



啟動資料來源掃描 NetApp Data Classification

NetApp
March 02, 2026

目錄

啟動資料來源掃描	1
使用NetApp Data Classification掃描資料來源	1
映射掃描和分類掃描之間有什麼區別	1
使用NetApp Data Classification掃描Amazon FSx for ONTAP卷	4
開始之前	5
部署資料分類實例	5
在您的系統中啟用資料分類	5
驗證資料分類是否有權存取卷	6
啟用和停用磁碟區上的掃描	7
掃描資料保護卷	8
使用NetApp Data Classification掃描Azure NetApp Files卷	9
發現要掃描的Azure NetApp 檔案系統Discover the Azure NetApp Files system that you want to scan	9
部署資料分類實例	9
在您的系統中啟用資料分類	9
驗證資料分類是否有權存取卷	10
啟用或停用磁碟區掃描	11
使用NetApp Data Classification掃描Cloud Volumes ONTAP和本地ONTAP卷	12
先決條件	12
驗證資料分類是否有權存取卷	12
啟用或停用磁碟區掃描	13
使用NetApp Data Classification	14
審查先決條件	14
部署資料分類實例	15
新增資料庫伺服器	15
啟用和停用資料庫模式掃描	16
使用NetApp Data Classification掃描Google Cloud NetApp Volumes	17
發現您要掃描的Google Cloud NetApp Volumes系統	17
部署資料分類實例	17
在您的系統中啟用資料分類	17
驗證資料分類是否有權存取卷	18
啟用和停用磁碟區上的掃描	19
使用NetApp Data Classification掃描檔案共用	20
先決條件	20
建立文件共享組	20
編輯檔案共享群組	22
追蹤掃描進度	24
使用NetApp Data Classification掃描StorageGRID數據	25
查看StorageGRID要求	25
部署資料分類實例	25

將StorageGRID服務新增至資料分類	25
啟用並停用StorageGRID桶上的掃描	26

啟動資料來源掃描

使用NetApp Data Classification掃描資料來源

NetApp Data Classification 會掃描您所選擇的儲存庫（包括磁碟區、資料庫結構或其他使用者資料）中的資料，以識別個人和敏感資料。Data Classification 接著會對您的組織資料進行對應、分類每個檔案，並識別資料中的預定義模式。掃描的結果是一份包含個人資訊、敏感個人資訊、資料類別和檔案類型的索引。

初步掃描後，資料分類將以循環方式持續掃描您的資料以偵測增量變化。這就是為什麼保持實例運行很重要。

您可以在磁碟區層級或資料庫模式層級啟用和停用掃描。

映射掃描和分類掃描之間有什麼區別

您可以在資料分類中進行兩種類型的掃描：

- 僅映射掃描僅提供資料的進階概覽，並在選定的資料來源上執行。僅映射掃描比映射和分類掃描花費的時間更少，因為它們不存取文件來查看其中的資料。您可能希望首先執行此操作來確定研究領域，然後對這些領域執行地圖和分類掃描。
- 地圖和分類掃描 為您的資料提供深層掃描。

下表顯示了一些差異：

特徵	映射和分類掃描	僅映射掃描
掃描速度	慢的	快速地
定價	自由的	自由的
容量	限制為 500 TiB*	限制為 500 TiB*
文件類型和已使用容量列表	是的	是的
文件數量和已用容量	是的	是的
文件的年齡和大小	是的	是的
能夠運行" 數據映射報告 "	是的	是的
數據調查頁面查看文件詳細信息	是的	不
在文件中搜尋名稱	是的	不
創造" 已儲存的查詢 "提供自訂搜尋結果	是的	不
能夠運行其他報告	是的	不
能夠查看文件中的元資料**	不	是的

* 資料分類不會對其可掃描的資料量施加限制。每個控制台代理程式支援掃描和顯示 500 TiB 的資料。要掃描超過 500 TiB 的數據，"[安裝另一個控制台代理](#)"然後"[部署另一個資料分類實例](#)"。+ 控制台 UI 顯示來自單一連接器的資料。有關查看來自多個控制台代理的資料的提示，請參閱"[使用多個控制台代理](#)"。

** 在映射掃描期間從檔案中提取以下元資料：

- 系統
- 系統類型
- 儲存庫
- 文件類型
- 已用容量
- 文件數量
- 文件大小
- 文件創建
- 文件上次訪問
- 文件上次修改時間
- 文件發現時間
- 權限擷取

治理儀表板差異：

特徵	地圖和分類	地圖
過時的數據	是的	是的
非業務數據	是的	是的
重複文件	是的	是的
預定義已儲存的查詢	是的	不
預設儲存的查詢	是的	是的
DDA 報告	是的	是的
地圖報告	是的	是的
靈敏度等級檢測	是的	不
具有廣泛權限的敏感數據	是的	不
開放權限	是的	是的
數據時代	是的	是的
數據大小	是的	是的
類別	是的	不
文件類型	是的	是的

合規性儀表板差異：

特徵	地圖和分類	地圖
個人資訊	是的	不
敏感個人資訊	是的	不
隱私風險評估報告	是的	不
HIPAA 報告	是的	不
PCI DSS 報告	是的	不

調查過濾器差異：

特徵	地圖和分類	地圖
已儲存的查詢	是的	是的
系統類型	是的	是的
系統	是的	是的
儲存庫	是的	是的
文件類型	是的	是的
文件大小	是的	是的
創建時間	是的	是的
發現時間	是的	是的
上次修改時間	是的	是的
上次訪問	是的	是的
開放權限	是的	是的
檔案目錄路徑	是的	是的
類別	是的	不
敏感度等級	是的	不
識別符數量	是的	不
個人資料	是的	不
敏感個人數據	是的	不
資料主體	是的	不
重複項	是的	是的
分類狀態	是的	狀態始終為“見解有限”
掃描分析事件	是的	是的
文件哈希	是的	是的
有存取權限的使用者數	是的	是的
使用者/群組權限	是的	是的
文件所有者	是的	是的
目錄類型	是的	是的

使用NetApp Data Classification掃描Amazon FSx for ONTAP卷

完成幾個步驟即可使用NetApp Data Classification掃描Amazon FSx for ONTAP磁碟區。

開始之前

- 您需要 AWS 中一個活動的控制台代理來部署和管理資料分類。
- 建立系統時選擇的安全群組必須允許來自資料分類實例的流量。您可以使用連接到 FSx for ONTAP 檔案系統的 ENI 找到關聯的安全性群組，並使用 AWS 管理主控台對其進行編輯。

"Linux 執行個體的 AWS 安全群組"

"Windows 執行個體的 AWS 安全性群組"

"AWS 彈性網路介面 (ENI)"

- 確保以下連接埠對資料分類實例開放：
 - 對於 NFS – 連接埠 111 和 2049。
 - 對於 CIFS – 連接埠 139 和 445。

部署資料分類實例

"部署資料分類"如果尚未部署實例。

您應該在與 AWS 主控台代理程式和要掃描的 FSx 磁碟區相同的 AWS 網路中部署資料分類。

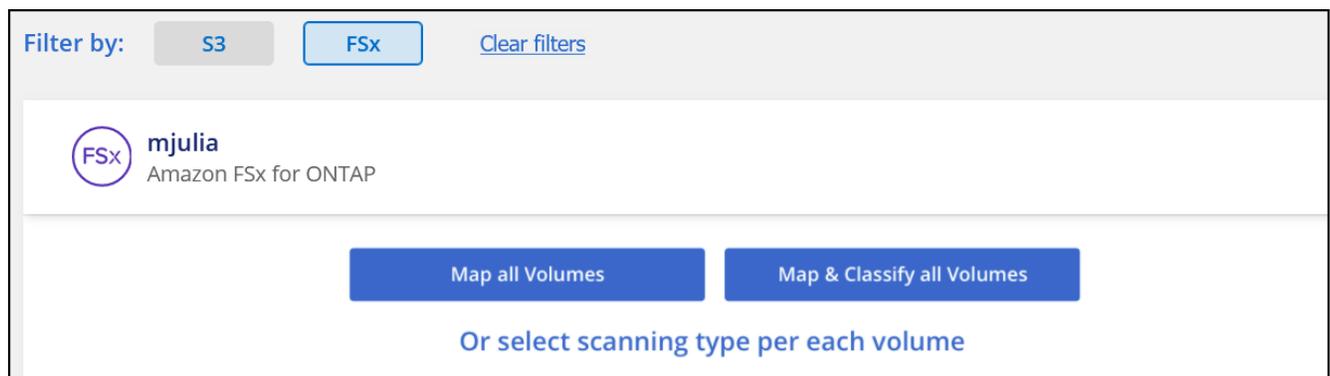
*注意：*掃描 FSx 磁碟區時，目前不支援在本機位置部署資料分類。

只要實例具有互聯網連接，資料分類軟體的升級就會自動進行。

在您的系統中啟用資料分類

您可以為 FSx for ONTAP 磁碟區啟用資料分類。

1. 從 NetApp Console，治理 > 分類。
2. 從資料分類選單中，選擇*配置*。



3. 選擇如何掃描每個系統中的磁碟區。"了解映射和分類掃描"：
 - 若要對應所有捲，請選擇*映射所有磁碟區*。
 - 若要對應和分類所有捲，請選擇*映射和分類所有捲*。

- 若要自訂每個磁碟區的掃描，請選擇*或選擇每個磁碟區的掃描類型*，然後選擇要對應和/或分類的磁碟區。

4. 在確認對話方塊中，選擇「核准」以使資料分類開始掃描您的磁碟區。

結果

資料分類開始掃描您在系統中選擇的磁碟區。一旦資料分類完成初始掃描，結果將在合規性儀表中提供。所需時間取決於資料量——可能是幾分鐘或幾小時。您可以透過導航到配置選單然後選擇系統配置來追蹤初始掃描的進度。在進度條中追蹤每次掃描的進度；您可以將滑鼠懸停在進度條上，以查看相對於磁碟區中總檔案數的掃描檔案數。



- 預設情況下，如果資料分類在 CIFS 中沒有寫入屬性權限，或者在 NFS 中沒有寫入權限，系統將不會掃描磁碟區中的文件，因為資料分類無法將「上次存取時間」還原為原始時間戳記。如果您不介意上次造訪時間是否重設，請選擇*或為每個磁碟區選擇掃描類型*。結果頁面有一個您可以啟用的設置，以便資料分類可以掃描卷，而不管權限如何。
- 資料分類僅掃描卷下的一個檔案共用。如果您的磁碟區中有多個共享，則需要將這些其他共享作為共享群組單獨掃描。["查看有關此數據分類限制的更多詳細信息"](#)。

驗證資料分類是否有權存取卷

透過檢查網路、安全群組和匯出策略，確保資料分類可以存取磁碟區。

您需要向資料分類提供 CIFS 憑證，以便它可以存取 CIFS 磁碟區。

步驟

1. 從資料分類選單中，選擇*配置*。
2. 在配置頁面上，選擇*查看詳細資訊*以查看狀態並修正任何錯誤。

例如，下圖顯示由於資料分類實例和磁碟區之間的網路連線問題，資料分類無法掃描磁碟區。

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	jrmclone	NFS	● No Access	Check network connectivity between the Data Sense ...

3. 確保資料分類實例與包含 FSx for ONTAP磁碟區的每個網路之間存在網路連線。



對於 FSx for ONTAP，資料分類只能掃描與控制台位於相同區域的磁碟區。

4. 確保 NFS 磁碟區匯出策略包含資料分類執行個體的 IP 位址，以便它可以存取每個磁碟區上的資料。
5. 如果您使用 CIFS，請向資料分類提供 Active Directory 憑證，以便它可以掃描 CIFS 磁碟區。
 - a. 從資料分類選單中，選擇*配置*。
 - b. 對於每個系統，選擇*編輯 CIFS 憑證*並輸入資料分類存取系統上的 CIFS 磁碟區所需的使用者名稱和密碼。

憑證可以是唯讀的，但提供管理員憑證可確保資料分類可以讀取任何需要提升權限的資料。憑證儲存在資料分類實例上。

如果您想要確保檔案的「上次存取時間」不會因資料分類掃描而改變，建議使用者在 CIFS 中具有寫入

屬性權限或在 NFS 中具有寫入權限。如果可能，請將 Active Directory 使用者設定為組織中具有所有檔案權限的父群組的一部分。

輸入憑證後，您應該會看到一條訊息，表示所有 CIFS 磁碟區均已成功驗證。

啟用和停用磁碟區上的掃描

您可以隨時從設定頁面啟動或停止任何系統上的掃描。您也可以將掃描從僅映射掃描切換到映射和分類掃描，反之亦然。建議您掃描系統中的所有磁碟區。



只有當您在標題區域中選擇了 **Map** 或 **Map & Classify** 設定時，才會自動掃描新增至系統的新磁碟區。當在標題區域設定為*自訂*或*關閉*時，您需要在系統中新增加的每個新磁碟區上啟動對應和/或完整掃描。

頁面頂部的「缺少「寫入」權限時掃描」開關預設為停用狀態。這意味著，如果資料分類在 CIFS 中沒有寫入屬性權限或在 NFS 中沒有寫入權限，系統將不會掃描文件，因為資料分類無法將「上次存取時間」恢復為原始時間戳記。如果您不介意是否重設上次造訪時間，請開啟開關，無論權限為何，都會掃描所有檔案。["了解更多"](#)。



只有當您在標題區域中設定了 **Map** 或 **Map & Classify** 設定時，才會自動掃描新增到系統的新磁碟區。當所有磁碟區的設定都是「自訂」或「關閉」時，您需要為新增的每個新磁碟區手動啟動掃描。

Volumes selected for Data Classification scan (11/15)

Off Map Map & Classify Custom Mapping vs. Classification → Retry All Edit CIFS Credentials

Scan when missing "write" permissions

Scan	Storage repository (Volume)	Type	Mapping status	Scan progress	Required Action
Off Map Map & Classify	bank_statements	NFS	Paused 2025-07-16 08:51 Last full cycle: 2025-07-16 08:50	Mapped 219 Classified 219	...
Off Map Map & Classify ☆	cifs_labs	CIFS	Finished 2025-10-06 10:29 Last full cycle: 2025-10-06 10:29	Mapped 5.2K	...
Off Map Map & Classify	cifs_labs_second	CIFS			...
Off Map Map & Classify	cifs_labs_second_insight	NFS			...
Off Map Map & Classify	datasence	NFS	Paused 2025-07-15 09:10 Last full cycle: 2025-07-15 09:06	Mapped 127K	...

步驟

1. 從資料分類選單中，選擇*配置*。
2. 選擇一個系統，然後選擇*配置*。
3. 若要啟用或停用所有磁碟區的掃描，請在所有磁碟區上方的標題中選擇對應、對應和分類或關閉。

若要啟用或停用對單一卷的掃描，請在清單中找到該卷，然後選擇卷名稱旁的映射、映射和分類或關閉。

結果

當您啟用掃描時，資料分類將開始掃描您在系統中選擇的磁碟區。一旦資料分類開始掃描，結果就會開始出現在

合規性儀表中。掃描完成時間取決於資料量，從幾分鐘到幾小時不等。

掃描資料保護卷

預設情況下，不會掃描資料保護 (DP) 卷，因為它們未暴露在外部，且資料分類無法存取它們。這些是來自 FSx for ONTAP檔案系統的SnapMirror操作的目標磁碟區。

最初，磁碟區清單將這些磁碟區標識為_類型_ DP，其_狀態_ 未掃描*和_所需操作_ *啟用對 DP 磁碟區的存取。

The screenshot shows the 'Working Environment Name' Configuration page. At the top, it says '22/28 Volumes selected for compliance scan'. There are two buttons: 'Enable Access to DP Volumes' (highlighted with a red box) and 'Edit CIFS Credentials'. Below this is a table with columns: Scan, Storage Repository (Volume), Type, Status, and Required Action. The table contains three rows:

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off	VolumeName1	DP	Not Scanning	Enable access to DP Volumes
Off	VolumeName2	NFS	Continuously Scanning	
Off	VolumeName3	CIFS	Not Scanning	

步驟

如果要掃描這些資料保護磁碟區：

1. 從資料分類選單中，選擇*配置*。
2. 選擇頁面頂部的「啟用對 DP 磁碟區的存取」*。
3. 查看確認訊息並再次選擇*啟用對 DP 磁碟區的存取*。
 - 最初在來源 FSx for ONTAP檔案系統中建立為 NFS 磁碟區的磁碟區已啟用。
 - 最初在來源 FSx for ONTAP檔案系統中建立為 CIFS 磁碟區的磁碟區會要求您輸入 CIFS 憑證來掃描這些 DP 磁碟區。如果您已經輸入了 Active Directory 憑證，以便資料分類可以掃描 CIFS 卷，您可以使用這些憑證，或者您可以指定一組不同的管理員憑證。

The screenshot shows the 'Provide Active Directory Credentials' dialog box. It has two radio buttons: 'Use existing CIFS Scanning Credentials (user1@domain2)' (selected and highlighted with a red box) and 'Use Custom Credentials'. Below the radio buttons are two input fields: 'Active Directory Domain' and 'DNS IP Address'. At the bottom, there are two buttons: 'Enable Access to DP Volumes' and 'Cancel'.

The screenshot shows the 'Provide Active Directory Credentials' dialog box. It has two radio buttons: 'Use existing CIFS Scanning Credentials (user1@domain2)' and 'Use Custom Credentials' (selected and highlighted with a red box). Below the radio buttons are two input fields: 'Username' and 'Password'. Below these are two more input fields: 'Active Directory Domain' and 'DNS IP Address'. At the bottom, there are two buttons: 'Enable Access to DP Volumes' and 'Cancel'.

4. 啟動您想要掃描的每個 DP 磁碟區。

結果

一旦啟用，資料分類將從每個啟動掃描的 DP 磁碟區建立一個 NFS 共用。共享導出策略僅允許從資料分類實例進行存取。

如果您在最初啟用對 DP 磁碟區的存取權時沒有 CIFS 資料保護卷，後來又添加了一些，則按鈕 啟用對 CIFS DP 的存取 將出現在設定頁面的頂部。選擇此按鈕並新增 CIFS 憑證以啟用對這些 CIFS DP 磁碟區的存取。



Active Directory 憑證僅在第一個 CIFS DP 磁碟區的儲存 VM 中註冊，因此該 SVM 上的所有 DP 磁碟區都將掃描。駐留在其他 SVM 上的任何磁碟區都不會註冊 Active Directory 憑證，因此不會掃描這些 DP 磁碟區。

使用 NetApp Data Classification 掃描 Azure NetApp Files 卷

完成幾個步驟即可開始使用適用於 Azure NetApp Files 的 NetApp Data Classification。

發現要掃描的 Azure NetApp 檔案系統 **Discover the Azure NetApp Files system that you want to scan**

如果要掃描的 Azure NetApp Files 系統尚未作為系統出現在 NetApp Console 中，["將其新增至系統頁面"](#)。

部署資料分類實例

["部署資料分類"](#) 如果尚未部署實例。

掃描 Azure NetApp Files 區時，資料分類必須部署在雲端中，並且必須部署在與要掃描的磁碟區相同的區域中。

*注意：*掃描 Azure NetApp Files 區時，目前不支援在本機位置部署資料分類。

在您的系統中啟用資料分類

您可以在 Azure NetApp Files 區上啟用資料分類。

1. 從資料分類選單中，選擇 ***配置***。



2. 選擇如何掃描每個系統中的磁碟區。["了解映射和分類掃描"](#)：
 - 若要對應所有捲，請選擇 ***映射所有磁碟區***。
 - 若要對應和分類所有捲，請選擇 ***映射和分類所有捲***。
 - 若要自訂每個磁碟區的掃描，請選擇 ***或選擇每個磁碟區的掃描類型***，然後選擇要對應或對應和分類的磁碟區。

看[啟用或停用磁碟區掃描](#)了解詳情。

3. 在確認對話方塊中，選擇*批准*。

結果

資料分類開始掃描您在系統中選擇的磁碟區。一旦資料分類完成初始掃描，結果就會顯示在合規性儀表板中。所需時間取決於資料量——可能是幾分鐘或幾小時。您可以透過導航到配置選單然後選擇系統配置來追蹤初始掃描的進度。資料分類顯示每次掃描的進度條。您可以將滑鼠懸停在進度條上，以查看相對於磁碟區中檔案總數的已掃描檔案數。

- 預設情況下，如果資料分類在 CIFS 中沒有寫入屬性權限，或者在 NFS 中沒有寫入權限，系統將不會掃描磁碟區中的文件，因為資料分類無法將「上次存取時間」還原為原始時間戳記。如果您不介意上次造訪時間是否重設，請選擇*或為每個磁碟區選擇掃描類型*。結果頁面有一個您可以啟用的設置，以便資料分類可以掃描卷，而不管權限如何。
- 資料分類僅掃描卷下的一個檔案共用。如果您的磁碟區中有多個共享，則需要將這些其他共享作為共享群組單獨掃描。["了解此資料分類限制"](#)。

驗證資料分類是否有權存取卷

透過檢查網路、安全群組和匯出策略，確保資料分類可以存取磁碟區。您需要為資料分類提供 CIFS 憑證，以便它可以存取 CIFS 磁碟區。



對於 Azure NetApp Files，資料分類只能掃描與控制台位於同一區域的磁碟區。

清單

- 確保資料分類實例與包含 Azure NetApp Files 區的每個網路之間存在網路連線。
- 確保以下連接埠對資料分類實例開放：
 - 對於 NFS – 連接埠 111 和 2049。
 - 對於 CIFS – 連接埠 139 和 445。
- 確保 NFS 磁碟區匯出策略包含資料分類執行個體的 IP 位址，以便它可以存取每個磁碟區上的資料。

步驟

1. 從資料分類選單中，選擇*配置*。
 - a. 如果您使用 CIFS (SMB)，請確保 Active Directory 憑證正確。對於每個系統，選擇*編輯 CIFS 憑證*，然後輸入資料分類存取系統上的 CIFS 磁碟區所需的使用者名稱和密碼。

憑證可以是唯讀的；提供管理員憑證可確保資料分類可以讀取任何需要提升權限的資料。憑證儲存在資料分類實例上。

如果您想要確保檔案的「上次存取時間」不會因資料分類掃描而改變，建議使用者在 CIFS 中具有寫入屬性權限或在 NFS 中具有寫入權限。如果可能，請將 Active Directory 使用者設定為組織中具有所有檔案權限的父群組的一部分。

輸入憑證後，您應該會看到一條訊息，表示所有 CIFS 磁碟區均已成功驗證。

Name:

Newdatastore

Volumes:

● 12 Continuously Scanning ● 8 Not Scanning

[View Details](#)

CIFS Credentials Status:

✔ Valid CIFS credentials for all accessible volumes

[Edit CIFS Credentials](#)

- 在設定頁面上，選擇*查看詳細資訊*以查看每個 CIFS 和 NFS 磁碟區的状态。如有必要，請修正任何錯誤，例如網路連線問題。

啟用或停用磁碟區掃描

您可以隨時從設定頁面啟動或停止任何系統上的掃描。您也可以將掃描從僅映射掃描切換到映射和分類掃描，反之亦然。建議您掃描系統中的所有磁碟區。



只有當您在標題區域中選擇了 **Map** 或 **Map & Classify** 設定時，才會自動掃描新增至系統的新磁碟區。當在標題區域設定為*自訂*或*關閉*時，您需要在系統中新增加的每個新磁碟區上啟動對應和/或完整掃描。

頁面頂部的「缺少「寫入」權限時掃描」開關預設為停用狀態。這意味著，如果資料分類在 CIFS 中沒有寫入屬性權限或在 NFS 中沒有寫入權限，系統將不會掃描文件，因為資料分類無法將「上次存取時間」恢復為原始時間戳記。如果您不介意是否重設上次造訪時間，請開啟開關，無論權限為何，都會掃描所有檔案。[了解更多](#)。



只有當您在標題區域中設定了 **Map** 或 **Map & Classify** 設定時，才會自動掃描新增到系統的新磁碟區。當所有磁碟區的設定都是「自訂」或「關閉」時，您需要為新增的每個新磁碟區手動啟動掃描。

Volumes selected for Data Classification scan (11/15)

Off Map Map & Classify Custom Mapping vs. Classification →

Scan when missing "write" permissions

[Retry All](#) [Edit CIFS Credentials](#)

Scan	Storage repository (Volume)	Type	Mapping status	Scan progress	Required Action
Off Map Map & Classify	bank_statements	NFS	● Paused 2025-07-16 08:51 Last full cycle: 2025-07-16 08:50	Mapped 219 Classified 219	...
Off Map Map & Classify ☆	cifs_labs	CIFS	● Finished 2025-10-06 10:29 Last full cycle: 2025-10-06 10:29	Mapped 5.2K	...
Off Map Map & Classify	cifs_labs_second	CIFS			...
Off Map Map & Classify	cifs_labs_second_insight	NFS			...
Off Map Map & Classify	datasence	NFS	● Paused 2025-07-15 09:10 Last full cycle: 2025-07-15 09:06	Mapped 127K	...

步驟

- 從資料分類選單中，選擇*配置*。
- 選擇一個系統，然後選擇*配置*。
- 若要啟用或停用所有磁碟區的掃描，請在所有磁碟區上方的標題中選擇對應、對應和分類或關閉。

若要啟用或停用對單一卷的掃描，請在清單中找到該卷，然後選擇卷名稱旁的映射、映射和分類或關閉。

結果

當您啟用掃描時，資料分類將開始掃描您在系統中選擇的磁碟區。一旦資料分類開始掃描，結果就會開始出現在合規性儀表中。掃描完成時間取決於資料量，從幾分鐘到幾小時不等。

使用NetApp Data Classification掃描Cloud Volumes ONTAP和本地ONTAP卷

完成幾個步驟即可開始使用NetApp Data Classification掃描您的Cloud Volumes ONTAP和本機ONTAP磁碟區。

先決條件

在啟用資料分類之前，請確保您具有支援的配置。

- 如果您正在掃描可透過網路存取的Cloud Volumes ONTAP和本機ONTAP系統，您可以"[在雲端部署資料分類](#)"或者"[在可以存取互聯網的本地位置](#)"。
- 如果您要掃描安裝在沒有網路存取的暗站中的本機ONTAP系統，則需要"[在沒有網路存取的相同本地位置部署資料分類](#)"。這要求將控制台代理部署在同一本地位置。

驗證資料分類是否有權存取卷

透過檢查網路、安全群組和匯出策略，確保資料分類可以存取磁碟區。您需要向資料分類提供 CIFS 憑證，以便它可以存取 CIFS 磁碟區。

清單

- 確保資料分類實例與包含Cloud Volumes ONTAP或本地ONTAP叢集的磁碟區的每個網路之間存在網路連線。
- 確保Cloud Volumes ONTAP的安全群組允許來自資料分類實例的入站流量。

您可以為來自資料分類實例的 IP 位址的流量開啟安全性群組，也可以為來自虛擬網路內部的所有流量開啟安全性群組。

- 確保 NFS 磁碟區匯出策略包含資料分類執行個體的 IP 位址，以便它可以存取每個磁碟區上的資料。

步驟

1. 從資料分類選單中，選擇*配置*。

Governance Compliance Investigation Classification settings Policies **Configuration**

ONTAPCluster Scan Configuration

Volumes selected for Classification scan (9/13) 🔍

Mapping vs. Classification →

Scan when missing "write" permissions

Scan	Storage Repository (Volume)	Type	Mapping status	Scan progress	Required Action
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	bank_statements	NFS	• Error 2025-01-09 18:53 Last full cycle: 2025-01-09 18:48	Mapped 210 Classified 210	<input type="button" value="Retry"/> ...
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	cifs_labs	CIFS			...
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	cifs_labs_second	CIFS			...
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	datasence	NFS	• Error 2025-01-12 06:11 Last full cycle: 2025-01-12 06:06	Mapped 127K Classified 127K	<input type="button" value="Retry"/> ...
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	german_data	NFS	• Error 2024-10-10 01:35 Last full cycle: 2024-10-10 01:29	Mapped 13 Classified 13	<input type="button" value="Retry"/> ...
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	german_data_share	CIFS			...

1-13 of 13

- 如果您使用 CIFS，請向資料分類提供 Active Directory 憑證，以便它可以掃描 CIFS 磁碟區。對於每個系統，選擇*編輯 CIFS 憑證*並輸入資料分類存取系統上的 CIFS 磁碟區所需的使用者名稱和密碼。

憑證可以是唯讀的，但提供管理員憑證可確保資料分類可以讀取任何需要提升權限的資料。憑證儲存在資料分類實例上。

如果您想要確保檔案的「上次存取時間」不會因資料分類掃描而改變，建議使用者在 CIFS 中具有寫入屬性權限或在 NFS 中具有寫入權限。如果可能，請將 Active Directory 使用者設定為組織中具有所有檔案權限的父群組的一部分。

如果您正確輸入了憑證，則會出現一則訊息確認所有 CIFS 磁碟區均已成功驗證。

- 在設定頁面上，選擇*設定*以查看每個 CIFS 和 NFS 磁碟區的狀態並修正任何錯誤。

啟用或停用磁碟區掃描

您可以隨時從設定頁面啟動或停止任何系統上的掃描。您也可以將掃描從僅映射掃描切換到映射和分類掃描，反之亦然。建議您掃描系統中的所有磁碟區。



只有當您在標題區域中選擇了 **Map** 或 **Map & Classify** 設定時，才會自動掃描新增至系統的新磁碟區。當在標題區域設定為*自訂*或*關閉*時，您需要在系統中新增的每個新磁碟區上啟動對應和/或完整掃描。

頁面頂部的「缺少「寫入」權限時掃描」開關預設為停用狀態。這意味著，如果資料分類在 CIFS 中沒有寫入屬性權限或在 NFS 中沒有寫入權限，系統將不會掃描文件，因為資料分類無法將「上次存取時間」恢復為原始時間戳記。如果您不介意是否重設上次造訪時間，請開啟開關，無論權限為何，都會掃描所有檔案。["了解更多"](#)。



只有當您在標題區域中設定了 **Map** 或 **Map & Classify** 設定時，才會自動掃描新增到系統的新磁碟區。當所有磁碟區的設定都是「自訂」或「關閉」時，您需要為新增的每個新磁碟區手動啟動掃描。

Volumes selected for Data Classification scan (11/15)

Off | Map | Map & Classify | Custom Mapping vs. Classification → Retry All Edit CIFS Credentials

Scan when missing "write" permissions

Scan	Storage repository (Volume)	Type	Mapping status	Scan progress	Required Action
Off Map Map & Classify	bank_statements	NFS	<ul style="list-style-type: none"> Paused 2025-07-16 08:51 Last full cycle: 2025-07-16 08:50 	Mapped 219 Classified 219	...
Off Map Map & Classify ☆	cifs_labs	CIFS	<ul style="list-style-type: none"> Finished 2025-10-06 10:29 Last full cycle: 2025-10-06 10:29 	Mapped 5.2K	...
Off Map Map & Classify	cifs_labs_second	CIFS			...
Off Map Map & Classify	cifs_labs_second_insight	NFS			...
Off Map Map & Classify	datasence	NFS	<ul style="list-style-type: none"> Paused 2025-07-15 09:10 Last full cycle: 2025-07-15 09:06 	Mapped 127K	...

步驟

1. 從資料分類選單中，選擇*配置*。
2. 選擇一個系統，然後選擇*配置*。
3. 若要啟用或停用所有磁碟區的掃描，請在所有磁碟區上方的標題中選擇對應、對應和分類或關閉。

若要啟用或停用對單一卷的掃描，請在清單中找到該卷，然後選擇卷名稱旁的映射、映射和分類或關閉。

結果

當您啟用掃描時，資料分類將開始掃描您在系統中選擇的磁碟區。一旦資料分類開始掃描，結果就會開始出現在合規性儀表中。掃描完成時間取決於資料量，從幾分鐘到幾小時不等。



資料分類僅掃描卷下的一個檔案共用。如果您的磁碟區中有多個共享，則需要將這些其他共享作為共享群組單獨掃描。["查看有關此數據分類限制的更多詳細信息"](#)。

使用NetApp Data Classification

完成幾個步驟即可開始使用NetApp Data Classification掃描資料庫模式。

審查先決條件

在啟用資料分類之前，請查看以下先決條件，以確保您具有受支援的配置。

支援的資料庫

資料分類可以掃描以下資料庫中的模式：

- 亞馬遜關係型資料庫服務 (Amazon RDS)
- MongoDB
- MySQL
- 甲骨文
- PostgreSQL
- SAP HANA
- SQL 伺服器 (MSSQL)



資料庫中必須啟用統計資訊收集功能。

資料庫要求

任何與資料分類實例連接的資料庫都可以掃描，無論它託管在何處。您只需要以下資訊即可連接到資料庫：

- IP 位址或主機名
- 港口
- 服務名稱（僅用於存取 Oracle 資料庫）
- 允許讀取架構的憑證

選擇使用者名稱和密碼時，請務必選擇對要掃描的所有模式和表格具有完全讀取權限的使用者名稱和密碼。我們建議您為資料分類系統建立一個具有所有必需權限的專用使用者。



對於 MongoDB，需要只讀管理員角色。

部署資料分類實例

如果尚未部署實例，則部署資料分類。

如果您正在掃描可透過網際網路存取的資料庫模式，您可以["在雲端部署資料分類"](#)或者["在可以存取網際網路的本地位置部署資料分類"](#)。

如果您正在掃描安裝在沒有網路存取的暗網中的資料庫模式，則需要["在沒有網路存取的相同本地位置部署資料分類"](#)。這也要求將控制台代理部署在同一本地位置。

新增資料庫伺服器

新增架構所在的資料庫伺服器。

1. 從資料分類選單中，選擇*配置*。
2. 在設定頁面中，選擇*新增系統* > 新增資料庫伺服器。
3. 輸入所需資訊以識別資料庫伺服器。
 - a. 選擇資料庫類型。
 - b. 輸入連接埠和主機名稱或 IP 位址以連接到資料庫。

- c. 對於 Oracle 資料庫，輸入服務名稱。
- d. 輸入憑證以便資料分類可以存取伺服器。
- e. 選擇*新增資料庫伺服器*。

Add DB Server

To activate Compliance on Databases, first add a Database Server. After this step, you'll be able to select which Database Schemas you would like to activate Compliance for.

Database

Database Type: Host Name or IP Address:

Port: Service Name:

Credentials

Username: Password:

Add DB Server **Cancel**

該資料庫已新增至系統清單。

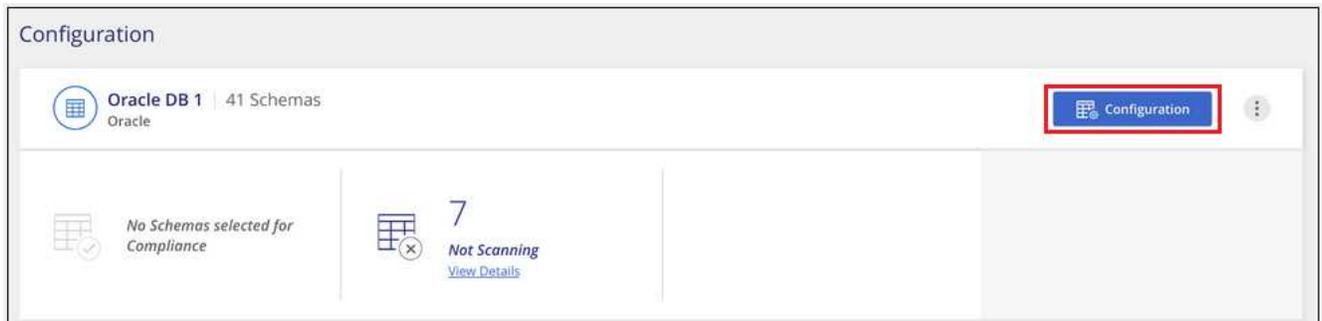
啟用和停用資料庫模式掃描

您可以隨時停止或開始對您的模式進行全面掃描。

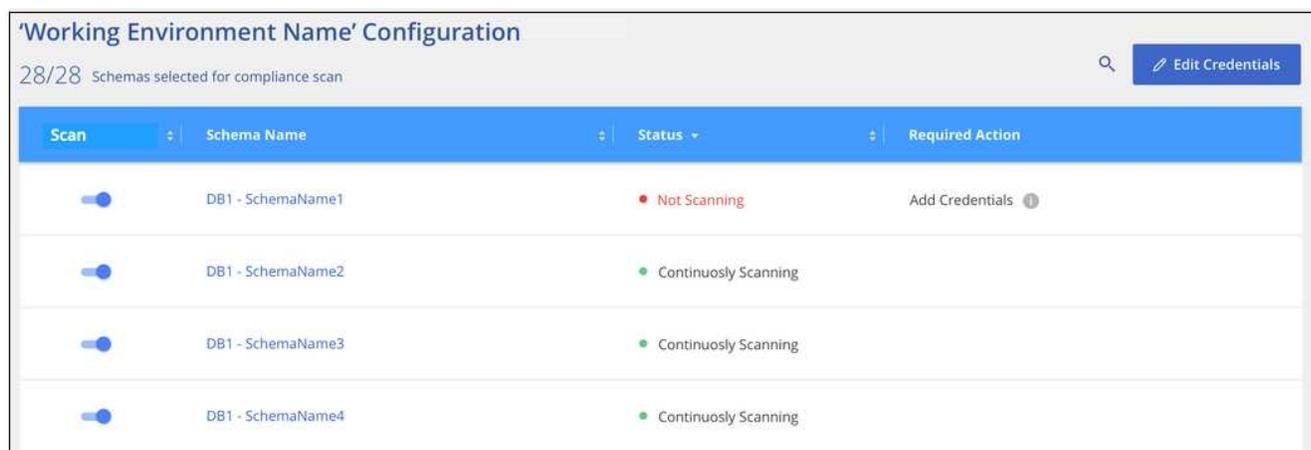


沒有選項可以選擇僅映射資料庫模式的掃描。

1. 在配置頁面中，選擇要設定的資料庫的*配置*按鈕。



2. 透過向右移動滑桿來選擇要掃描的模式。



The screenshot shows a configuration page titled "Working Environment Name' Configuration". At the top, it indicates "28/28 Schemas selected for compliance scan" and has an "Edit Credentials" button. Below is a table with the following columns: Scan, Schema Name, Status, and Required Action.

Scan	Schema Name	Status	Required Action
<input checked="" type="checkbox"/>	DB1 - SchemaName1	Not Scanning	Add Credentials ⓘ
<input checked="" type="checkbox"/>	DB1 - SchemaName2	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName3	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName4	Continuously Scanning	

結果

資料分類開始掃描您啟用的資料庫模式。您可以透過導航到配置選單然後選擇系統配置來追蹤初始掃描的進度。每次掃描的進度都顯示為進度條。您也可以將滑鼠停留在進度列上，查看相對於磁碟區中檔案總數的已掃描檔案數。如果有任何錯誤，它們將出現在「狀態」列中，並顯示修復錯誤所需的操作。

資料分類每天掃描您的資料庫一次；資料庫不像其他資料來源那樣被連續掃描。

使用NetApp Data Classification掃描Google Cloud NetApp Volumes

NetApp Data Classification支援Google Cloud NetApp Volumes作為一個系統。了解如何掃描您的Google Cloud NetApp Volumes系統。

發現您要掃描的Google Cloud NetApp Volumes系統

如果您要掃描的Google Cloud NetApp Volumes系統尚未作為系統出現在NetApp Console中，"[將其新增至系統頁面](#)"。

部署資料分類實例

"[部署資料分類](#)"如果尚未部署實例。

掃描Google Cloud NetApp Volumes時，資料分類必須部署在雲端中，並且必須部署在與您要掃描的磁碟區相同的區域。

*注意：*掃描Google Cloud NetApp Volumes時，目前不支援在本機位置部署資料分類。

在您的系統中啟用資料分類

您可以在Google Cloud NetApp Volumes系統上啟用資料分類。

1. 從資料分類選單中，選擇*配置*。
2. 選擇如何掃描每個系統中的磁碟區。"[了解映射和分類掃描](#)"：

- 若要對應所有捲，請選擇*映射所有磁碟區*
- 若要對應和分類所有捲，請選擇*映射和分類所有捲*
- 若要自訂每個磁碟區的掃描，請選擇*或選擇每個磁碟區的掃描類型*，然後選擇要對應和/或分類的磁碟區。

看[啟用和停用磁碟區上的掃描](#)了解詳情。

3. 在確認對話方塊中，選擇*批准*。

結果

資料分類開始掃描您在系統中選擇的磁碟區。一旦資料分類完成初始掃描，結果就會顯示在合規性儀表板中。所需時間取決於資料量：幾分鐘到幾個小時。您可以在配置選單的系統配置部分追蹤初始掃描的進度。資料分類顯示每次掃描的進度條。您也可以將滑鼠停留在進度列上，查看相對於磁碟區中總檔案數的已掃描檔案數。

- 預設情況下，如果資料分類在 CIFS 中沒有寫入屬性權限，或者在 NFS 中沒有寫入權限，系統將不會掃描磁碟區中的文件，因為資料分類無法將「上次存取時間」還原為原始時間戳記。如果您不介意上次造訪時間是否重設，請選擇*或為每個磁碟區選擇掃描類型*。結果頁面有一個您可以啟用的設置，以便資料分類可以掃描卷，而不管權限如何。
- 資料分類僅掃描卷下的一個檔案共用。如果您的磁碟區中有多個共享，則需要將這些其他共享作為共享群組單獨掃描。["了解此資料分類限制"](#)。

驗證資料分類是否有權存取卷

透過檢查您的網路、安全群組和匯出策略，確保資料分類可以存取磁碟區。對於 CIFS 卷，您需要為資料分類提供 CIFS 憑證。



對於 Google Cloud NetApp Volumes，資料分類只能掃描與控制台位於同一區域的磁碟區。

清單

- 確保資料分類實例與包含 Google Cloud NetApp Volumes 的每個網路之間存在網路連線。
- 確保以下連接埠對資料分類實例開放：
 - 對於 NFS – 連接埠 111 和 2049。
 - 對於 CIFS – 連接埠 139 和 445。
- 確保 NFS 磁碟區匯出策略包含資料分類執行個體的 IP 位址，以便它可以存取每個磁碟區上的資料。

步驟

1. 從資料分類選單中，選擇*配置*。
 - a. 如果您使用 CIFS (SMB)，請確保 Active Directory 憑證正確。對於每個系統，選擇*編輯 CIFS 憑證*，然後輸入資料分類存取系統上的 CIFS 磁碟區所需的使用者名稱和密碼。

憑證可以是唯讀的，但提供管理員憑證可確保資料分類可以讀取任何需要提升權限的資料。憑證儲存在資料分類實例上。

如果您想要確保檔案的「上次存取時間」不會因資料分類掃描而改變，建議使用者在 CIFS 中具有寫入屬性權限或在 NFS 中具有寫入權限。如果可能，請將 Active Directory 使用者設定為組織中具有所有檔案權限的父群組的一部分。

輸入憑證後，您應該會看到一條訊息，表示所有 CIFS 磁碟區均已成功驗證。



2. 在設定頁面上，選擇*查看詳細資訊*以查看每個 CIFS 和 NFS 磁碟區的狀態並修正任何錯誤。

啟用和停用磁碟區上的掃描

您可以隨時從設定頁面啟動或停止任何系統上的掃描。您也可以將掃描從僅映射掃描切換到映射和分類掃描，反之亦然。建議您掃描系統中的所有磁碟區。

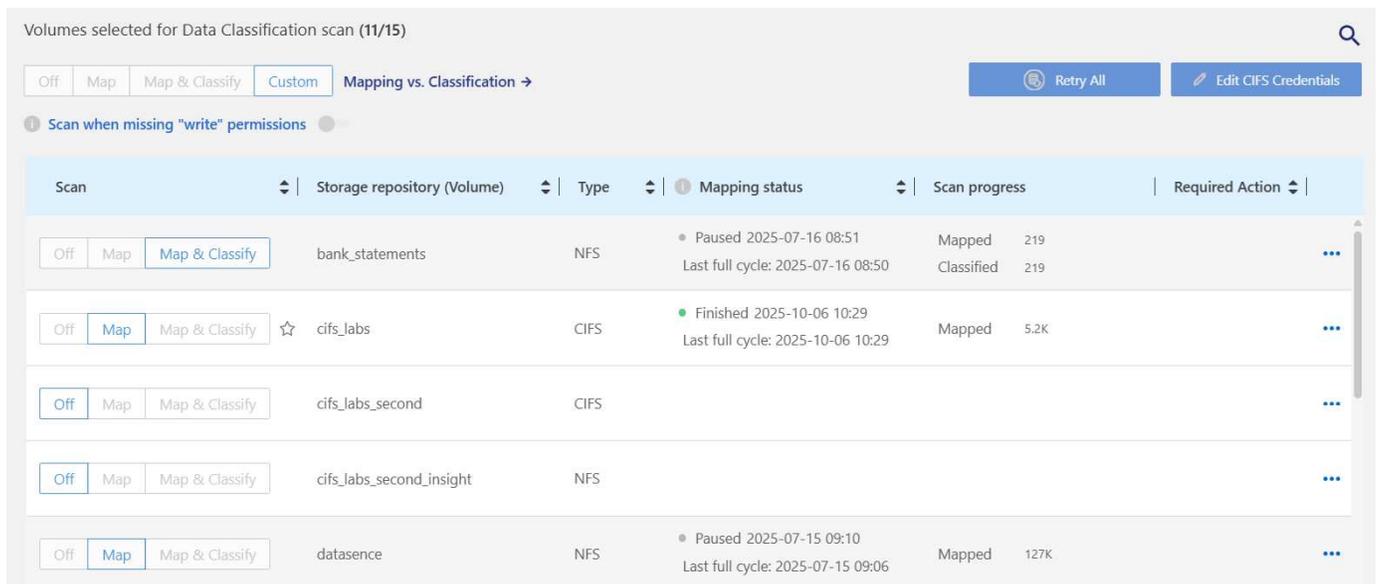


只有當您在標題區域中選擇了 **Map** 或 **Map & Classify** 設定時，才會自動掃描新增至系統的新磁碟區。當在標題區域設定為*自訂*或*關閉*時，您需要在系統中新增的每個新磁碟區上啟動對應和/或完整掃描。

頁面頂部的「缺少「寫入」權限時掃描」開關預設為停用狀態。這意味著，如果資料分類在 CIFS 中沒有寫入屬性權限或在 NFS 中沒有寫入權限，系統將不會掃描文件，因為資料分類無法將「上次存取時間」恢復為原始時間戳記。如果您不介意是否重設上次造訪時間，請開啟開關，無論權限為何，都會掃描所有檔案。["了解更多"](#)。



只有當您在標題區域中設定了 **Map** 或 **Map & Classify** 設定時，才會自動掃描新增到系統的新磁碟區。當所有磁碟區的設定都是「自訂」或「關閉」時，您需要為新增的每個新磁碟區手動啟動掃描。



Scan	Storage repository (Volume)	Type	Mapping status	Scan progress	Required Action
Off Map Map & Classify	bank_statements	NFS	● Paused 2025-07-16 08:51 Last full cycle: 2025-07-16 08:50	Mapped 219 Classified 219	...
Off Map Map & Classify ☆	cifs_labs	CIFS	● Finished 2025-10-06 10:29 Last full cycle: 2025-10-06 10:29	Mapped 5.2K	...
Off Map Map & Classify	cifs_labs_second	CIFS			...
Off Map Map & Classify	cifs_labs_second_insight	NFS			...
Off Map Map & Classify	datasec	NFS	● Paused 2025-07-15 09:10 Last full cycle: 2025-07-15 09:06	Mapped 127K	...

步驟

1. 從資料分類選單中，選擇*配置*。
2. 選擇一個系統，然後選擇*配置*。
3. 若要啟用或停用所有磁碟區的掃描，請在所有磁碟區上方的標題中選擇對應、對應和分類或關閉。

若要啟用或停用對單一卷的掃描，請在清單中找到該卷，然後選擇卷名稱旁的映射、映射和分類或關閉。

結果

當您啟用掃描時，資料分類將開始掃描您在系統中選擇的磁碟區。一旦資料分類開始掃描，結果就會開始出現在合規性儀表中。掃描完成時間取決於資料量，從幾分鐘到幾小時不等。

使用NetApp Data Classification掃描檔案共用

若要掃描檔案共用，您必須先在NetApp Data Classification中建立檔案共用群組。檔案共用群組適用於本機或雲端中託管的 NFS 或 CIFS (SMB) 共用。



資料分類核心版本不支援掃描非NetApp檔案共享的資料。

先決條件

在啟用資料分類之前，請查看以下先決條件，以確保您具有受支援的配置。

- 共享可以託管在任何地方，包括雲端或本地端。可以將舊版NetApp 7-模式儲存系統中的 CIFS 共用掃描為檔案共用。
 - 資料分類無法從 7 模式系統中提取權限或「上次存取時間」。
 - 由於某些 Linux 版本和 7-模式系統上的 CIFS 共用之間存在已知問題，因此您必須將共用配置為僅使用啟用了 NTLM 驗證的 SMBv1。
- 資料分類實例和共用之間需要有網路連線。
- 您可以將 DFS（分散式檔案系統）共用新增為常規 CIFS 共用。由於資料分類不知道共用是基於組合為單一 CIFS 共用的多個伺服器/磁碟區所建構的，因此當訊息實際上僅適用於位於不同伺服器/磁碟區上的一個資料夾/共用時，您可能會收到有關共用的權限或連線錯誤。
- 對於 CIFS (SMB) 共用，請確保您擁有可提供共用讀取存取權限的 Active Directory 憑證。如果資料分類需要掃描任何需要提升權限的數據，則最好使用管理員憑證。

如果您想要確保檔案的「上次存取時間」不會因資料分類掃描而改變，建議使用者在 CIFS 中具有寫入屬性權限或在 NFS 中具有寫入權限。如果可能，請將 Active Directory 使用者設定為組織中具有所有檔案權限的父群組的一部分。

- 群組中的所有 CIFS 檔案共用必須使用相同的 Active Directory 憑證。
- 您可以混合使用 NFS 和 CIFS（使用 Kerberos 或 NTLM）共用。您必須單獨將共用新增至群組。也就是說，您必須完成該過程兩次 - 每個協議一次。
 - 您無法建立混合 CIFS 驗證類型（Kerberos 和 NTLM）的檔案共用群組。
- 如果您使用具有 Kerberos 驗證的 CIFS，請確保資料分類可以存取所提供的 IP 位址。如果 IP 位址無法訪問，則無法新增檔案共用。

建立文件共享組

將檔案共用新增至群組時，必須使用格式 <host_name>:/<share_path>。

您可以單獨新增文件共享，也可以輸入要掃描的文件共享的行分隔清單。您一次最多可以添加 100 股。

步驟

1. 從資料分類選單中，選擇*配置*。
2. 從設定頁面中，選擇*新增系統*>*新增檔案共用群組*。
3. 在新增檔案共享群組對話方塊中，輸入共享群組的名稱，然後選擇*繼續*。
4. 選擇要新增的文件共享的協定。

Add Shares

Directly add any NFS or CIFS (SMB) File Shares, located in the cloud or on-premises.

Select Protocol

You'll be able to add additional shares from the other protocol later.

- NFS
- CIFS (NTLM Authentication)
- CIFS (Kerberos Authentication)

Type or paste below the Shares to add

Provide a list of shares, line-separated. You can add up to 100 shares at a time (you'll be able to add more later).

```
Hostname:/SHAREPATH  
Hostname:/SHAREPATH  
Hostname:/SHAREPATH
```

Continue

Cancel

- a. 如果您要新增具有 NTLM 驗證的 CIFS 共用，請輸入 Active Directory 憑證以存取 CIFS 磁碟區。儘管支援唯讀憑證，但建議您使用管理員憑證提供完全存取權限。選擇儲存。
5. 新增要掃描的檔案共用（每行一個檔案共用）。然後選擇繼續。
 6. 確認對話方塊顯示已新增的共享數量。

如果對話方塊列出了任何無法新增的共享，請擷取此資訊以便解決問題。如果問題與命名約定有關，您可以使用已修正的名稱重新新增共用。

7. 配置磁碟區上的掃描：
 - 若要對檔案共用啟用僅映射掃描，請選擇*映射*。
 - 若要對檔案共用啟用完整掃描，請選擇*Map & Classify*。

- 若要停用檔案共用上的掃描，請選擇「關閉」。



頁面頂部的「缺少「寫入屬性」權限時掃描」開關預設為停用狀態。這意味著，如果資料分類在 CIFS 中沒有寫入屬性權限或在 NFS 中沒有寫入權限，系統將不會掃描文件，因為資料分類無法將「上次存取時間」恢復為原始時間戳記。+ 如果將*缺少「寫入屬性」權限時掃描*切換為*開*，則掃描將重置上次存取時間並掃描所有文件，而不管權限如何。+ 要了解有關上次訪問時間戳的更多信息，請參閱"[從資料分類中的資料來源收集的元資料](#)"。

結果

資料分類開始掃描您新增的檔案共用中的檔案。你可以[追蹤掃描進度](#)並在儀表中查看掃描結果。



如果對於使用 Kerberos 驗證的 CIFS 配置的掃描未成功完成，請檢查配置選項卡中是否有錯誤。

編輯檔案共享群組

建立檔案共用群組後，您可以編輯 CIFS 協定或新增和刪除檔案共用。

編輯 CIFS 協定配置

1. 從資料分類選單中，選擇*配置*。
2. 從設定頁面中，選擇要修改的檔案共用群組。
3. 選擇編輯 **CIFS** 憑證。

Edit CIFS Authentication

Classification requires Active Directory credentials to access CIFS Volumes in Micky.

The credentials can be read-only, but providing admin credentials ensures that Classification can read any data that requires elevated permissions.

Select Authentication Method

NTLM

Kerberos

Username ⓘ

domain\user or user@domain

Password

Password

Save

Cancel

4. 選擇身份驗證方法：**NTLM** 或 **Kerberos**。
5. 輸入 Active Directory 使用者名稱和密碼。
6. 選擇儲存以完成該過程。

將文件共享新增至掃描

1. 從資料分類選單中，選擇*配置*。
2. 從設定頁面中，選擇要修改的檔案共用群組。
3. 選擇 + 新增共享。
4. 選擇要新增的文件共享的協定。

Add Shares

Directly add any NFS or CIFS (SMB) File Shares, located in the cloud or on-premises.

Select Protocol

You'll be able to add additional shares from the other protocol later.

- NFS
- CIFS (NTLM Authentication)
- CIFS (Kerberos Authentication)

Type or paste below the Shares to add

Provide a list of shares, line-separated. You can add up to 100 shares at a time (you'll be able to add more later).

```
Hostname:/SHAREPATH  
Hostname:/SHAREPATH  
Hostname:/SHAREPATH
```

Continue

Cancel

如果您要將文件共用新增至已設定的協議，則無需進行任何變更。

如果您要使用第二種協定新增檔案共用，請確保您已正確配置身份驗證，詳情請見["先決條件"](#)。

5. 使用以下格式新增要掃描的檔案共用（每行一個檔案共用） <host_name>:/<share_path> 。
6. 選擇繼續以完成新增檔案共用。

從掃描中刪除檔案共享

1. 從資料分類選單中，選擇*配置*。
2. 選擇要從中刪除檔案共享的系統。
3. 選擇*配置*。
4. 在配置頁面中，選擇操作 ... 對於要刪除的檔案共用。
5. 從操作選單中，選擇*刪除共用*。

追蹤掃描進度

您可以追蹤初始掃描的進度。

1. 選擇配置選單。
2. 選擇系統配置。
3. 對於儲存庫，檢查掃描進度列以查看其狀態。

使用NetApp Data Classification掃描StorageGRID數據

完成幾個步驟即可直接使用NetApp Data Classification開始掃描StorageGRID內的資料。

查看StorageGRID要求

在啟用資料分類之前，請查看以下先決條件，以確保您具有受支援的配置。

- 您需要有端點 URL 才能連接物件儲存服務。
- 您需要擁有來自StorageGRID的存取金鑰和金鑰，以便資料分類可以存取儲存桶。

部署資料分類實例

如果尚未部署實例，則部署資料分類。

如果您正在掃描可透過網際網路存取的StorageGRID數據，您可以["在雲端部署資料分類"](#)或者["在可以存取網際網路的本地位置部署資料分類"](#)。

如果您要掃描安裝在沒有網路存取的暗站中的StorageGRID數據，則需要["在沒有網路存取的相同本地位置部署資料分類"](#)。這也要求將控制台代理部署在同一本地位置。

將StorageGRID服務新增至資料分類

新增StorageGRID服務。

步驟

1. 從資料分類選單中，選擇*配置*選項。
2. 在設定頁面中，選擇「新增系統」>「新增StorageGRID」。
3. 在新增StorageGRID服務對話方塊中，輸入StorageGRID服務的詳細資訊並選擇*繼續*。
 - a. 輸入您想要使用的系統名稱。此名稱應反映您要連線的StorageGRID服務的名稱。
 - b. 輸入 Endpoint URL 以存取物件儲存服務。
 - c. 輸入存取密鑰和密鑰，以便資料分類可以存取StorageGRID中的儲存桶。

Add StorageGRID

BlueXP Classification can scan data from NetApp StorageGRID, which uses the S3 protocol. [Learn more](#)

To continue, provide the following details. Next, you'll select the buckets you want to scan.

Name the Working Environment

Endpoint URL

Access Key

Secret Key

結果

StorageGRID已新增至系統清單。

啟用並停用StorageGRID桶上的掃描

在StorageGRID上啟用資料分類後，下一步是設定要掃描的儲存桶。資料分類發現這些儲存桶並將它們顯示在您建立的系統中。

步驟

1. 在設定頁面中，找到StorageGRID系統。
2. 在StorageGRID系統圖塊上，選擇 配置。
3. 完成以下步驟之一來啟用或停用掃描：
 - 若要對儲存體桶啟用僅對應掃描，請選擇*Map*。
 - 若要對儲存桶啟用完整掃描，請選擇*Map & Classify*。
 - 若要停用儲存桶的掃描，請選擇「關閉」。

結果

資料分類開始掃描您啟用的儲存桶。您可以透過導航到配置選單然後選擇系統配置來追蹤初始掃描的進度。每次掃描的進度都顯示為進度條。您也可以將滑鼠停留在進度列上，查看相對於磁碟區中總檔案數的已掃描檔案數。如果有任何錯誤，它們將出現在「狀態」列中，並顯示修復錯誤所需的操作。

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。