetaApp 資料分類支援保存您的搜尋查詢。使用已儲存的查詢，您可以建立自訂篩選器來對資料調查頁面的常見查詢進行排序。資料分類還包括基於常見請求的預先定義保存的查詢。

合規性儀表板中的「已儲存的查詢」標籤列出了此資料分類實例上可用的所有預訂和自訂已儲存查詢。

已儲存的查詢也可以儲存為策略。查詢過濾數據，而策略允許您對數據採取行動。透過策略：您可以刪除發現的

資料或發送有關發現的資料的電子郵件更新。

已儲存的查詢也會出現在調查頁面的篩選器清單中。



在調查頁面中查看已儲存的查詢結果

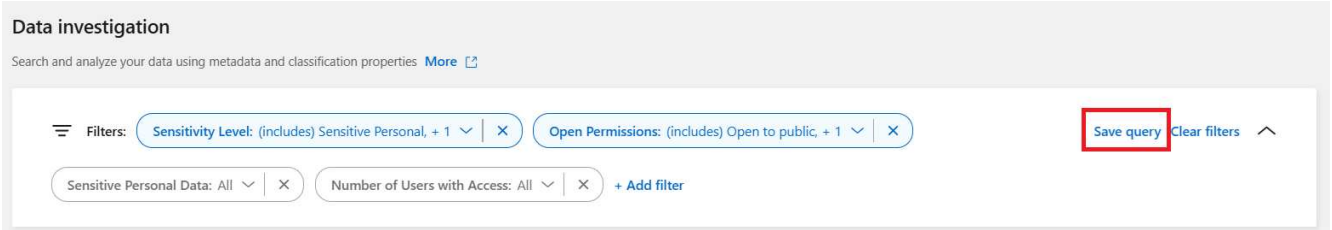
若要在調查頁面中顯示已儲存查詢的結果，請選擇 按鈕進行特定搜索，然後選擇*調查結果*。

建立已儲存的查詢和策略

您可以建立自己的自訂已儲存查詢，以提供特定於您組織的查詢結果。傳回符合搜尋條件的所有檔案和目錄（共用和資料夾）的結果。

步驟

1. 在調查標籤中，透過選擇要使用的篩選器來定義搜尋。看"在調查頁面中過濾數據"了解詳情。
2. 一旦您根據自己的喜好設定了所有過濾器特性，請選擇*儲存查詢*。

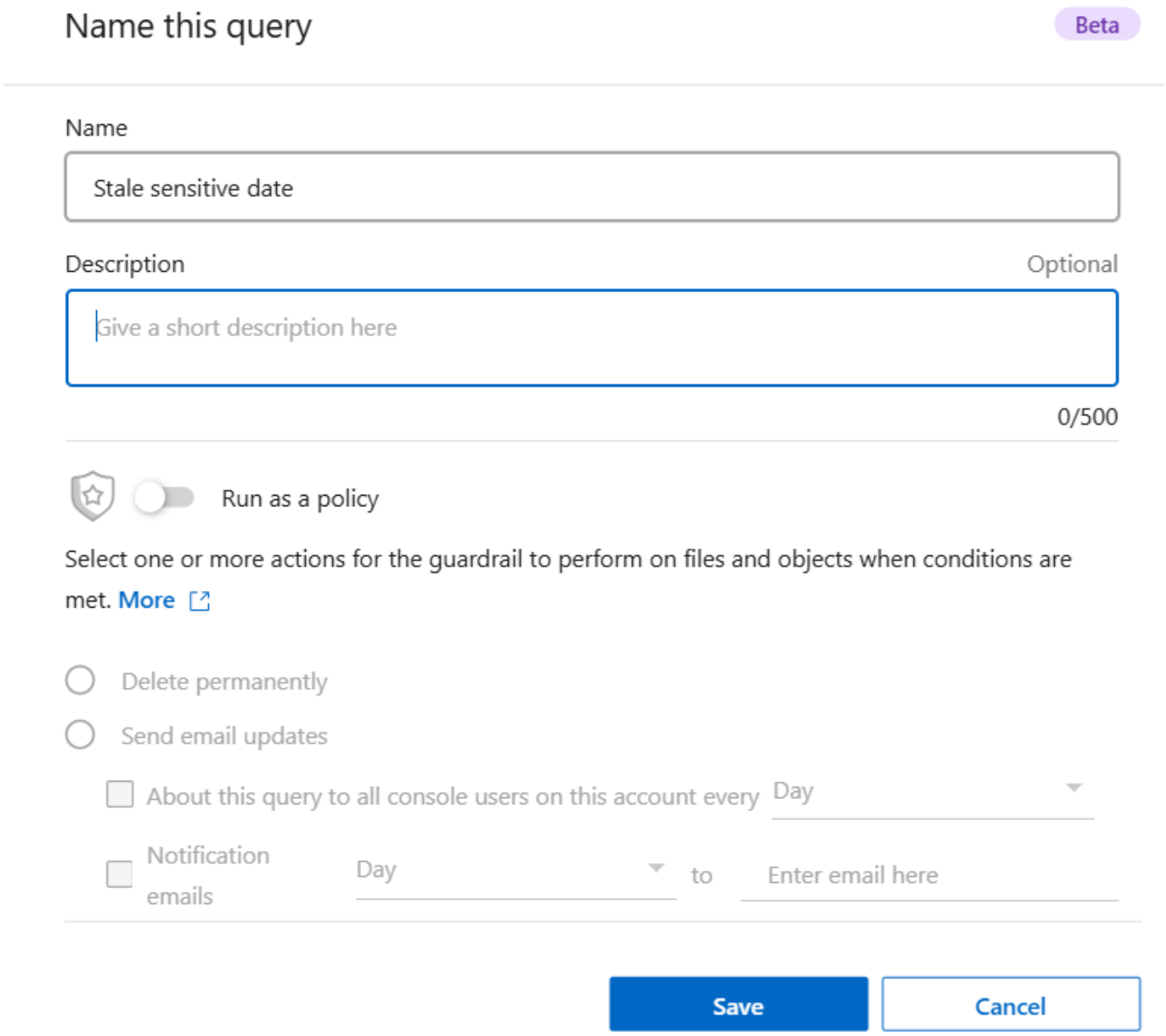


3. 為已儲存的查詢命名並新增描述。該名稱必須是唯一的。
4. 您可以選擇將查詢儲存為策略：

a. 若要將查詢儲存為策略，請切換*作為策略執行*開關。

b. 選擇*永久刪除*或*發送電子郵件更新*。如果您選擇電子郵件更新，您可以每天、每週或每月透過電子郵件將查詢結果傳送給所有控制台使用者。或者，您可以以相同的頻率將通知傳送到特定的電子郵件地址。

5. 選擇*儲存*。



建立搜尋或策略後，您可以在已儲存的查詢標籤中查看它。

編輯已儲存的查詢或策略

您可以修改已儲存查詢的名稱和描述。您也可以將查詢轉換為策略，反之亦然。

您不能修改預設儲存的查詢。您不能修改已儲存查詢的篩選器。您可以交替查看已儲存查詢的調查結果，變更或

修改篩選器，然後將其儲存為新查詢或政策。

步驟

1. 在「已儲存的查詢」頁面中，選擇要變更的搜尋的「編輯搜尋」。

2. 對名稱和描述欄位進行變更。僅更改名稱和描述欄位。

   您可以選擇將查詢轉換為策略，或將策略轉換為已儲存的查詢。根據需要切換*作為策略運作*開關。..如果您要將查詢轉換為策略，請選擇*永久刪除*或*發送電子郵件更新*。如果您選擇電子郵件更新，您可以每天、每週或每月透過電子郵件將查詢結果傳送給所有控制台使用者。或者，您可以以相同的頻率將通知傳送到特定的電子郵件地址。

3. 選擇“儲存”以完成變更。

刪除已儲存的查詢

如果您不再需要任何自訂已儲存的查詢或策略，可以將其刪除。您無法刪除預設儲存的查詢。

若要刪除已儲存的查詢，請選擇 按鈕進行特定搜索，選擇*刪除查詢*，然後在確認對話框中再次選擇*刪除查詢*。

預設查詢

資料分類提供以下系統定義的搜尋查詢：

- 資料主體姓名 - 高風險

  包含超過 50 個資料主體名稱的文件

- 電子郵件地址 - 高風險

  包含超過 50 個電子郵件地址的文件或資料庫列中超過 50% 的行包含電子郵件地址

- 個人資料 - 高風險

  包含超過 20 個個人資料標識符的文件或資料庫列中超過 50% 的行包含個人資料標識符

- 私人資料 - 已過期 7 年以上

  包含個人或敏感個人資訊的文件，上次修改超過 7 年

- 保護 - 高

  包含密碼、信用卡資訊、IBAN 號碼或社會安全號碼的文件或資料庫列

- 保護 - 低

超過 3 年未訪問的文件

- 保護 - 中等

  包含具有個人資料識別碼（包括身分證號碼、稅務識別號碼、駕駛執照號碼、藥品 ID 或護照號碼）的文件或資料庫列的文件

- 敏感個人資料 - 高風險

  包含超過 20 個敏感個人資料識別碼的文件或資料庫列中超過 50% 的行包含敏感個人數據

更改儲存庫的NetApp Data Classification掃描設置

您可以管理在每個系統和資料來源中如何掃描資料。您可以在「儲存庫」基礎上進行變更；這表示您可以根據正在掃描的資料來源類型對每個磁碟區、模式、使用者等進行變更。

您可以更改的一些內容包括是否掃描儲存庫，以及NetApp Data Classification是否正在執行"映射掃描或映射和分類掃描"。您也可以暫停和恢復掃描，例如，如果您需要在一段時間內停止掃描某個磁碟區。

查看儲存庫的掃描狀態

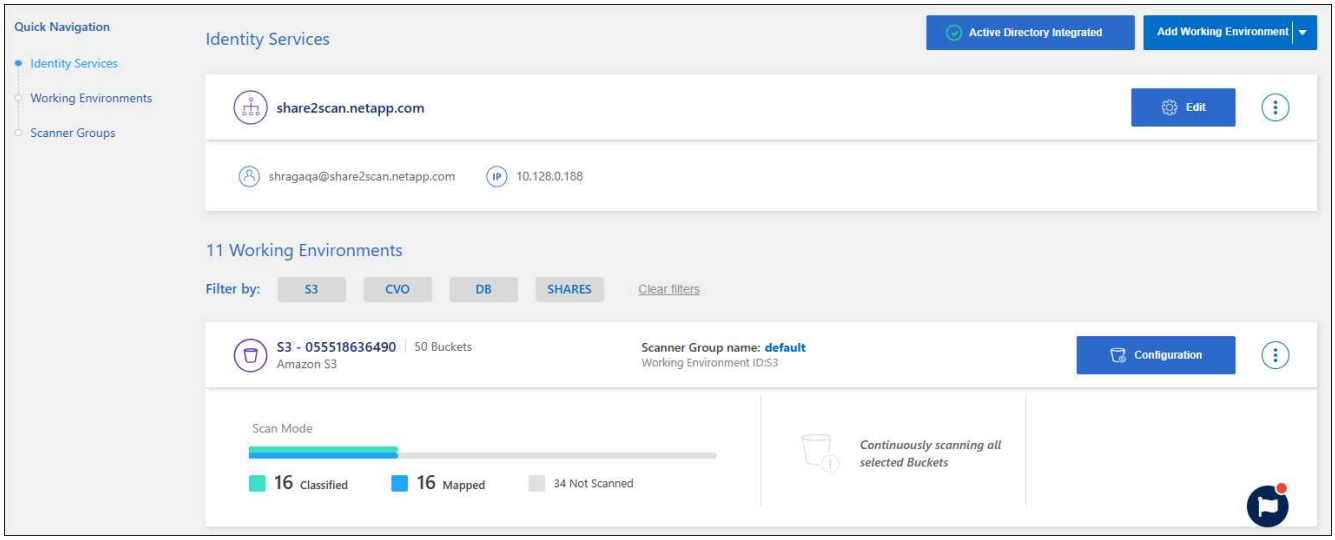
您可以查看NetApp Data Classification正在為每個系統和資料來源掃描的各個儲存庫（磁碟區、儲存桶等）。您還可以看到有多少已被“映射”，有多少已被“分類”。分類需要更長的時間，因為所有資料都進行了完整的 AI 識別。

您可以在設定頁面查看各個工作環境的掃描狀態：

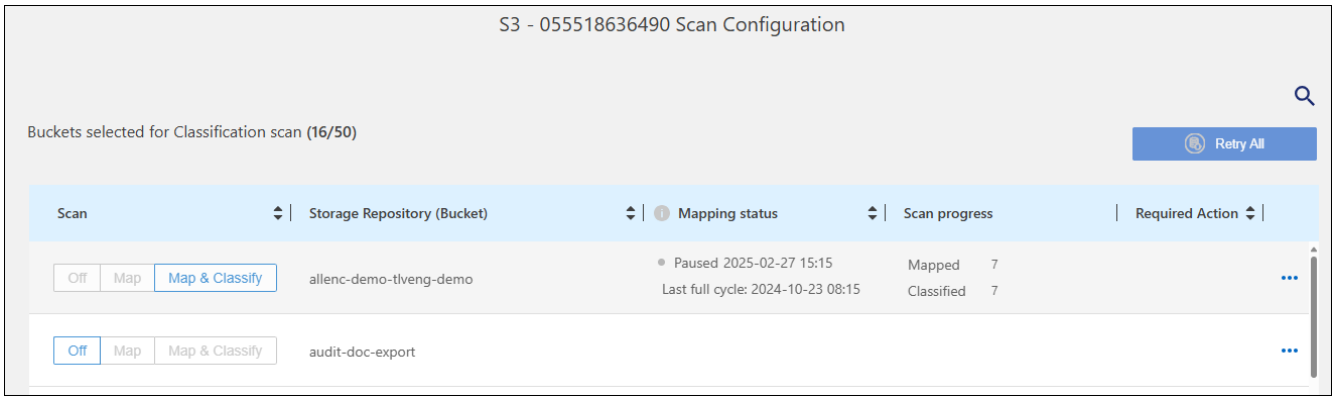
- 初始化（淺藍色點）：地圖或分類配置已啟動。此狀態會短暫顯示，然後過渡到「待處理佇列」狀態。
- 待處理佇列（橘色圓點）：掃描任務正在等待列入掃描佇列。
- 已排隊（橘色圓點）：任務已成功新增至掃描佇列。當佇列中的捲輪到達時，系統將開始映射或分類該磁碟區。
- 正在運行（綠點）：佇列中的掃描任務正在選定的儲存庫上積極進行。
- 完成（綠點）：儲存庫掃描已完成。
- 已暫停（灰點）：您已暫停掃描。雖然系統中未顯示音量變化，但掃描結果仍可使用。
- 錯誤（紅點）：掃描無法完成，因為遇到了問題。如果您需要完成某項操作，錯誤將出現在「所需操作」列下的工具提示中。否則，系統將顯示“錯誤”狀態並嘗試恢復。完成後，狀態就會改變。
- 未掃描：選擇了「關閉」磁碟區配置，系統未掃描該磁碟區。

步驟

1. 從資料分類選單中，選擇*配置*。



2. 從配置標籤中，選擇系統的*配置*按鈕。
3. 在掃描配置頁面中，查看所有儲存庫的掃描設定。



4. 掃描期間，將遊標停留在「對應狀態」列中的進度條上，即可查看該儲存庫中待對應或分類的檔案數量。

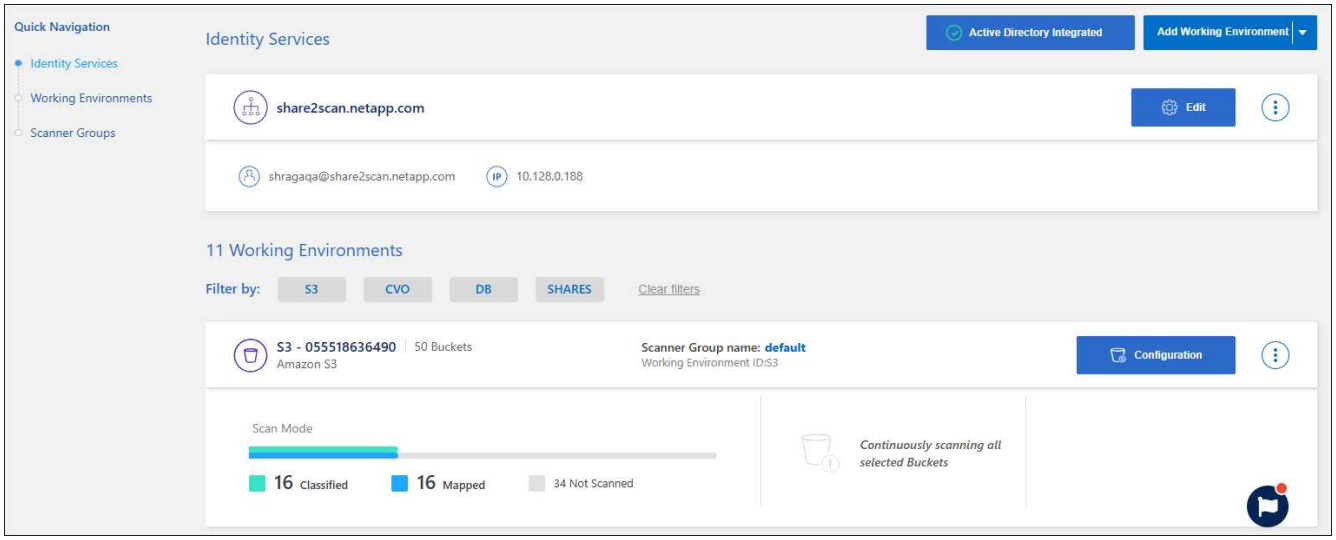
更改儲存庫的掃描類型

您可以隨時從設定頁面啟動或停止系統中的僅對應掃描或對應和分類掃描。您也可以從僅映射掃描變更為映射和分類掃描，反之亦然。

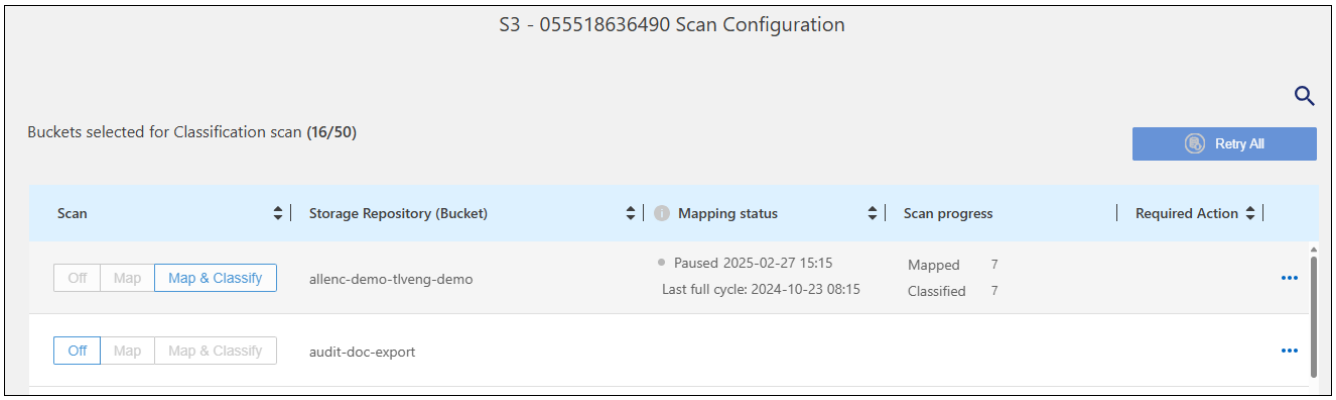
資料庫不能設定為僅映射掃描。資料庫掃描可以關閉或開啟；其中「開啟」相當於「映射和分類」。

步驟

1. 從資料分類選單中，選擇*配置*。
2. 從配置標籤中，選擇系統的*配置*按鈕。

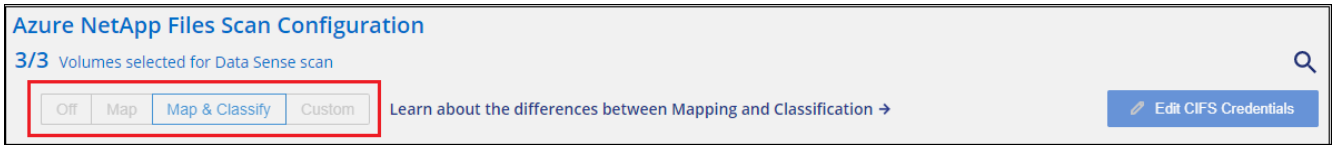


3. 在掃描設定頁面中，變更任何儲存庫（本例中為儲存桶）以執行*Map*或*Map & Classify*掃描。



某些類型的系統可讓您使用頁面頂部的按鈕列全域變更所有儲存庫的掃描類型。這對於Cloud Volumes ONTAP、本機ONTAP、 Azure NetApp Files和Amazon FSx for ONTAP系統有效。

下面的範例顯示了Azure NetApp Files系統的按鈕列。



優先掃描

您可以優先考慮最重要的僅映射掃描或映射和分類掃描，以確保高優先級掃描首先完成。

預設情況下，掃描會按照啟動的順序排隊。透過設定掃描優先權，您可以將掃描移至佇列的最前面。可以對多個掃描進行優先排序。優先權會依照先進先出的順序指定，這表示您優先考慮的第一個掃描將移至佇列的最前面；您優先考慮的第二個掃描將成為佇列中的第二個掃描，依此類推。

優先權是一次性授予的。映射資料的自動重新掃描按照預設順序進行。

步驟

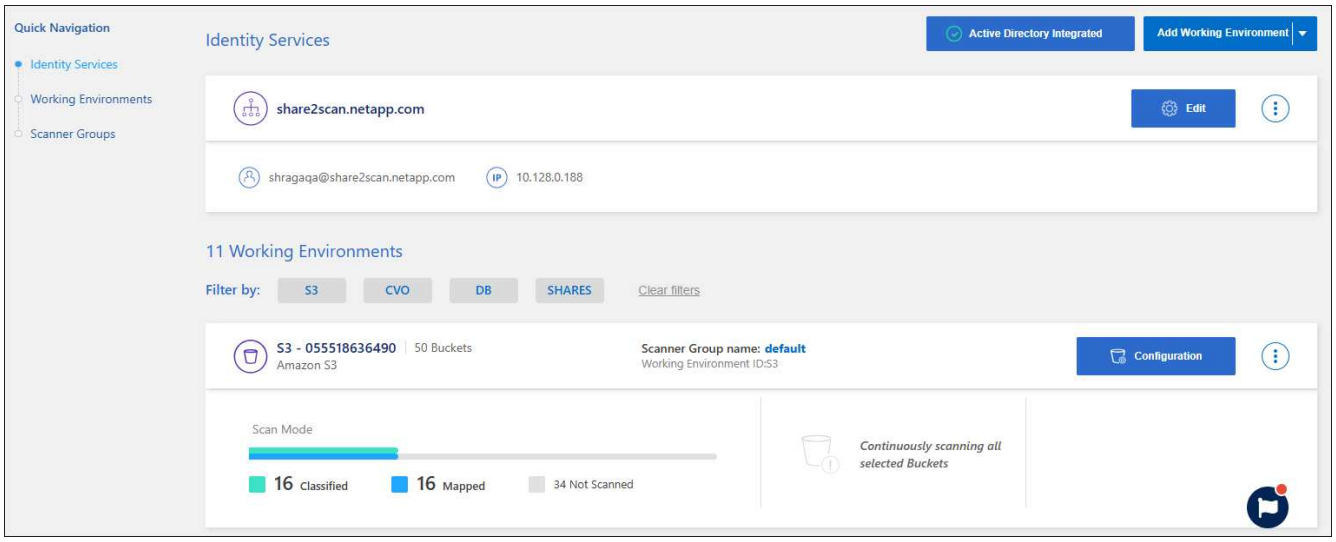
1. 從資料分類選單中，選擇*配置*。
2. 選擇您想要優先考慮的資源。
3. 從行動 `...`選項，選擇*優先掃描*。

停止掃描儲存庫

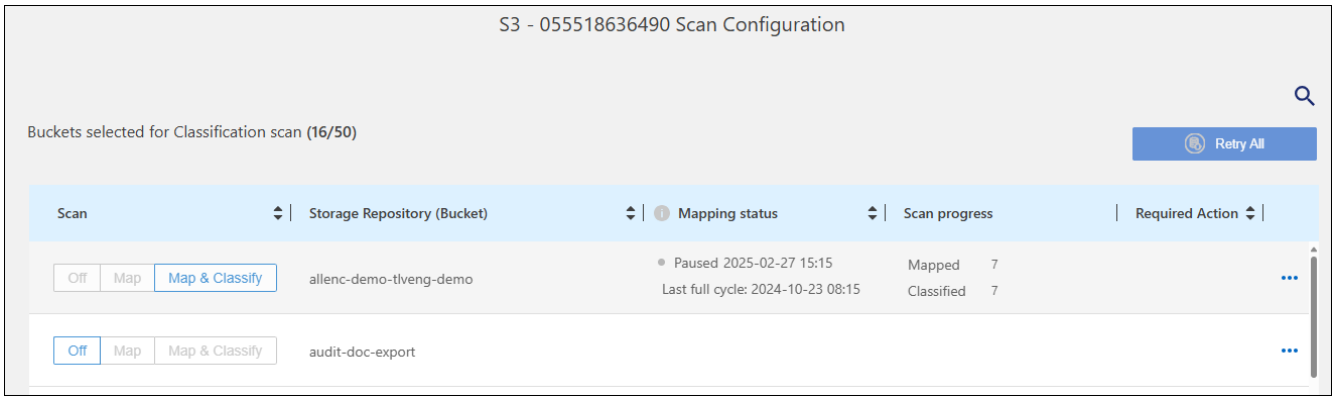
如果您不再需要監控儲存庫（例如磁碟區）的合規性，則可以停止掃描它。您可以透過關閉掃描來實現此目的。當掃描關閉時，有關該磁碟區的所有索引和資訊將從系統中刪除，並且掃描資料的收費也將停止。

步驟

1. 從資料分類選單中，選擇*配置*。
2. 從配置標籤中，選擇系統的*配置*按鈕。



3. 在掃描設定頁面中選擇「關閉」以停止掃描特定儲存桶。



暫停並恢復儲存庫掃描

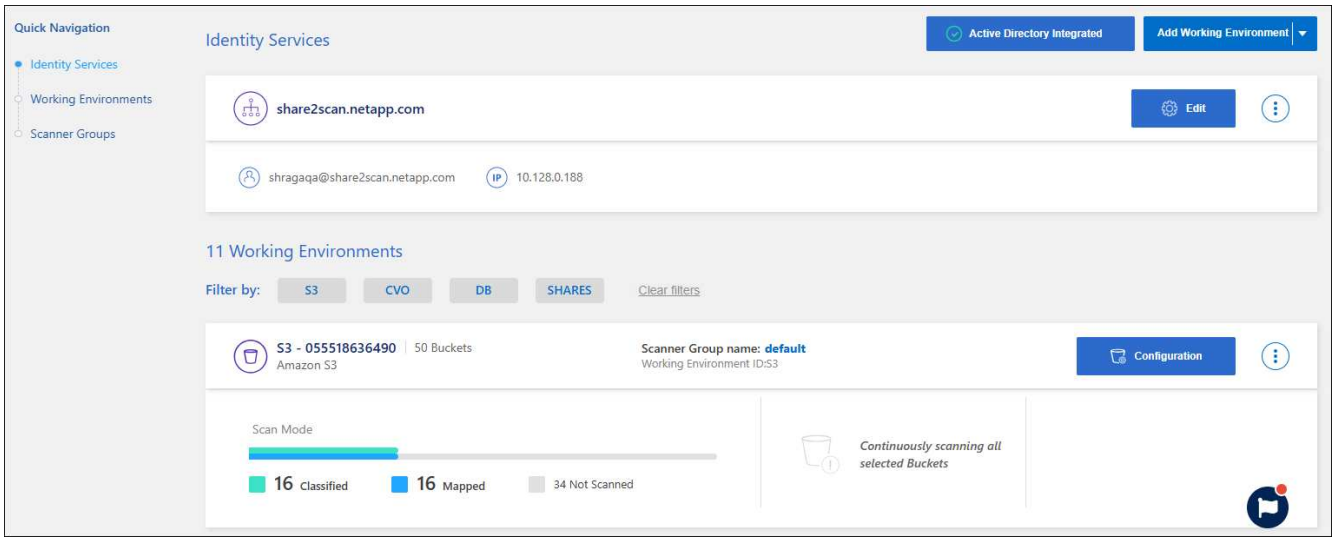
如果您想暫時停止掃描某些內容，您可以「暫停」儲存庫掃描。暫停掃描意味著資料分類將不再對儲存庫中的變更或新增執行任何未來的掃描。所有目前的掃描結果仍可在資料分類中查看。

即使暫停掃描，也不會免除計費費用，因為資料仍然保留在系統中。

您可以隨時恢復掃描。

步驟

1. 從資料分類選單中，選擇*配置*。
2. 從配置標籤中，選擇系統的*配置*按鈕。



3. 在掃描配置頁面中，選擇操作 ••• 圖示.
4. 選擇「暫停」暫停對磁碟區的掃描，或選擇「恢復」恢復先前已暫停的磁碟區的掃描。

查看NetApp Data Classification合規性報告

NetApp Data Classification提供報告，您可以使用這些報告來更好地了解組織的資料隱私計畫的狀態。

預設情況下，資料分類儀表板顯示所有系統、資料庫和資料來源的合規性和治理資料。如果您想要查看僅包含部分系統資料的報告，您可以進行篩選以僅查看這些系統的資料。

- 只有當您對資料來源執行完整分類掃描時，才可取得合規性報告。已進行僅映射掃描的資料來源只能產生資料映射報告。
- NetApp無法保證資料分類識別的個人資料和敏感個人資料 100% 的準確性。您應該始終透過查看數據來驗證資訊。

以下報告可用於資料分類：

- 資料發現評估報告：對掃描環境進行高級分析，以突出系統的發現並顯示關注領域和潛在的補救步驟。此報告可在治理儀表板中找到。
- 完整資料映射概覽報表：提供有關係統中檔案的大小和數量的資訊。這包括使用容量、資料年限、資料大小和檔案類型。此報告可在治理儀表板中找到。
- 資料主體存取請求報告：使您能夠提取包含有關資料主體的特定名稱或個人識別碼資訊的所有文件的報告。此報告可在合規性儀表板中找到。
- **HIPAA** 報告：幫助您識別文件中健康資訊的分佈。此報告可在合規性儀表板中找到。

- **PCI DSS** 報告：幫助您識別文件中信用卡資訊的分佈。此報告可在合規性儀表板中找到。
- 隱私風險評估報告：提供來自您的資料的隱私見解和隱私風險評分。此報告可在合規性儀表板中找到。
- 特定資訊類型的報告：可提供包含已識別文件（包含個人資料和敏感個人資料）詳細資訊的報告。您也可以查看按類別和文件類型細分的文件。

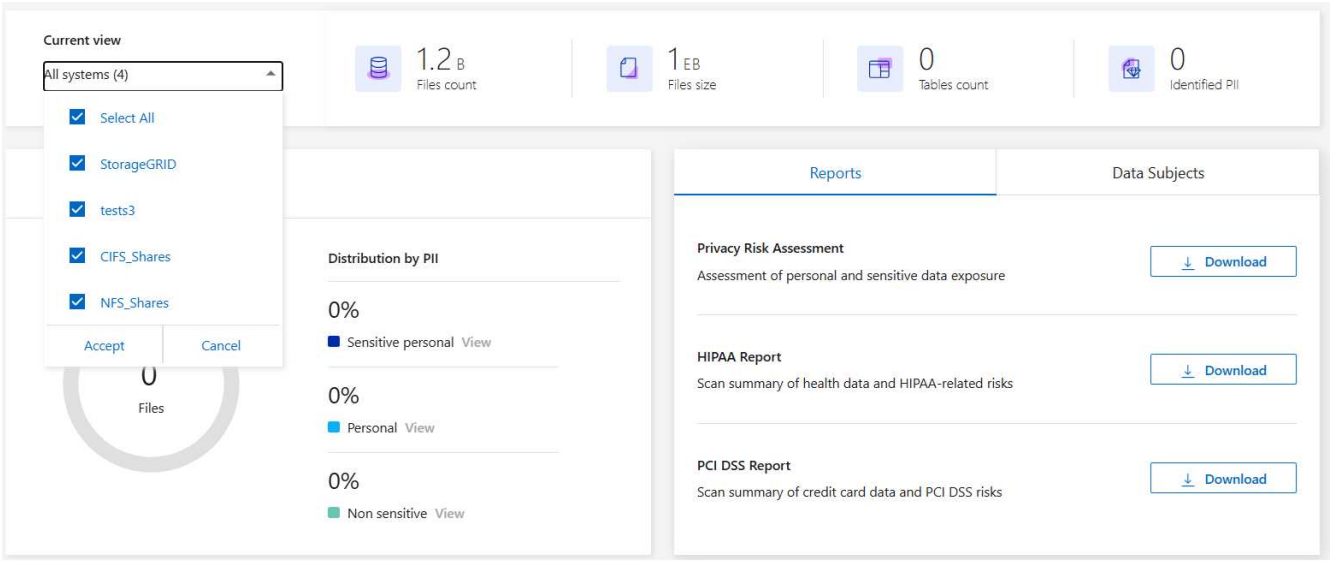
選擇報告系統

您可以過濾資料分類合規性儀表板的內容，以查看所有系統和資料庫的合規性數據，或僅查看特定係統的合規性數據。

當您篩選儀表板時，資料分類會將合規性資料和報表範圍限定到您選擇的系統。

步驟

1. 從資料分類選單中，選擇*合規性*。
2. 選擇系統過濾器下拉式選單，然後選擇系統。
3. 選擇接受來確認您的選擇。



資料主體存取請求報告

歐洲 GDPR 等隱私法規賦予資料主體（例如客戶或員工）存取其個人資料的權利。當資料主體請求此資訊時，這稱為 DSAR（資料主體存取請求）。各組織必須「毫不拖延」地回應這些請求，最晚不得超過收到請求後的一個月。

您可以透過搜尋主題的全名或已知識別碼（例如電子郵件地址）然後下載報告來回應 DSAR。該報告旨在幫助您的組織遵守 GDPR 或類似的資料隱私法。

*資料分類如何幫助您回應 DSAR？ *

當您執行資料主體搜尋時，資料分類會找到包含該人姓名或識別碼的所有檔案。資料分類檢查最新的預索引資料的名稱或識別碼。它不會啟動新的掃描。

搜尋完成後，您可以下載資料主體存取請求報告的檔案清單。該報告匯總了數據中的見解，並將其轉化為法律術

語，以便您可以將其發送給相關人員。

目前資料庫不支援資料主體搜尋。

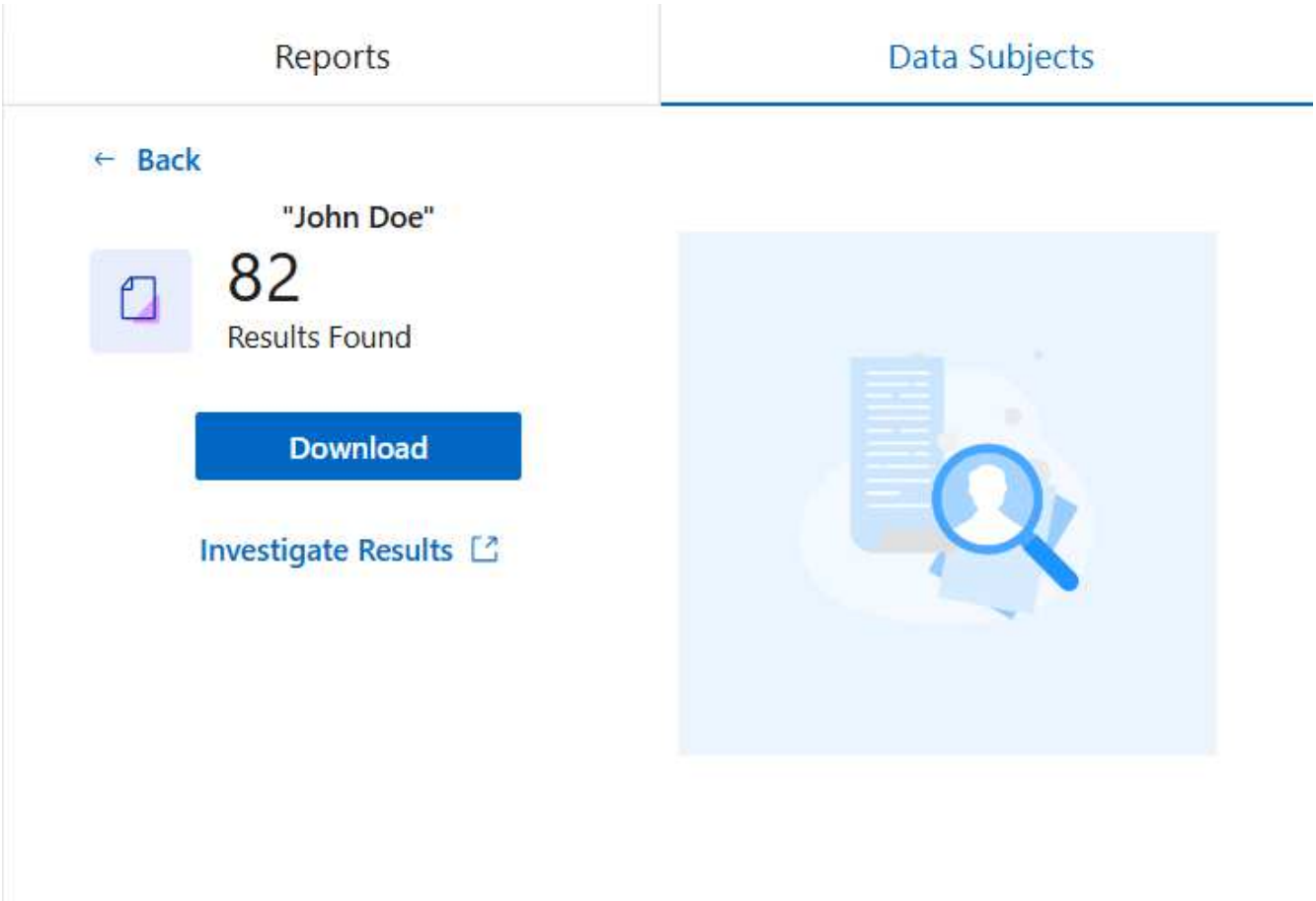
搜尋資料主體並下載報告

搜尋資料主體的全名或已知標識符，然後下載檔案清單報表或 DSAR 報表。您可以透過以下方式搜尋"任何個人資訊類型"。

搜尋資料主體的姓名時支援英語、德語、日語和西班牙語。稍後將添加對更多語言的支援。

步驟

1. 從資料分類選單中，選擇*合規性*。
2. 在合規性頁面中，找到資料主體選項卡。
3. 在「資料主體」部分，輸入名稱或已知標識符，然後選擇「搜尋」。
4. 搜尋完成後，選擇下載以存取資料主體存取請求回應。選擇調查結果以在資料調查頁面中查看更多資訊。



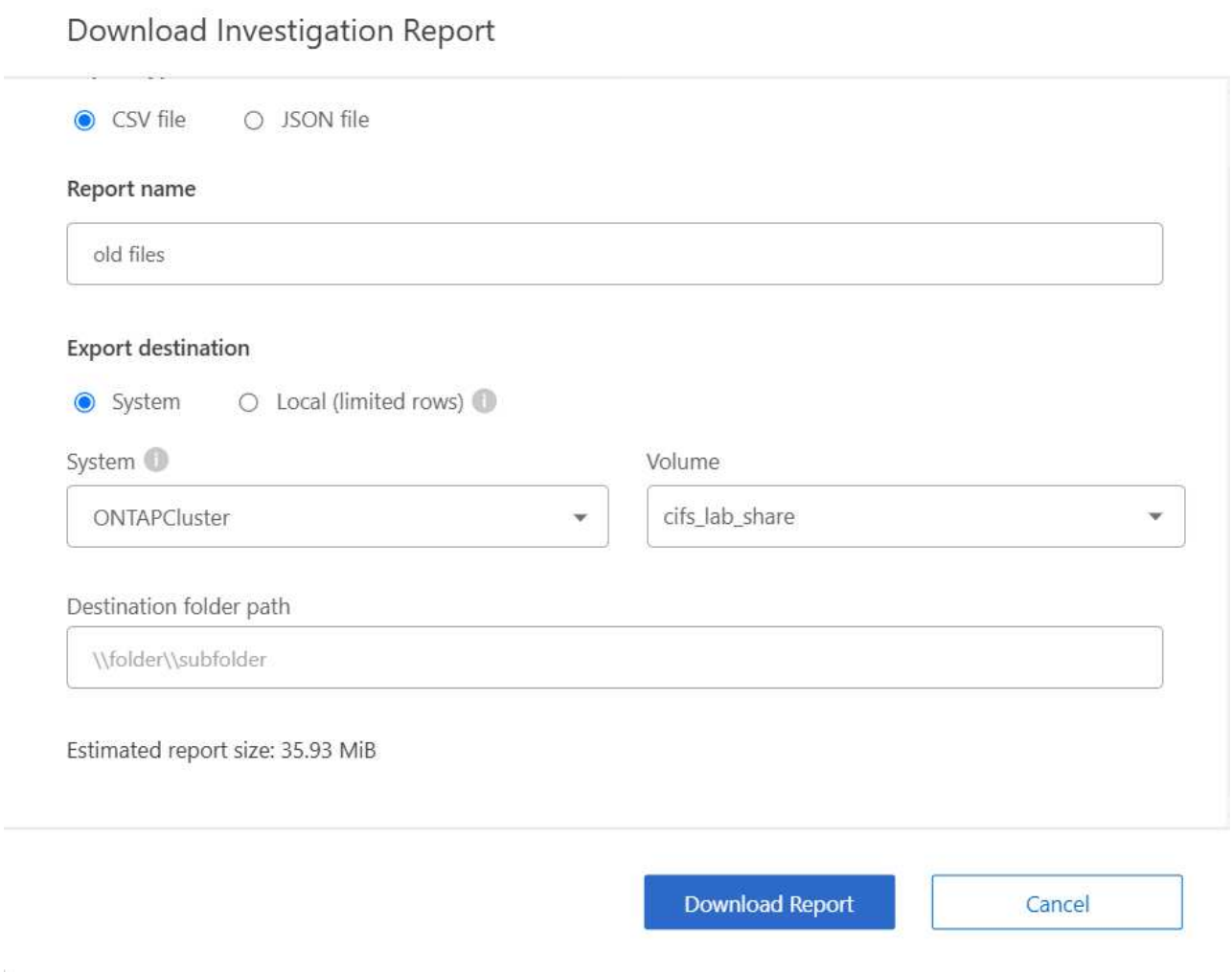
5. 查看資料分類中的結果或透過選擇下載圖示將其下載為報告。
   a. 選擇下載圖示後，配置您的下載設定：
      - 選擇影片格式：CSV 或 JSON
      - 輸入*報告名稱*

- 選擇匯出目的地：*系統*或您的*本機*機器。

  如果您選擇系統，則會下載所有資料。您還必須選擇*系統*、磁碟區*和*目標資料夾路徑。

如果您選擇*本地*，則會將報告限制為前 10,000 行非結構化資料；5,000 行非結構化資料和 1,000 行結構化資料。

a. 選擇下載報告開始下載。



健康保險流通與責任法案（HIPAA）報告

健康保險流通與責任法案 (HIPAA) 報告可以幫助您識別包含健康資訊的文件。它旨在幫助您的組織遵守 HIPAA 資料隱私法的要求。資料分類尋找的資訊包括：

- 健康參考模式
- ICD-10-CM 醫療代碼
- ICD-9-CM 醫療代碼
- HR - 健康類別
- 健康應用資料類別

該報告包含以下資訊：

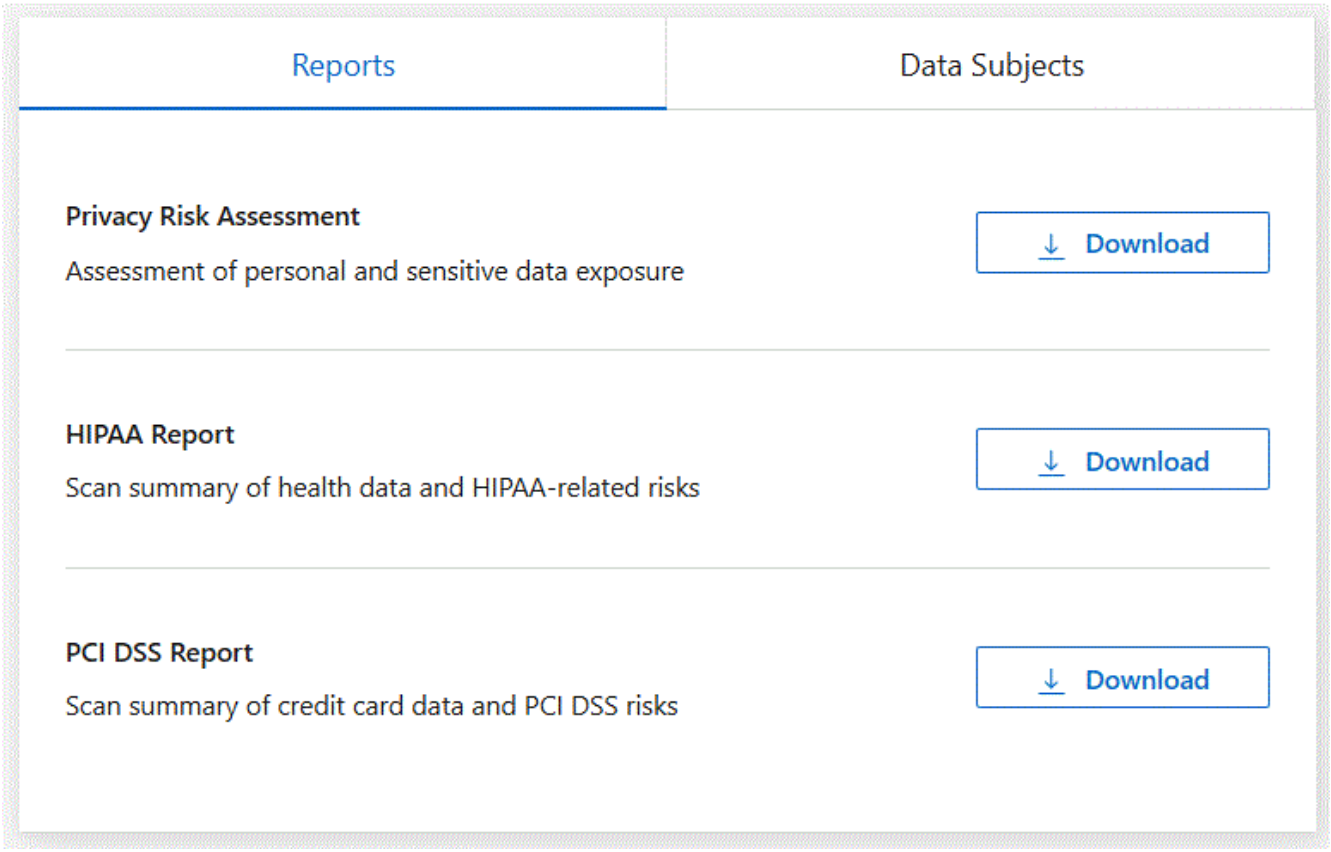
- 概述：有多少文件包含健康資訊以及在哪些系統中。
- 加密：加密或未加密系統中包含健康資訊的檔案的百分比。此資訊特定於Cloud Volumes ONTAP。
- 勒索軟體防護：在啟用或未啟用勒索軟體防護的系統上，包含健康資訊的檔案的百分比。此資訊特定於Cloud Volumes ONTAP。
- 保留：文件最後修改的時間範圍。這很有用，因為您不應該將健康資訊保存超過處理所需的時間。
- 健康資訊分發：發現健康資訊的系統以及是否啟用了加密和勒索軟體保護。

產生 **HIPAA** 報告

轉到“合規性”選項卡以產生報告。

步驟

1. 從資料分類選單中，選擇*合規性*。
2. 找到報告窗格。選擇*HIPAA 報告*旁邊的下載圖示。



結果

資料分類產生 PDF 報告。

支付卡產業資料安全標準 (PCI DSS) 報告

支付卡產業資料安全標準 (PCI DSS) 報告可以幫助您識別文件中信用卡資訊的分佈。

該報告包含以下資訊：

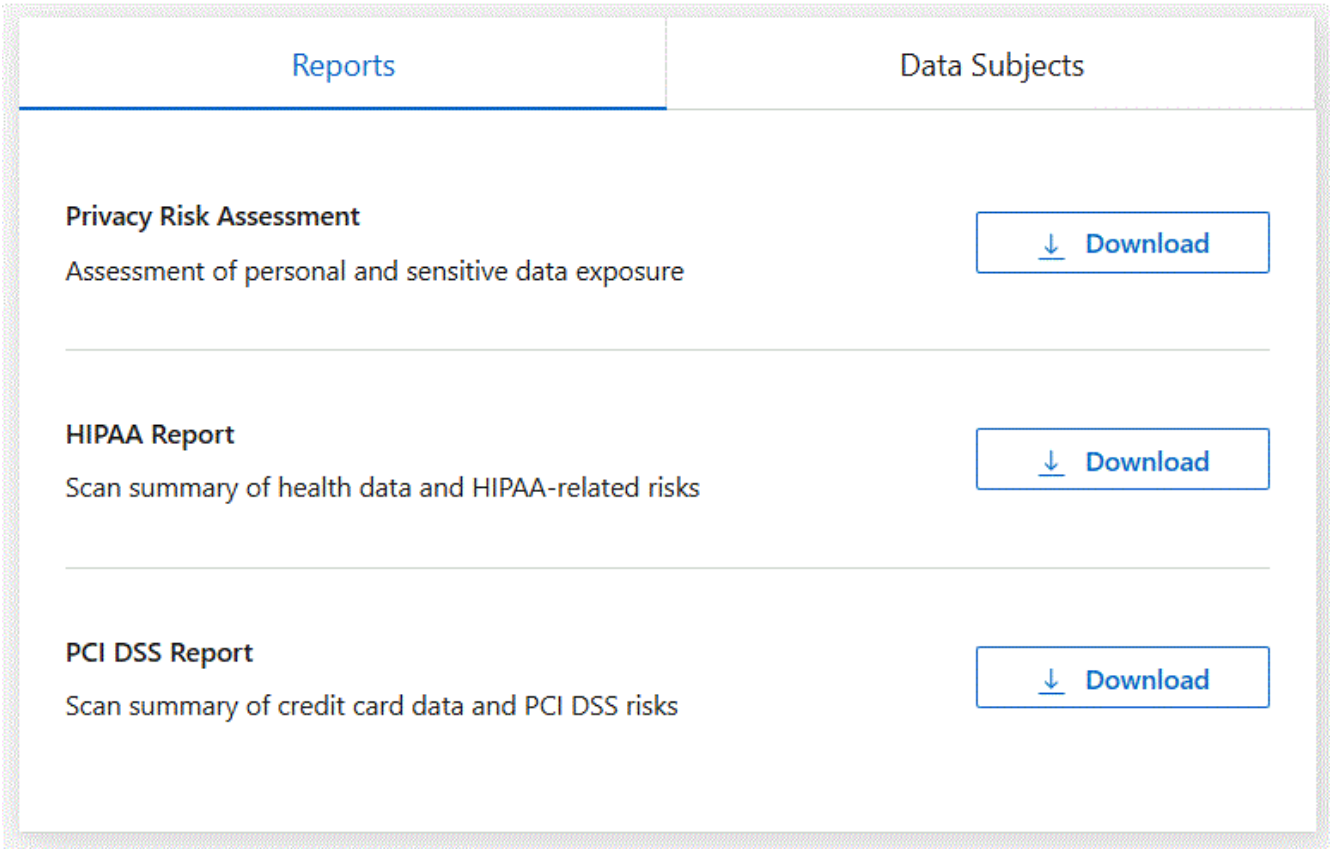
- 概述：有多少文件包含信用卡資訊以及在哪些系統中。
- 加密：加密或未加密系統中包含信用卡資訊的檔案的百分比。此資訊特定於Cloud Volumes ONTAP。
- 勒索軟體保護：在啟用或未啟用勒索軟體保護的系統上，包含信用卡資訊的檔案的百分比。此資訊特定於Cloud Volumes ONTAP。
- 保留：文件最後修改的時間範圍。這很有用，因為您不應該將信用卡資訊保存的時間超過處理所需的時間。
- 信用卡資訊分發：發現信用卡資訊的系統以及是否啟用了加密和勒索軟體保護。

產生 **PCI DSS** 報告

轉到"合規性"選項卡以產生報告。

步驟

1. 從資料分類選單中，選擇*合規性*。
2. 找到報告窗格。選擇*PCI DSS 報表*旁邊的下載圖示。



結果

資料分類會產生一份 PDF 報告，您可以根據需要查看並傳送給其他群組。

隱私風險評估報告

隱私權風險評估報告概述了您組織的隱私權風險狀況，這是 GDPR 和 CCPA 等隱私權法規所要求的。

該報告包含以下資訊：

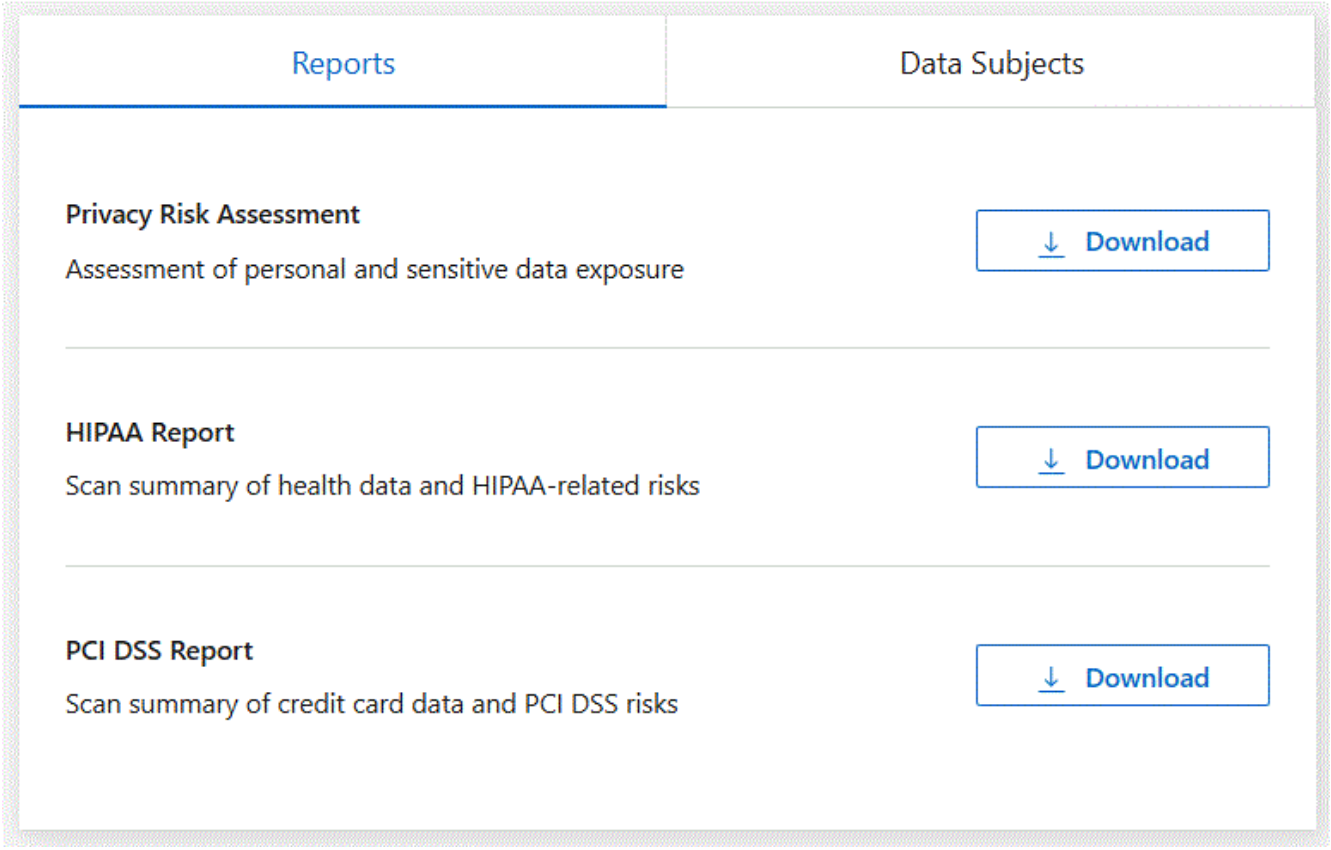
- 合規狀態：嚴重性評分和資料分佈，無論是非敏感資料、個人資料或敏感個人資料。
- 評估概述：發現的個人資料類型以及資料類別的細分。
- 本次評估中的資料主體：按地點劃分的已找到國家識別碼的人數。

產生隱私權風險評估報告

轉到“合規性”選項卡以產生報告。

步驟

1. 從資料分類選單中，選擇*合規性*。
2. 找到報告窗格。選擇*隱私風險評估報告*旁邊的下載圖示。



結果

資料分類會產生一份 PDF 報告，您可以根據需要查看並傳送給其他群組。

嚴重程度評分

資料分類根據三個變數計算隱私風險評估報告的嚴重性分數：

- 個人資料佔所有資料的百分比。
- 敏感個人資料佔所有資料的比例。
- 包含資料主體的文件百分比，由國家識別碼（例如國民身分證、社會安全號碼和稅號）決定。

決定分數的邏輯如下：

嚴重程度評分	邏輯
0	所有三個變數都恰好為 0%
1	其中一個變數大於 0%
2	其中一個變數大於3%
3	其中兩個變數大於 3%
4	其中三個變數大於 3%
5	其中一個變數大於6%
6	其中兩個變數大於 6%
7	其中三個變數大於 6%
8	其中一個變數大於15%
9	其中兩個變數大於 15%
10	其中三個變數大於 15%

監控NetApp Data Classification的運作狀況

NetApp Data Classification健康監視器儀表板提供即時監控和效能洞察。健康監視器會捕獲有關您的資料分類基礎架構、系統運行狀況、使用指標和利用率資料的信息，使您能夠識別和解決問題。

健康監測洞察

健康監測儀錶板以四類資訊呈現資訊。

- 基礎設施狀況

  查看版本狀態、系統穩定性、部署類型和機器規模等資訊。

- 問題容器

  查看「問題容器」字段，以了解哪些容器已停止或頻繁重新啟動。利用這些資訊調查具體的容器。

- 系統資訊

  系統資訊面板會擷取有關NetApp Console和資料分類的關鍵訊息，例如公用和私人 IP 位址、主機名稱、作業系統、控制台版本和控制台 ID。

- 用途和使用方法

  查看 CPU 使用率、磁碟使用率、磁碟使用率和記憶體使用率。這些值以儲存單位（GB）或總使用量的百分比顯示。如果任何欄位顯示警告，請選擇該警告以取得相關資訊和補救建議。

訪問健康監測儀表板

1. 在資料分類中，選擇配置。
2. 在「配置」標題下，選擇「資料分類運作狀況監視器」。
3. 在健康監測儀表板中，您可以：
   - 審查使用情況和利用情況。如果任何使用情況或使用率指標顯示警告，請選擇該警告以取得解決問題的建議。
   - 切換圖表以顯示 CPU 使用率、磁碟使用率、磁碟使用率和記憶體使用率。您可以變更 x 軸，以按小時（6、12 或 24 小時）或天（2、7 或 14 天）顯示內容。
   - 刷新儀錶板以查看最新資料指標。