



啟動資料來源的掃描 Cloud Data Sense

NetApp
May 16, 2022

目錄

啟動資料來源的掃描	1
Cloud Data Sense for Cloud Volumes ONTAP 功能的入門指南、適用於內部部署ONTAP 和內部部署	1
Cloud Data Sense for Azure NetApp Files 功能入門	6
開始瞭解Cloud Data Sense for Amazon FSX ONTAP for Sf	10
Amazon S3的Cloud Data Sense入門	14
正在掃描資料庫架構	20
正在掃描 OneDrive 帳戶	24
掃描SharePoint帳戶	27
正在掃描Google雲端硬碟帳戶	31
正在掃描檔案共用	33
掃描使用S3傳輸協定的物件儲存設備	36

啟動資料來源的掃描

Cloud Data Sense for Cloud Volumes ONTAP 功能的入門指南、適用於內部部署ONTAP 和內部部署

請完成幾個步驟、Cloud Volumes ONTAP 使用Cloud Data Sense開始掃描您的內部和內部部署ONTAP 的各個方面。

快速入門

請依照下列步驟快速入門、或向下捲動至其餘部分以取得完整詳細資料。

在掃描磁碟區之前、您必須先在Cloud Manager中將系統新增為工作環境：

- 對於供應功能的系統、這些工作環境應該已經可在 Cloud Manager 中使用 Cloud Volumes ONTAP
- 對於內部部署 ONTAP 的不全系統、"[Cloud Manager 必須探索 ONTAP 整個叢集](#)"

"部署Cloud Data Sense" 如果尚未部署執行個體、

按一下「資料感應」、選取「組態」索引標籤、然後啟動特定工作環境中磁碟區的法規遵循掃描。

雲端資料感測功能已經啟用、請確定它可以存取所有磁碟區。

- Cloud Data Sense執行個體需要網路連線至Cloud Volumes ONTAP 每個子網路或內部ONTAP 的支援系統。
- 適用於此功能的安全群組Cloud Volumes ONTAP 必須允許來自Data Sense執行個體的傳入連線。
- 請確定這些連接埠已開放給Data Sense執行個體：
 - NFS：連接埠111和2049。
 - 適用於CIFS：連接埠139和445。
- NFS Volume匯出原則必須允許從Data Sense執行個體存取。
- Data Sense需要Active Directory認證來掃描CIFS磁碟區。

按一下* Compliance > Configuration > Edit CIFS Credential*、然後提供認證資料。

選取或取消選取您要掃描的磁碟區、Cloud Data Sense將會開始或停止掃描。

探索您要掃描的資料來源

如果您要掃描的資料來源尚未在 Cloud Manager 環境中、您可以將其新增至繪圖。

您的 NetApp 系統應該已經可在 Cloud Manager 的畫版中使用。Cloud Volumes ONTAP若為內部部署ONTAP 的功能、您必須擁有 "[Cloud Manager 會探索這些叢集](#)"。

部署Cloud Data Sense執行個體

如果尚未部署執行個體、請部署Cloud Data Sense。

如果您要掃描Cloud Volumes ONTAP 可ONTAP 透過網際網路存取的內部功能不全的功能、您可以 ["在雲端部署Cloud Data Sense"](#) 或 ["位於內部部署位置、可存取網際網路"](#)。

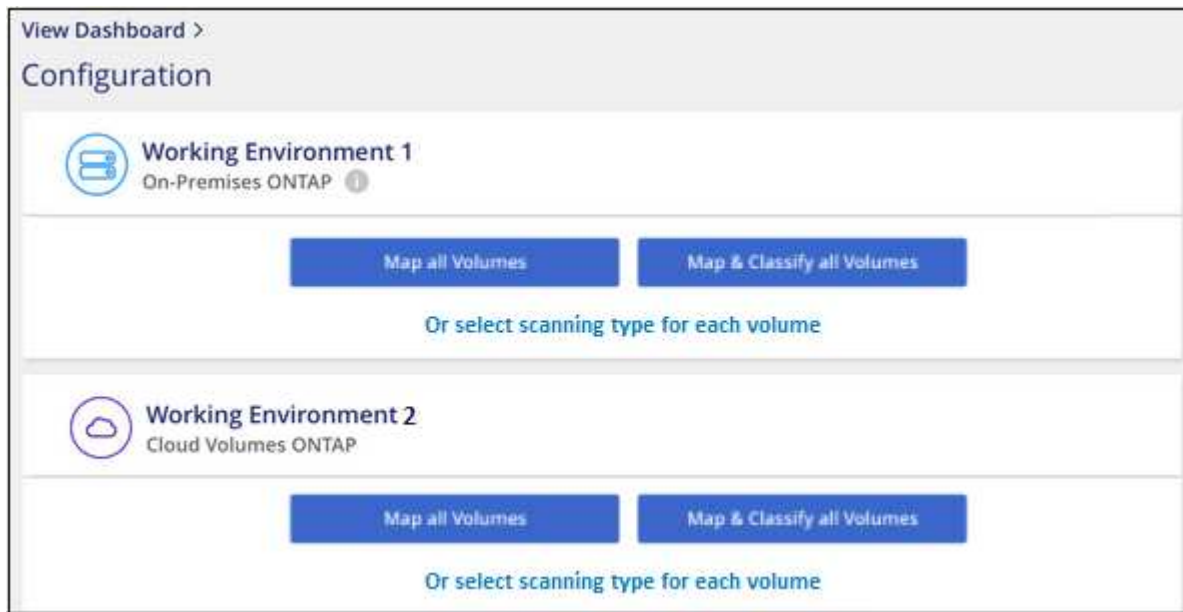
如果您正在掃描ONTAP 安裝在沒有網際網路連線的黑暗站台上的內部部署的資訊系統、您需要 ["在無法存取網際網路的同一個內部部署位置部署Cloud Data Sense"](#)。這也需要將Cloud Manager Connector部署在同一個內部部署位置。

只要執行個體具備網際網路連線、就會自動升級至Data Sense軟體。

在您的工作環境中實現雲端資料的意義

您可以在Cloud Volumes ONTAP AWS、Azure和GCP等系統上、以及內部部署ONTAP 的叢集上啟用Cloud Data Sense。

1. 在Cloud Manager頂端、按一下* Data Sense （資料感測）、然後選取 Configuration（組態）*索引標籤。



2. 選取您要在每個工作環境中掃描磁碟區的方式。 ["深入瞭解對應與分類掃描"](#)：
 - 若要對應所有磁碟區、請按一下*對應所有磁碟區*。
 - 若要對應及分類所有磁碟區、請按一下*對應並分類所有磁碟區*。
 - 若要自訂每個Volume的掃描、請按一下*或選取每個Volume *的掃描類型、然後選擇您要對應和/或分類的Volume。

請參閱 [啟用及停用磁碟區的法規遵循掃描](#) 以取得詳細資料。

3. 在確認對話方塊中、按一下*核准*、讓Data Sense開始掃描您的磁碟區。

Cloud Data Sense會開始掃描您在工作環境中選取的磁碟區。一旦Cloud Data Sense完成初始掃描、就會在「法規遵循」儀表板中顯示結果。所需時間取決於資料量、可能需要幾分鐘或幾小時。

驗證Cloud Data Sense是否可存取磁碟區

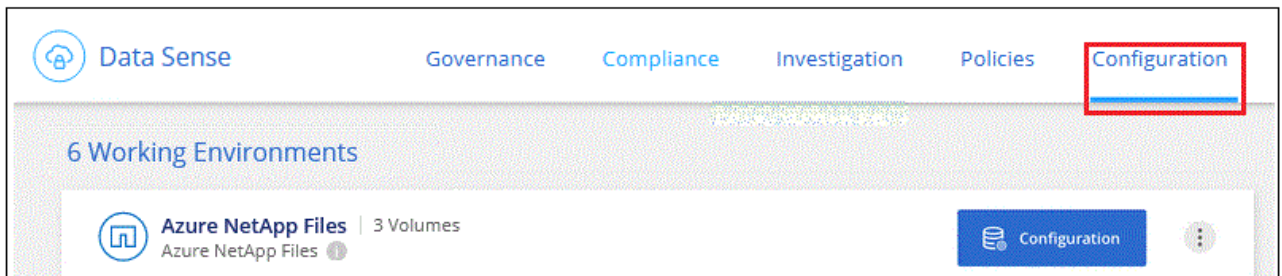
請檢查您的網路、安全性群組和匯出原則、確保Cloud Data Sense能夠存取磁碟區。您必須提供資料認證、以利資料認證、讓IT能夠存取CIFS磁碟區。

步驟

1. 請確定Cloud Data Sense執行個體與每個網路之間都有網路連線、其中包含Cloud Volumes ONTAP 適用於下列ONTAP 叢集的Volume或內部的叢集。
2. 確保Cloud Volumes ONTAP 適用於此功能的安全性群組允許來自Data Sense執行個體的傳入流量。

您可以從Data Sense執行個體的IP位址開啟流量的安全性群組、也可以開啟虛擬網路內部所有流量的安全性群組。

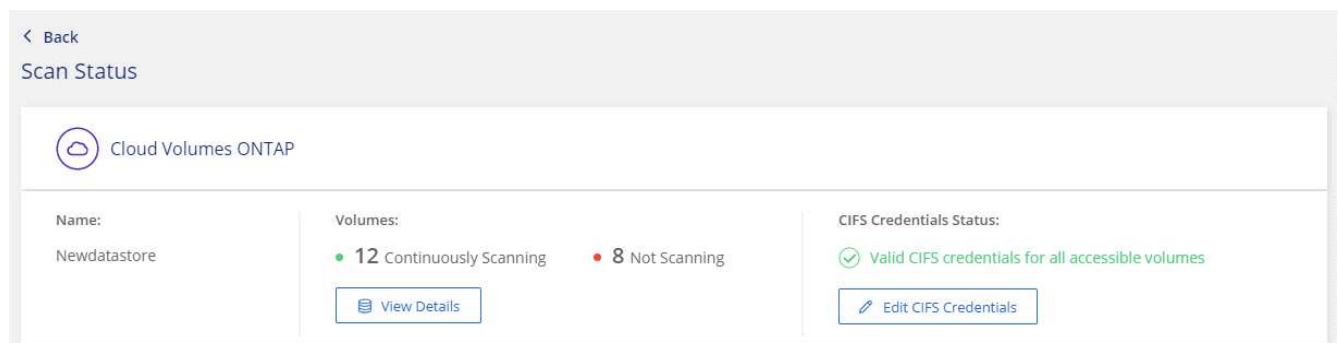
3. 確認下列連接埠已開放給Data Sense執行個體：
 - NFS：連接埠111和2049。
 - 適用於CIFS：連接埠139和445。
4. 確保NFS Volume匯出原則包含Data Sense執行個體的IP位址、以便存取每個Volume上的資料。
5. 如果您使用CIFS、請提供Data Sense搭配Active Directory認證、以便掃描CIFS磁碟區。
 - a. 在Cloud Manager頂端、按一下* Data Sense *。
 - b. 單擊 * Configuration （配置） * 選項卡。



- c. 針對每個工作環境、按一下*編輯CIFS認證*、然後輸入Data Sense存取系統上CIFS磁碟區所需的使用者名稱和密碼。

認證資料可以是唯讀的、但提供管理認證可確保Data Sense能夠讀取任何需要提升權限的資料。認證資料儲存在Cloud Data Sense執行個體上。

輸入認證之後、您應該會看到一則訊息、指出所有 CIFS 磁碟區都已成功驗證。



- 在「_Configuration」頁面上、按一下「檢視詳細資料」以檢閱每個CIFS和NFS磁碟區的狀態、並修正任何錯誤。

例如、下圖顯示四個磁碟區；其中一個因為Data Sense執行個體與磁碟區之間的網路連線問題而無法掃描Cloud Data Sense。

cognitoWE Scan Configuration					
44/79 Volumes selected for Data Sense scan					
<div>Off Map Map & Classify Custom Learn about the differences →</div> <div>Edit CIFS Credentials</div>					
Scan	Storage Repository (Volume)	Type	Status	Required Action	
Off Map Map & Classify	AdiProtest2501	NFS	Continuously Scanning		
Off Map Map & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...	
Off Map Map & Classify	AlexTestSecond	NFS	Not Scanning		
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously Scanning		

啟用及停用磁碟區的法規遵循掃描

您可以隨時從「組態」頁面、在工作環境中啟動或停止僅對應掃描、或是對應和分類掃描。您也可以從純對應掃描變更為對應和分類掃描、反之亦然。建議您掃描所有 Volume。

cognitoWE Scan Configuration					
44/79 Volumes selected for Data Sense scan					
<div>Off Map Map & Classify Custom Learn about the differences →</div> <div>Edit CIFS Credentials</div>					
Scan	Storage Repository (Volume)	Type	Status	Required Action	
Off Map Map & Classify	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...	
Off Map Map & Classify	AdiProtest2501	NFS	Continuously Scanning		
Off Map Map & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...	
Off Map Map & Classify	AlexTestSecond	NFS	Not Scanning		
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously Scanning		

至：	請執行下列動作：
在磁碟區上啟用純對應掃描	在Volume (Volume) 區域中、按一下*地圖*
啟用磁碟區的完整掃描	在Volume (Volume) 區域中、按一下*地圖與分類*
停用在Volume上掃描	在Volume (Volume) 區域中、按一下* Off (關閉) *
在所有磁碟區上啟用純對應掃描	在標題區域中、按一下*地圖*
在所有磁碟區上啟用完整掃描	在標題區域中、按一下*地圖與分類*
停用所有Volume上的掃描	在標題區域中、按一下*關*



只有在標題區域中設定了*地圖*或*地圖與分類*設定之後、才會自動掃描新增至工作環境的磁碟區。在標題區域中設為*自訂*或*關閉*時、您必須在工作環境中新增的每個新磁碟區上啟動對應和/或完整掃描。

正在掃描資料保護磁碟區

根據預設、不會掃描資料保護 (DP) 磁碟區、因為這些磁碟區並未對外公開、而且Cloud Data Sense無法存取它們。這些都是從內部部署 ONTAP 的 SnapMirror 系統或 Cloud Volumes ONTAP 從某個系統進行 SnapMirror 作業的目的地 Volume。

一開始、磁碟區清單會將這些磁碟區識別為「_Type」*「DP*」、「_Status」*「Not 掃描」*、「_required Action」*「Enable Access to DP Volumes」（啟用對 DP 磁碟區的存取）。

'Working Environment Name' Configuration

22/28 Volumes selected for compliance scan

Off Map Map & Classify Custom Learn about the differences →

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

如果您要掃描這些資料保護磁碟區：

1. 按一下頁面頂端的*「Enable Access to DP Volumes」（啟用DP磁碟區存取）*。
2. 檢閱確認訊息、然後再按一下 *「Enable Access to DP Volumes（啟用 DP 磁碟區存取）」*。
 - 原始 ONTAP 資料來源系統中最初建立為 NFS Volume 的磁碟區將會啟用。
 - 最初在來源 ONTAP 系統中建立為 CIFS Volume 的磁碟區、需要輸入 CIFS 認證資料才能掃描這些 DP 磁碟區。如果您已經輸入Active Directory認證資料、以便Cloud Data Sense能夠掃描CIFS磁碟區、您可以使用這些認證資料、也可以指定不同的管理認證資料集。

Provide Active Directory Credentials

☒ Use existing CIFS Scanning Credentials (user1@domain2) ☐ Use Custom Credentials

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

Enable Access to DP Volumes Cancel

Provide Active Directory Credentials

☐ Use existing CIFS Scanning Credentials (user1@domain2) ☒ Use Custom Credentials

Username ⓘ Password

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

Enable Access to DP Volumes Cancel

3. 啟動您要掃描的每個 DP Volume 啟用其他磁碟區的方式相同。

一旦啟用、Cloud Data Sense便會從每個啟用掃描的DP磁碟區建立NFS共用區。共用匯出原則僅允許從Data

Sense執行個體存取。

附註：*如果您在一開始啟用DP磁碟區存取時沒有CIFS資料保護磁碟區、之後再新增部分資料、則「組態」頁面頂端會出現「啟用CIFS DP*存取」按鈕。按一下此按鈕並新增 CIFS 認證、以啟用對這些 CIFS DP 磁碟區的存取。



Active Directory認證資料只會在第一個CIFS DP Volume的儲存VM中註冊、因此會掃描該SVM上的所有DP磁碟區。任何位於其他SVM上的磁碟區都不會登錄Active Directory認證、因此不會掃描這些DP磁碟區。

Cloud Data Sense for Azure NetApp Files 功能入門

完成幾個步驟、開始使用Cloud Data Sense for Azure NetApp Files 整套功能。

快速入門

請依照下列步驟快速入門、或向下捲動至其餘部分以取得完整詳細資料。

在掃描Azure NetApp Files 完所有資料之前、"[必須設定 Cloud Manager 才能探索組態](#)"。

"[在Cloud Manager中部署Cloud Data](#)" 如果尚未部署執行個體、

按一下「* Compliance * (* 符合性 *)」、選取「* Configuration * (* 組態 *)」索引標籤、然後針對特定工作環境中的磁碟區啟動法規遵循掃描。

雲端資料感測功能已經啟用、請確定它可以存取所有磁碟區。

- Cloud Data Sense執行個體需要網路連線至每Azure NetApp Files 個子網路。
- 請確定這些連接埠已開放給Data Sense執行個體：
 - NFS：連接埠111和2049。
 - 適用於CIFS：連接埠139和445。
- NFS Volume匯出原則必須允許從Data Sense執行個體存取。
- Data Sense需要Active Directory認證來掃描CIFS磁碟區。

按一下* Compliance > Configuration > Edit CIFS Credential*、然後提供認證資料。

選取或取消選取您要掃描的磁碟區、Cloud Data Sense將會開始或停止掃描。

探索Azure NetApp Files 您要掃描的整個系統

如果Azure NetApp Files 您要掃描的這個系統尚未在Cloud Manager中做為工作環境、您現在可以將它新增到繪圖中。

"[瞭解如何在Azure NetApp Files Cloud Manager中探索此功能](#)"。

部署Cloud Data Sense執行個體

"部署Cloud Data Sense" 如果尚未部署執行個體、

掃描Azure NetApp Files 完等量磁碟區時、必須將Data Sense部署在雲端、而且必須部署在您要掃描的磁碟區所在的相同區域。

*附註：*掃描Azure NetApp Files 完整個過程中、目前不支援在內部部署位置部署Cloud Data Sense。

只要執行個體具備網際網路連線、就會自動升級至Data Sense軟體。

在您的工作環境中實現雲端資料的意義

您可以在Azure NetApp Files 您的功能區上啟用Cloud Data Sense。

1. 在Cloud Manager頂端、按一下* Data Sense （資料感測）、然後選取 Configuration（組態）*索引標籤。



2. 選取您要在每個工作環境中掃描磁碟區的方式。"深入瞭解對應與分類掃描":
 - 若要對應所有磁碟區、請按一下*對應所有磁碟區*。
 - 若要對應及分類所有磁碟區、請按一下*對應並分類所有磁碟區*。
 - 若要自訂每個Volume的掃描、請按一下*或選取每個Volume *的掃描類型、然後選擇您要對應和/或分類的Volume。

請參閱 [啟用及停用磁碟區的法規遵循掃描](#) 以取得詳細資料。

3. 在確認對話方塊中、按一下*核准*、讓Data Sense開始掃描您的磁碟區。

Cloud Data Sense會開始掃描您在工作環境中選取的磁碟區。一旦Cloud Data Sense完成初始掃描、就會在「法規遵循」儀表板中顯示結果。所需時間取決於資料量、可能需要幾分鐘或幾小時。

驗證Cloud Data Sense是否可存取磁碟區

請檢查您的網路、安全性群組和匯出原則、確保Cloud Data Sense能夠存取磁碟區。您必須提供資料認證、以利資料認證、讓IT能夠存取CIFS磁碟區。

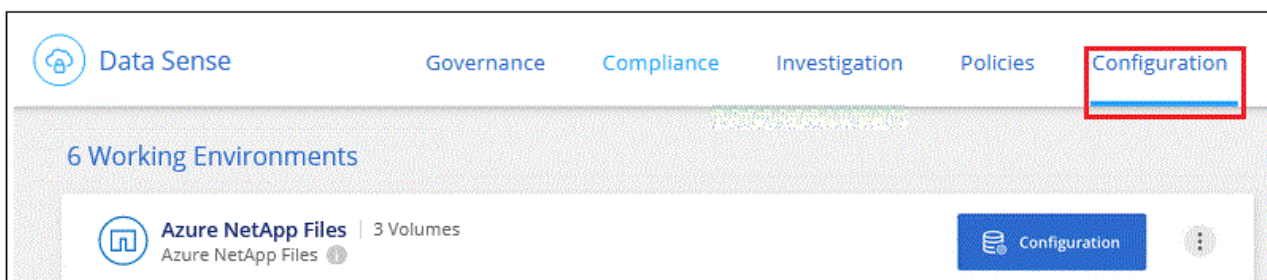
步驟

1. 請確定Cloud Data Sense執行個體與每個網路之間都有網路連線、其中包含Azure NetApp Files 供使用的Volume。



對本產品而言、Cloud Data Sense只能掃描與Cloud Manager位於同一區域的磁碟區。Azure NetApp Files

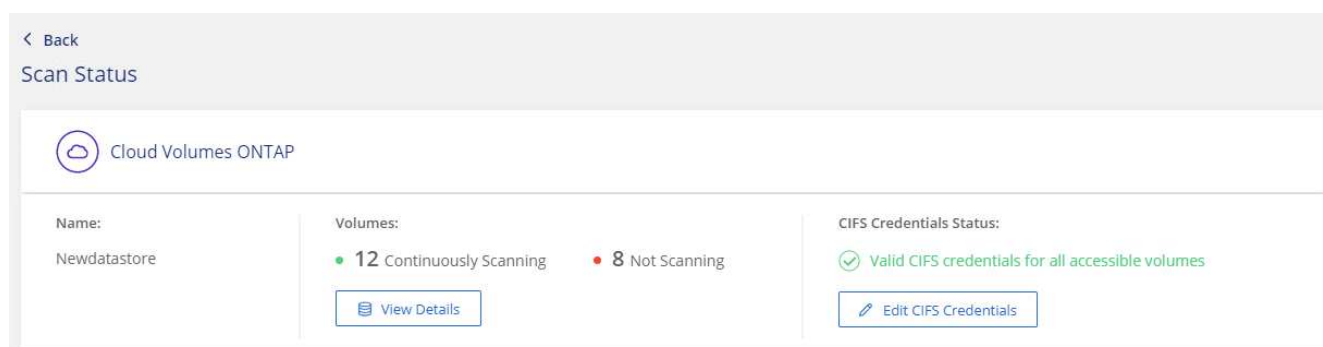
2. 確認下列連接埠已開放給Data Sense執行個體：
 - NFS：連接埠111和2049。
 - 適用於CIFS：連接埠139和445。
3. 確保NFS Volume匯出原則包含Data Sense執行個體的IP位址、以便存取每個Volume上的資料。
4. 如果您使用CIFS、請提供Data Sense搭配Active Directory認證、以便掃描CIFS磁碟區。
 - a. 在Cloud Manager頂端、按一下* Data Sense *。
 - b. 單擊 * Configuration (配置) * 選項卡。



- c. 針對每個工作環境、按一下*編輯CIFS認證*、然後輸入Data Sense存取系統上CIFS磁碟區所需的使用者名稱和密碼。

認證資料可以是唯讀的、但提供管理認證可確保Data Sense能夠讀取任何需要提升權限的資料。認證資料儲存在Cloud Data Sense執行個體上。

輸入認證之後、您應該會看到一則訊息、指出所有 CIFS 磁碟區都已成功驗證。



5. 在「_Configuration」頁面上、按一下「檢視詳細資料」以檢閱每個CIFS和NFS磁碟區的狀態、並修正任何錯誤。

例如、下圖顯示四個磁碟區；其中一個因為Data Sense執行個體與磁碟區之間的網路連線問題而無法掃描Cloud Data Sense。

cognigoWE Scan Configuration				
44/79 Volumes selected for Data Sense scan				
<div> Off Map Map & Classify Custom Learn about the differences → </div> <div>Edit CIFS Credentials</div>				
Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	AdiProtest2501	NFS	Continuously Scanning	
Off Map Map & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
Off Map Map & Classify	AlexTestSecond	NFS	Not Scanning	
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously Scanning	

啟用及停用磁碟區的法規遵循掃描

您可以隨時從「組態」頁面、在工作環境中啟動或停止僅對應掃描、或是對應和分類掃描。您也可以從純對應掃描變更為對應和分類掃描、反之亦然。建議您掃描所有 Volume。

cognigoWE Scan Configuration				
44/79 Volumes selected for Data Sense scan				
<div> Off Map Map & Classify Custom Learn about the differences → </div> <div>Edit CIFS Credentials</div>				
Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
Off Map Map & Classify	AdiProtest2501	NFS	Continuously Scanning	
Off Map Map & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
Off Map Map & Classify	AlexTestSecond	NFS	Not Scanning	
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously Scanning	

至：	請執行下列動作：
在磁碟區上啟用純對應掃描	在Volume (Volume) 區域中、按一下*地圖*
啟用磁碟區的完整掃描	在Volume (Volume) 區域中、按一下*地圖與分類*
停用在Volume上掃描	在Volume (Volume) 區域中、按一下* Off (關閉) *
在所有磁碟區上啟用純對應掃描	在標題區域中、按一下*地圖*
在所有磁碟區上啟用完整掃描	在標題區域中、按一下*地圖與分類*
停用所有Volume上的掃描	在標題區域中、按一下*關*



只有在標題區域中設定了*地圖*或*地圖與分類*設定之後、才會自動掃描新增至工作環境的磁碟區。在標題區域中設為*自訂*或*關閉*時、您必須在工作環境中新增的每個新磁碟區上啟動對應和/或完整掃描。

開始瞭解Cloud Data Sense for Amazon FSX ONTAP for Sf

請完成幾個步驟、開始使用ONTAP Cloud Data Sense掃描Amazon FSX for Sf大量 資料。

開始之前

- 您需要AWS中的Active Connector來部署和管理Data Sense。
- 您在建立工作環境時所選取的安全群組、必須允許來自Cloud Data Sense執行個體的流量。您可以使用ENI連線至FSX for ONTAP Sfor Sfile系統、找到相關的安全群組、然後使用AWS管理主控台進行編輯。

["適用於Linux執行個體的AWS安全性群組"](#)

["適用於Windows執行個體的AWS安全性群組"](#)

["AWS彈性網路介面 \(ENI\) "](#)

快速入門

請依照下列步驟快速入門、或向下捲動以取得完整詳細資料。

在掃描FSXfor ONTAP SfundVolume之前、["您必須設定一個FSX工作環境、並設定磁碟區"](#)。

["在Cloud Manager中部署Cloud Data"](#) 如果尚未部署執行個體、

按一下「資料感應」、選取「組態」索引標籤、然後啟動特定工作環境中磁碟區的法規遵循掃描。

雲端資料感測功能已經啟用、請確定它可以存取所有磁碟區。

- Cloud Data Sense執行個體需要網路連線至ONTAP 各個FSXfor E子 網路。
- 確定下列連接埠已開啟Data Sense執行個體：
 - NFS：連接埠111和2049。
 - 適用於CIFS：連接埠139和445。
- NFS Volume匯出原則必須允許從Data Sense執行個體存取。
- Data Sense需要Active Directory認證來掃描CIFS磁碟區。+按一下* Compliance > Configuration > Edit CIFS Credential*並提供認證資料。

選取或取消選取您要掃描的磁碟區、Cloud Data Sense將會開始或停止掃描。

探索您ONTAP 要掃描的FSXfor Sf2檔案系統

如果ONTAP 您要掃描的FSXfor Sfile系統尚未在Cloud Manager中做為工作環境、您現在可以將其新增至繪圖。

["瞭解如何在ONTAP Cloud Manager中探索或建立FSX for Sfile檔案系統"](#)。

部署Cloud Data Sense執行個體

"部署Cloud Data Sense" 如果尚未部署執行個體、

您應該在與Connector for AWS和您要掃描的FSX Volume相同的AWS網路中部署Data Sense。

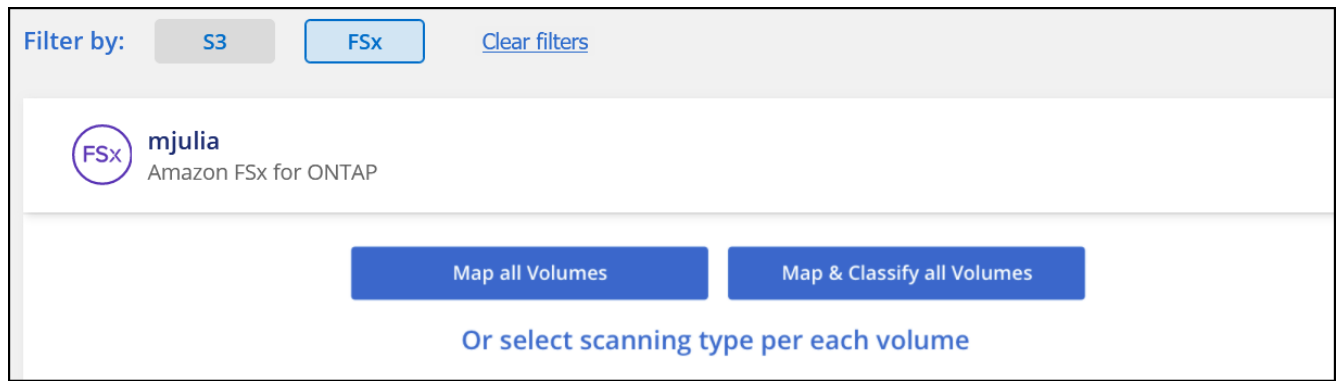
*附註：*掃描FSX Volume時、目前不支援在內部部署位置部署Cloud Data Sense。

只要執行個體具備網際網路連線、就會自動升級至Data Sense軟體。

在您的工作環境中實現雲端資料的意義

您可以啟用ONTAP 適用於FSX的Cloud Data Sense for FSX for S6 Volume。

1. 在Cloud Manager頂端、按一下* Data Sense （資料感測） 、然後選取 Configuration（組態） *索引標籤。



2. 選取您要在每個工作環境中掃描磁碟區的方式。"深入瞭解對應與分類掃描"：
 - 若要對應所有磁碟區、請按一下*對應所有磁碟區*。
 - 若要對應及分類所有磁碟區、請按一下*對應並分類所有磁碟區*。
 - 若要自訂每個Volume的掃描、請按一下*或選取每個Volume *的掃描類型、然後選擇您要對應和/或分類的Volume。

請參閱 [啟用及停用磁碟區的法規遵循掃描](#) 以取得詳細資料。

3. 在確認對話方塊中、按一下*核准*、讓Data Sense開始掃描您的磁碟區。

Cloud Data Sense會開始掃描您在工作環境中選取的磁碟區。一旦Cloud Data Sense完成初始掃描、就會在「法規遵循」儀表板中顯示結果。所需時間取決於資料量、可能需要幾分鐘或幾小時。

驗證Cloud Data Sense是否可存取磁碟區

請檢查您的網路、安全性群組和匯出原則、以確保Cloud Data Sense能夠存取磁碟區。

您必須提供資料認證、以利資料認證、讓IT能夠存取CIFS磁碟區。

步驟

1. 在「_Configuration」頁面上、按一下「檢視詳細資料」以檢閱狀態並修正任何錯誤。

例如、下圖顯示由於Data Sense執行個體與Volume之間的網路連線問題、Volume Cloud Data Sense無法掃描。

Scan	Storage Repository (Volume)	Type	Status	Required Action
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	jrmclone	NFS	● No Access	Check network connectivity between the Data Sense ...

- 請確定Cloud Data Sense執行個體與每個網路之間都有網路連線、其中包含FSXfor ONTAP EfSure的磁碟區。



若為FSXfor ONTAP Sfor Sf, Cloud Data Sense只能掃描與Cloud Manager相同區域的磁碟區。

- 請確定下列連接埠已開放給Data Sense執行個體。
 - NFS：連接埠111和2049。
 - 適用於CIFS：連接埠139和445。
- 確保NFS Volume匯出原則包含Data Sense執行個體的IP位址、以便存取每個Volume上的資料。
- 如果您使用CIFS、請提供Data Sense搭配Active Directory認證、以便掃描CIFS磁碟區。
 - 在Cloud Manager頂端、按一下* Data Sense *。
 - 單擊 * Configuration （配置） * 選項卡。
 - 針對每個工作環境、按一下*編輯CIFS認證*、然後輸入Data Sense存取系統上CIFS磁碟區所需的使用者名稱和密碼。

認證資料可以是唯讀的、但提供管理認證可確保Data Sense能夠讀取任何需要提升權限的資料。認證資料儲存在Cloud Data Sense執行個體上。

輸入認證之後、您應該會看到一則訊息、指出所有 CIFS 磁碟區都已成功驗證。

啟用及停用磁碟區的法規遵循掃描

您可以隨時從「組態」頁面、在工作環境中啟動或停止僅對應掃描、或是對應和分類掃描。您也可以從純對應掃描變更為對應和分類掃描、反之亦然。建議您掃描所有 Volume 。

cognitoWE Scan Configuration				
44/79 Volumes selected for Data Sense scan				
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/> <input type="button" value="Custom"/>	Learn about the differences → <input type="button" value="Edit CIFS Credentials"/>			
Scan	Storage Repository (Volume)	Type	Status	Required Action
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	AdiNFSVol_copy	NFS	● No Access	Access to the NFS volume was denied. Make sure tha...
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	AdiProtest2501	NFS	● Continuously Scanning	
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	AlexTest	NFS	● No Access	Access to the NFS volume was denied. Make sure tha...
<input checked="" type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	AlexTestSecond	NFS	● Not Scanning	
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	MoreDataNeed1000	NFS	● Continuously Scanning	

至：	請執行下列動作：
在磁碟區上啟用純對應掃描	在Volume（Volume）區域中、按一下*地圖*
啟用磁碟區的完整掃描	在Volume（Volume）區域中、按一下*地圖與分類*
停用在Volume上掃描	在Volume（Volume）區域中、按一下* Off（關閉） *
在所有磁碟區上啟用純對應掃描	在標題區域中、按一下*地圖*
在所有磁碟區上啟用完整掃描	在標題區域中、按一下*地圖與分類*
停用所有Volume上的掃描	在標題區域中、按一下*關*



只有在標題區域中設定了*地圖*或*地圖與分類*設定之後、才會自動掃描新增至工作環境的磁碟區。在標題區域中設為*自訂*或*關閉*時、您必須在工作環境中新增的每個新磁碟區上啟動對應和/或完整掃描。

正在掃描資料保護磁碟區

根據預設、不會掃描資料保護（DP）磁碟區、因為這些磁碟區並未對外公開、而且Cloud Data Sense無法存取它們。這些是來自FSXfor ONTAP Sfor the Sfor the Sfile系統的SnapMirror作業目的地Volume。

一開始、磁碟區清單會將這些磁碟區識別為「_Type」 * 「DP*」、「_Status」 * 「Not 掃描」 *、「_required Action」 * 「Enable Access to DP Volumes」（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 tabs for 'Off', 'Map', 'Map & Classify', and 'Custom'. A red box highlights the 'Enable Access to DP Volumes' button. Below the tabs is a table with columns: Scan, Storage Repository (Volume), Type, Status, and Required Action.

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

如果您要掃描這些資料保護磁碟區：

- 按一下頁面頂端的*「Enable Access to DP Volumes」（啟用DP磁碟區存取）*。
- 檢閱確認訊息、然後再按一下 * 「Enable Access to DP Volumes（啟用 DP 磁碟區存取）」 *。
 - 最初在來源FSXfor ONTAP the Sfor the Sfor the file系統中建立為NFS Volume的Volume將會啟用。
 - 最初在來源FSXfor ONTAP the Sfor the Sfile系統中建立為CIFS Volume的磁碟區、需要輸入CIFS認證資料才能掃描這些DP Volume。如果您已經輸入Active Directory認證資料、以便Cloud Data Sense能夠掃描CIFS磁碟區、您可以使用這些認證資料、也可以指定不同的管理認證資料集。

3. 啟動您要掃描的每個 DP Volume 啟用其他磁碟區的方式相同。

一旦啟用、Cloud Data Sense便會從每個啟用掃描的DP磁碟區建立NFS共用區。共用匯出原則僅允許從Data Sense執行個體存取。

附註：*如果您在一開始啟用DP磁碟區存取時沒有CIFS資料保護磁碟區、之後再新增部分資料、則「組態」頁面頂端會出現「啟用CIFS DP*存取」按鈕。按一下此按鈕並新增 CIFS 認證、以啟用對這些 CIFS DP 磁碟區的存取。



Active Directory認證資料只會在第一個CIFS DP Volume的儲存VM中註冊、因此會掃描該SVM上的所有DP磁碟區。任何位於其他SVM上的磁碟區都不會登錄Active Directory認證、因此不會掃描這些DP磁碟區。

Amazon S3的Cloud Data Sense入門

Cloud Data Sense可掃描您的Amazon S3儲存區、以識別位於S3物件儲存區中的個人和敏感資料。Cloud Data Sense可掃描帳戶中的任何儲存庫、無論該儲存庫是為NetApp解決方案所建立。

快速入門

請依照下列步驟快速入門、或向下捲動至其餘部分以取得完整詳細資料。

確保您的雲端環境符合Cloud Data Sense的要求、包括準備IAM角色、以及設定從Data Sense到S3的連線能力。請參閱完整清單。

"部署Cloud Data Sense" 如果尚未部署執行個體、

選取Amazon S3工作環境、按一下*「啟用」*、然後選取內含必要權限的IAM角色。

選取您要掃描的儲存區、Cloud Data Sense將開始掃描。

檢閱 S3 的必要條件

下列需求僅適用於掃描 S3 儲存區。

為Cloud Data Sense執行個體設定IAM角色

Cloud Data Sense需要權限才能連線至帳戶中的S3儲存區、並加以掃描。設定包含下列權限的 IAM 角色。在Amazon S3工作環境中啟用Data Sense時、Cloud Manager會提示您選擇IAM角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

提供從Cloud Data Sense到Amazon S3的連線能力

Cloud Data Sense需要連線至Amazon S3。提供此連線的最佳方法是透過 VPC 端點連線至 S3 服務。如需相關指示、請參閱 ["AWS 文件：建立閘道端點"](#)。

建立VPC端點時、請務必選取對應至Cloud Data Sense執行個體的區域、VPC和路由表。您也必須修改安全性群組、以新增允許流量到 S3 端點的傳出 HTTPS 規則。否則、Data Sense無法連線至S3服務。

如果您遇到任何問題、請參閱 ["AWS 支援知識中心：為什麼我無法使用閘道 VPC 端點連線至 S3 儲存區？"](#)

另一種方法是使用 NAT 閘道來提供連線。



您無法使用 Proxy 透過網際網路連線至 S3 。

部署Cloud Data Sense執行個體

"在Cloud Manager中部署Cloud Data" 如果尚未部署執行個體、

您必須使用部署在AWS中的Connector來部署執行個體、以便Cloud Manager自動探索此AWS帳戶中的S3儲存區、並在Amazon S3工作環境中顯示它們。

*附註：*掃描S3儲存區時、目前不支援在內部部署位置部署Cloud Data Sense。

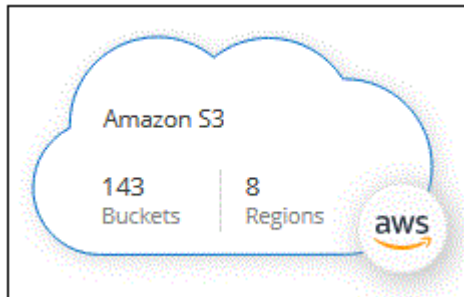
只要執行個體具備網際網路連線、就會自動升級至Data Sense軟體。

在S3工作環境中啟動Data Sense

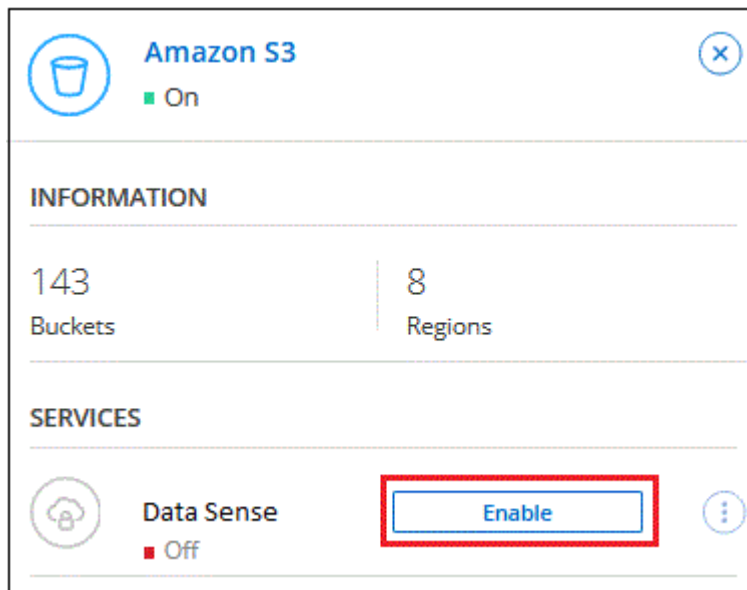
驗證先決條件之後、請在Amazon S3上啟用Cloud Data Sense。

步驟

1. 在 Cloud Manager 頂端、按一下 * Canvas* 。
2. 選取 Amazon S3 工作環境。



3. 在右側的「Data檢測」窗格中、按一下「啟用」。



4. 出現提示時、請將IAM角色指派給具有的Cloud Data Sense執行個體 必要的權限。

Assign an AWS IAM Role for Cloud Data Sense

To enable **Cloud Data Sense** on Amazon S3 buckets, select an existing IAM Role. Make sure that your AWS IAM Role has the permission defined in the [Policy Requirements](#).

Select IAM Role

occm

▼

VPC Endpoint for Amazon S3 Required

A VPC endpoint to the Amazon S3 service is required so **Data Sense** can securely scan the data.

Alternatively, ensure that the **Data Sense** instance has direct access to the internet via a NAT Gateway or Internet Gateway.

Free for the 1st TB


Over 1 TB you pay only for what you use. [Learn more about pricing.](#)

Enable

Cancel

5. 按一下「啟用」。



您也可以按一下「組態」頁面、針對工作環境啟用法規遵循掃描  按鈕並選擇*啟動Data檢測*。

Cloud Manager 會將 IAM 角色指派給執行個體。

啟用和停用 S3 儲存區的法規遵循掃描

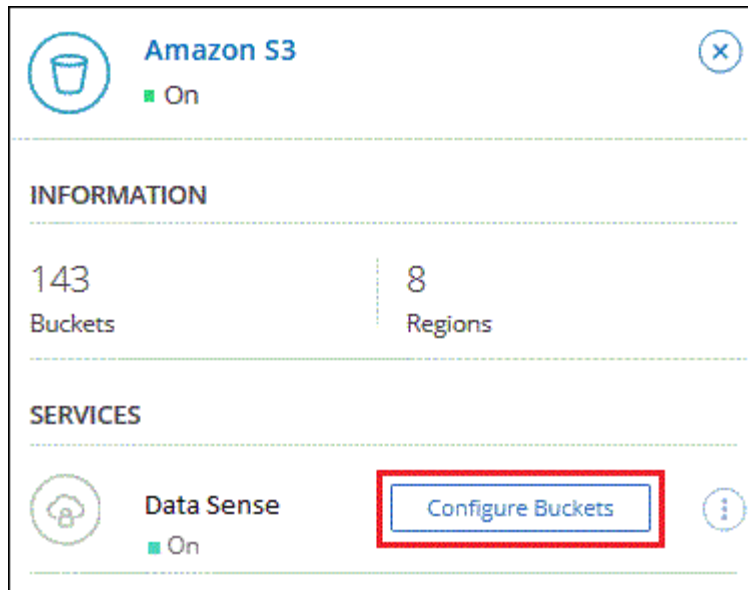
Cloud Manager在Amazon S3上啟用Cloud Data Sense之後、下一步是設定您要掃描的儲存區。

當 Cloud Manager 在 AWS 帳戶中執行時、若該帳戶中有您要掃描的 S3 儲存區、則會探索這些儲存區、並在 Amazon S3 工作環境中顯示這些儲存區。

雲端資料感應也能實現 [掃描位於不同 AWS 帳戶中的 S3 儲存區](#)。

步驟

1. 選取 Amazon S3 工作環境。
2. 在右側窗格中、按一下 * 設定鏟斗 *。



3. 在您的庫位上啟用純對應掃描、或是對應和分類掃描。

Amazon S3 Configuration			
15/28 Buckets in Scan Scope.			
Scan	Bucket Name	Status	Required Action
Off Map Map & Classify	BucketName1	● Not Scanning	Add Credentials
Off Map Map & Classify	BucketName2	● Continuously Scanning	
Off Map Map & Classify	BucketName3	● Not Scanning	

至：	請執行下列動作：
在儲存區上啟用僅對應掃描	按一下*地圖*
啟用庫位的完整掃描	按一下*地圖與分類*
停用儲存區上的掃描	按一下「關」

Cloud Data Sense會開始掃描您啟用的S3儲存區。如果有任何錯誤、它們會顯示在「Status（狀態）」欄中、以及修正錯誤所需的動作。

從其他 AWS 帳戶掃描儲存區

您可以從該帳戶指派角色、以存取現有的Cloud Data Sense執行個體、來掃描位於不同AWS帳戶下的S3儲存區。

步驟

1. 前往您要掃描 S3 儲存區的目標 AWS 帳戶、然後選取 * 其他 AWS 帳戶 * 來建立 IAM 角色。

Create role

1

2

3

4

Select type of trusted entity


 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID*

**Options**

- ☐ Require external ID (Best practice when a third party will assume this role)
- ☐ Require MFA 

請務必執行下列動作：

- 輸入Cloud Data Sense執行個體所在帳戶的ID。
- 將 * 最大 CLI/API 工作階段持續時間 * 從 1 小時變更為 12 小時、並儲存變更。
- 附加Cloud Data Sense IAM原則。請確定它擁有所需的權限。

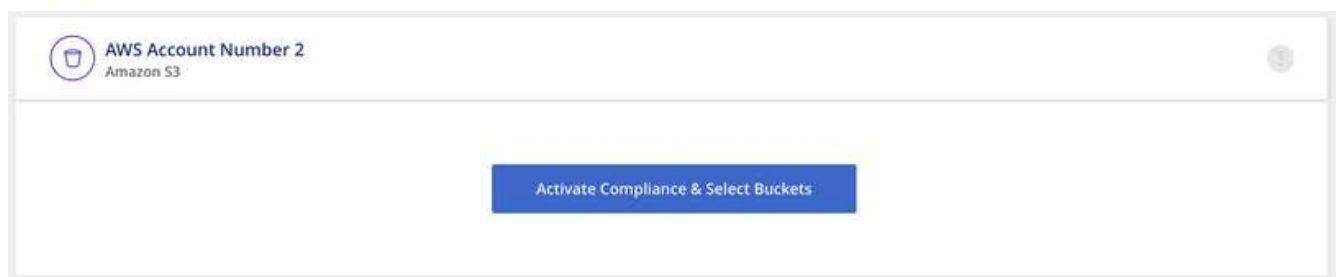
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

2. 前往Data Sense執行個體所在的來源AWS帳戶、然後選取附加至執行個體的IAM角色。
 - a. 將 * 最大 CLI/API 工作階段持續時間 * 從 1 小時變更為 12 小時、並儲存變更。
 - b. 按一下「* 附加原則 *」、然後按一下「* 建立原則 *」。
 - c. 建立包含「STS:AssumeRole」動作的原則、並指定您在目標帳戶中所建立角色的ARN。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-ID>:role/<ADDITIONAL_ROLE_NAME>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

Cloud Data Sense執行個體設定檔帳戶現在可存取額外的AWS帳戶。

- 移至「* Amazon S3 Configuration *」頁面、隨即顯示新的AWS帳戶。請注意、Cloud Data Sense可能需要幾分鐘的時間來同步處理新帳戶的工作環境、並顯示此資訊。



- 按一下「* 啟動Data Sense & Select bucket *」、然後選取您要掃描的儲存區。

Cloud Data Sense會開始掃描您啟用的新S3儲存區。

正在掃描資料庫架構

請完成幾個步驟、開始使用Cloud Data Sense掃描資料庫架構。

快速入門

請依照下列步驟快速入門、或向下捲動至其餘部分以取得完整詳細資料。

請確定您的資料庫受到支援、而且您擁有連線至資料庫所需的資訊。

"部署Cloud Data Sense" 如果尚未部署執行個體、

新增您要存取的資料庫伺服器。

選取您要掃描的架構。

檢閱先決條件

請先檢閱下列先決條件、確定您擁有支援的組態、然後再啟用Cloud Data Sense。

支援的資料庫

Cloud Data Sense可從下列資料庫掃描架構：

- Amazon關係資料庫服務（Amazon RDS）
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP HANA
- SQL Server （ MSSQL ）



必須在資料庫中啟用 * 統計資料收集功能。

資料庫需求

任何可連線至Cloud Data Sense執行個體的資料庫都可以掃描、無論其位於何處。您只需要下列資訊即可連線至資料庫：

- IP 位址或主機名稱
- 連接埠
- 服務名稱（僅用於存取 Oracle 資料庫）
- 允許對架構進行讀取存取的認證

選擇使用者名稱和密碼時、請務必選擇對您要掃描的所有架構和表格具有完整讀取權限的名稱和密碼。我們建議您建立具有所有必要權限的Cloud Data Sense系統專屬使用者。

- 附註： * 對於 MongoDB 、必須具備唯讀管理角色。

部署Cloud Data Sense執行個體

如果尚未部署執行個體、請部署Cloud Data Sense。

如果您要掃描可透過網際網路存取的資料庫架構、您可以 ["在雲端部署Cloud Data Sense"](#) 或 ["在內部部署位置部署Data Sense、並可存取網際網路"](#)。

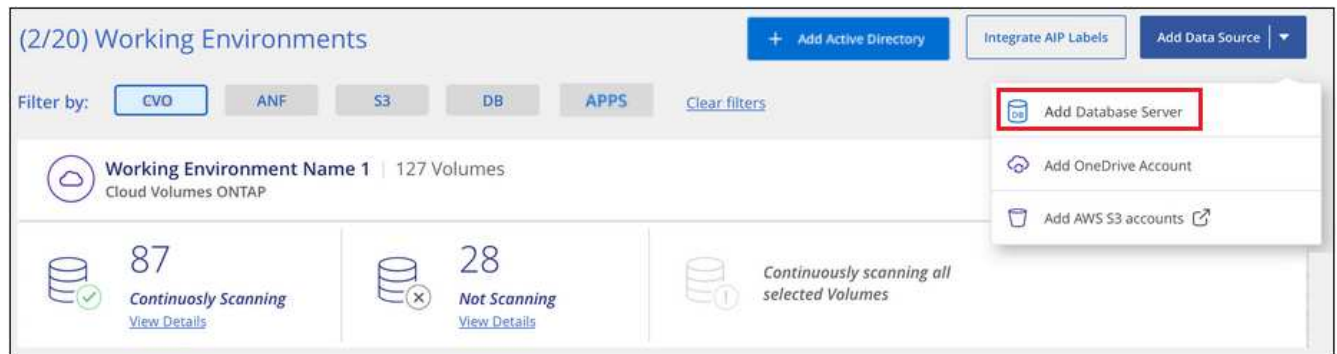
如果您要掃描安裝在無法存取網際網路的暗點中的資料庫架構、則必須執行 ["在無法存取網際網路的同一個內部部署位置部署Cloud Data Sense"](#)。這也需要將Cloud Manager Connector部署在同一個內部部署位置。

只要執行個體具備網際網路連線、就會自動升級至Data Sense軟體。

新增資料庫伺服器

新增架構所在的資料庫伺服器。

1. 在「工作環境組態」頁面中、按一下「* 新增資料來源 *」>「* 新增資料庫伺服器 *」。



2. 輸入識別資料庫伺服器所需的資訊。
 - a. 選取資料庫類型。
 - b. 輸入連接埠和要連線至資料庫的主機名稱或 IP 位址。
 - c. 對於 Oracle 資料庫、請輸入服務名稱。
 - d. 輸入認證資料、讓Cloud Data Sense能夠存取伺服器。
 - e. 按一下「* 新增 DB 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
<input type="text"/>	<input type="text"/>
Port	Service Name
<input type="text"/>	<input type="text"/>

Credentials

Username	Password
<input type="text"/>	<input type="text"/>

Add DB ServerCancel

資料庫會新增至工作環境清單。

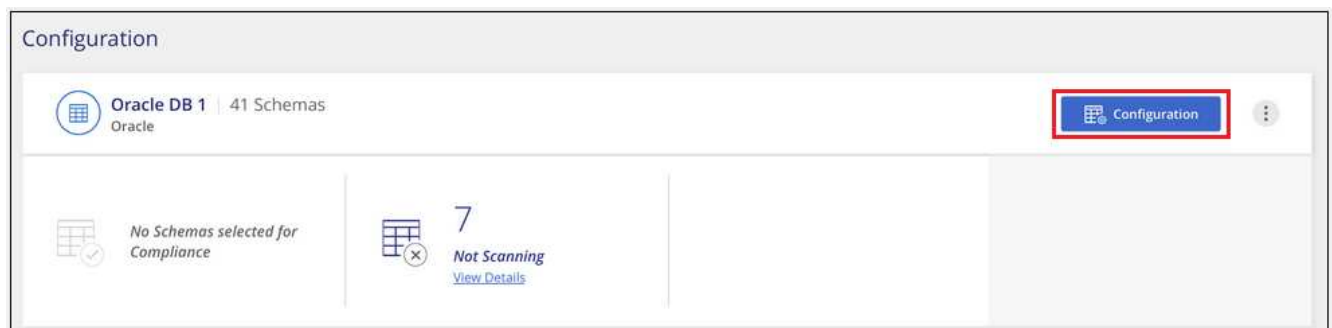
啟用及停用資料庫架構的法規遵循掃描

您可以隨時停止或開始完整掃描架構。



沒有選項可選取資料庫架構的純對應掃描。

1. 在「_Configuration」頁面中、按一下您要設定之資料庫的*組態*按鈕。



2. 將滑桿向右移動、選取您要掃描的架構。

'Working Environment Name' Configuration			
28/28 Schemas selected for compliance scan		<input type="text"/> Edit Credentials	
Scan	Schema Name	Status	Required Action
<input type="checkbox"/>	DB1 - SchemaName1	Not Scanning	Add Credentials ⓘ
<input type="checkbox"/>	DB1 - SchemaName2	Continuously Scanning	
<input type="checkbox"/>	DB1 - SchemaName3	Continuously Scanning	
<input type="checkbox"/>	DB1 - SchemaName4	Continuously Scanning	

Cloud Data Sense會開始掃描您啟用的資料庫架構。如果有任何錯誤、它們會顯示在「狀態」欄中、以及修正錯誤所需的動作。

正在掃描 OneDrive 帳戶

請完成幾個步驟、以Cloud Data Sense開始掃描使用者OneDrive資料夾中的檔案。

快速入門

請依照下列步驟快速入門、或向下捲動至其餘部分以取得完整詳細資料。

請確認您擁有登入 OneDrive 帳戶的管理認證。

["部署Cloud Data Sense"](#) 如果尚未部署執行個體、

使用管理使用者認證、登入您要存取的 OneDrive 帳戶、以便將其新增為新的工作環境。

從您要掃描的OneDrive帳戶新增使用者清單、然後選取掃描類型。您一次最多可新增 100 位使用者。

檢閱OneDrive要求

請先檢閱下列先決條件、確定您擁有支援的組態、然後再啟用Cloud Data Sense。

- 您必須擁有OneDrive for Business帳戶的管理員登入認證、才能提供使用者檔案的讀取存取權。
- 您需要一份以行分隔的電子郵件地址清單、列出您要掃描OneDrive資料夾的所有使用者。

部署Cloud Data Sense執行個體

如果尚未部署執行個體、請部署Cloud Data Sense。

資料感測可以是 ["部署於雲端"](#) 或 ["位於內部部署位置、可存取網際網路"](#)。

只要執行個體具備網際網路連線、就會自動升級至Data Sense軟體。

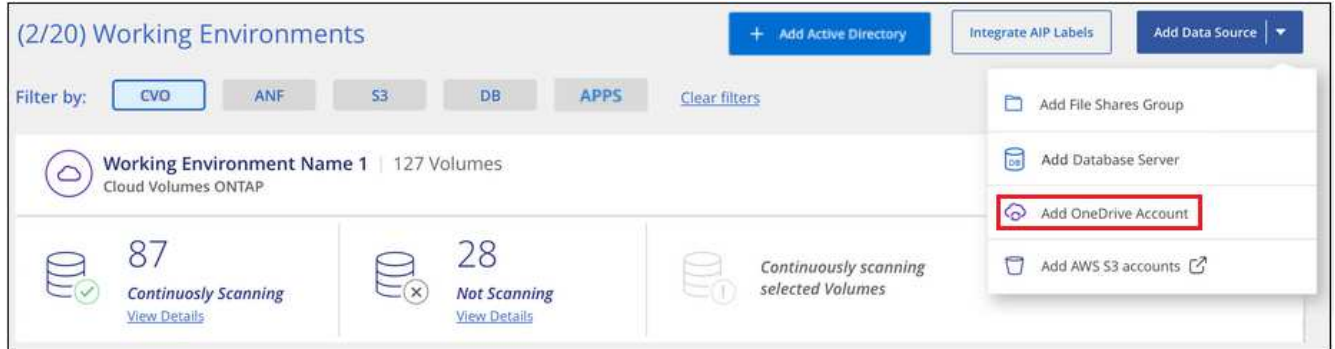
資料感測也可以是 ["部署在沒有網際網路存取的內部部署位置"](#)。不過、您必須提供網際網路存取功能、才能存取數個選定的端點、以掃描本機OneDrive檔案。 ["請參閱此處的必要端點清單"](#)。

新增 OneDrive 帳戶

新增使用者檔案所在的 OneDrive 帳戶。

步驟

1. 在「工作環境組態」頁面中、按一下「* 新增資料來源 *」>「* 新增 OneDrive 帳戶 *」。



2. 在「新增 OneDrive 帳戶」對話方塊中、按一下 *「登入 OneDrive*」。
3. 在顯示的Microsoft頁面中、選取OneDrive帳戶並輸入所需的管理使用者和密碼、然後按一下*接受*、以允許Cloud Data Sense從此帳戶讀取資料。

OneDrive 帳戶會新增至工作環境清單。

將 OneDrive 使用者新增至法規遵循掃描

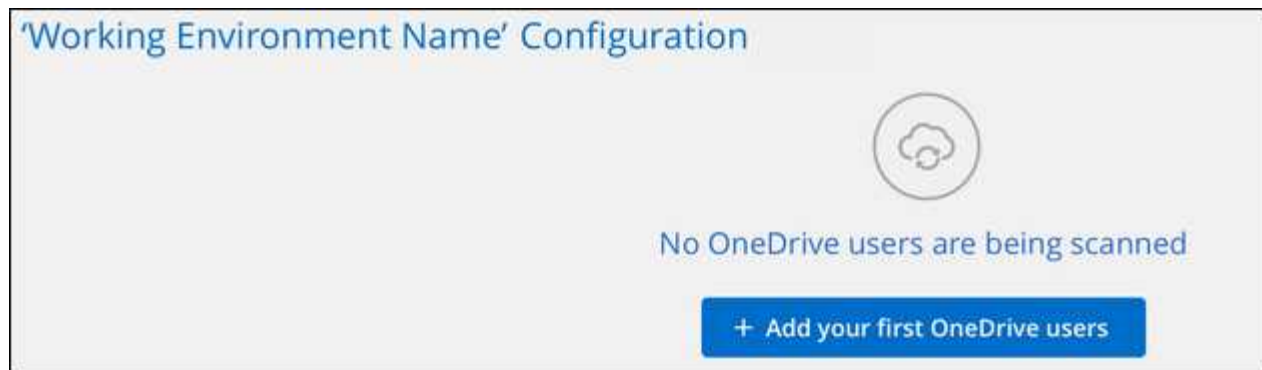
您可以新增個別OneDrive使用者或所有OneDrive使用者、以便Cloud Data Sense掃描他們的檔案。

步驟

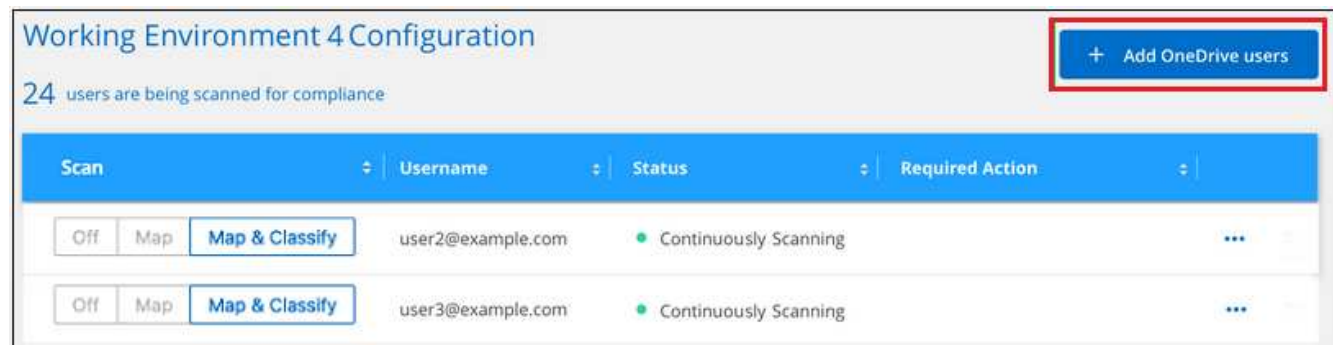
1. 在「_Configuration」頁面中、按一下OneDrive帳戶的*組態*按鈕。



2. 如果這是第一次新增此 OneDrive 帳戶的使用者、請按一下 *「Add your first OneDrive used*（新增您的第一個 OneDrive 使用者 *）」。



如果您要從OneDrive帳戶新增其他使用者、請按一下*「新增OneDrive使用者*」。



3. 為您要掃描檔案的使用者新增電子郵件地址（每行一個電子郵件地址（每個工作階段最多 100 個）、然後按一下 * 新增使用者 * 。

Add OneDrive users

Provide a list of OneDrive users for Cloud Data Sense to scan their data, line-separated. You can add up to 100 users at a time.

Type or paste below the OneDrive user accounts to add

User Accounts

user@example.com

user@example.com

user@example.com

user@example.com

user@example.com

user@example.com

user@example.com

Add Users
Cancel

確認對話方塊會顯示已新增的使用者人數。

如果對話方塊列出任何無法新增的使用者、請擷取此資訊、以便您解決問題。在某些情況下、您可以使用修正後的電子郵件地址重新新增使用者。

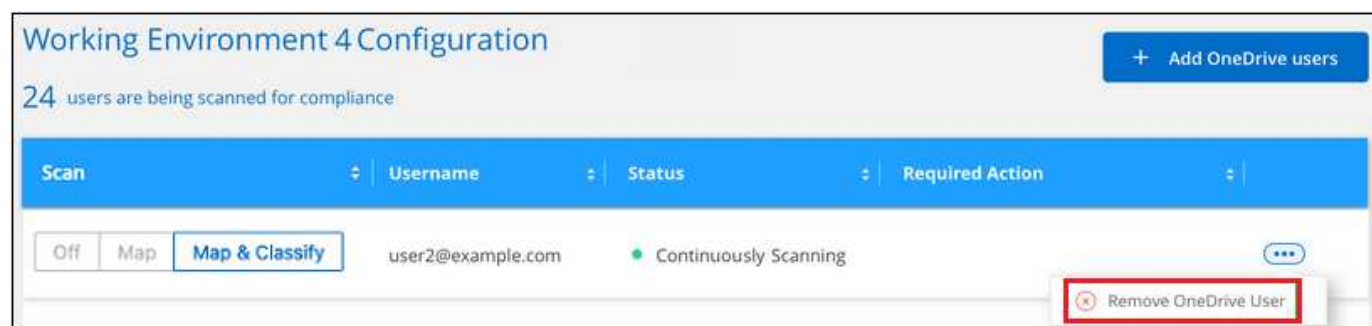
4. 啟用使用者檔案的純對應掃描、或對應與分類掃描。

至：	請執行下列動作：
啟用使用者檔案的純對應掃描	按一下*地圖*
啟用使用者檔案的完整掃描	按一下*地圖與分類*
停用掃描使用者檔案	按一下「關」

Cloud Data Sense會開始掃描您所新增使用者的檔案、結果會顯示在儀表板和其他位置。

將OneDrive使用者從法規遵循掃描中移除

如果使用者離開公司或變更其電子郵件地址、您可以隨時將個別 OneDrive 使用者的檔案掃描完畢。只要按一下「組態」頁面中的「* 移除 OneDrive 使用者 *」即可。



請注意、您可以 "從Data Sense刪除整個OneDrive帳戶" 如果您不想再從OneDrive帳戶掃描任何使用者資料、

掃描SharePoint帳戶

請完成幾個步驟、以Cloud Data Sense開始掃描SharePoint帳戶中的檔案。

快速入門

請依照下列步驟快速入門、或向下捲動至其餘部分以取得完整詳細資料。

請確定您擁有登入SharePoint帳戶的管理認證、而且您有要掃描之SharePoint網站的URL。

"部署Cloud Data Sense" 如果尚未部署執行個體、

使用管理使用者認證、登入您要存取的SharePoint帳戶、將其新增為新的資料來源/工作環境。

在SharePoint帳戶中新增您要掃描的SharePoint網站URL清單、然後選取掃描類型。您一次最多可以新增100個URL。

檢閱SharePoint需求

請檢閱下列先決條件、確定您已準備好在SharePoint帳戶上啟用Cloud Data Sense。

- 您必須擁有SharePoint帳戶的管理員登入認證、才能提供對所有SharePoint網站的讀取存取權。
- 您需要SharePoint網站URL的行分隔清單、以供掃描所有資料。

部署Cloud Data Sense執行個體

如果尚未部署執行個體、請部署Cloud Data Sense。

資料感測可以是 "部署於雲端" 或 "位於內部部署位置、可存取網際網路"。

只要執行個體具備網際網路連線、就會自動升級至Data Sense軟體。

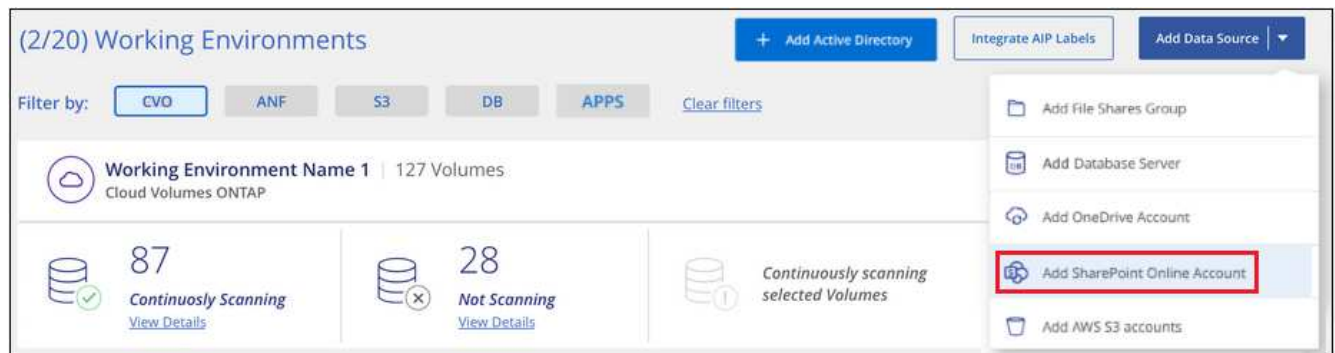
資料感測也可以是 "部署在沒有網際網路存取的內部部署位置"。不過、您必須提供網際網路存取功能、才能存取數個選定的端點、以掃描您的本機SharePoint檔案。"請參閱此處的必要端點清單"。

新增SharePoint帳戶

新增使用者檔案所在的SharePoint帳戶。

步驟

1. 在「工作環境組態」頁面中、按一下「新增資料來源」>「新增SharePoint Online帳戶」。



2. 在「新增SharePoint Online帳戶」對話方塊中、按一下*「登入SharePoint」*。
3. 在顯示的Microsoft頁面中、選取SharePoint帳戶並輸入所需的管理使用者和密碼、然後按一下*接受*、以允許Cloud Data Sense從此帳戶讀取資料。

SharePoint帳戶會新增至工作環境清單。

將SharePoint網站新增至法規遵循掃描

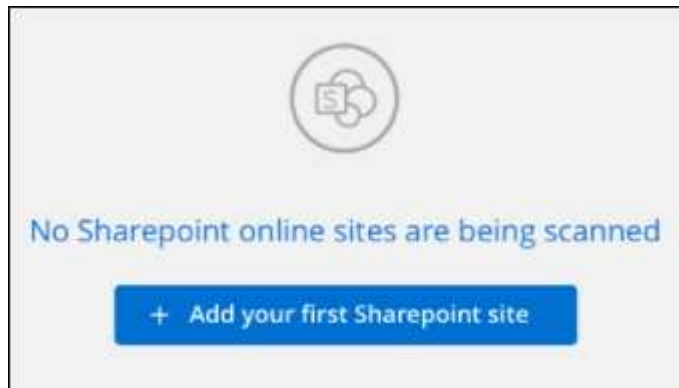
您可以新增個別SharePoint網站或帳戶中的所有SharePoint網站、以便Cloud Data Sense掃描相關檔案。

步驟

1. 在「_Configuration」頁面中、按一下SharePoint帳戶的*組態*按鈕。



2. 如果這是第一次新增此SharePoint帳戶的網站、請按一下*「新增您的第一個SharePoint網站」*。



如果您要從SharePoint帳戶新增其他使用者、請按一下*「新增SharePoint網站」*。



3. 新增您要掃描其檔案的網站URL -每行一個URL（每個工作階段最多100個）、然後按一下*「Add Sites」（新增網站）*。

Add Sharepoint Online Sites

Provide a list of Sharepoint sites for Cloud Data Sense to scan their data, line-separated. You can add up to 100 sites at a time.

Type or paste below the Sharepoint Site URL to add

Site URL

https://netapp.sharepoint.com/sites/ComplianceUserStories
 https://netapp.sharepoint.com/sites/ComplianceUserStories
 https://netapp.sharepoint.com/sites/ComplianceUserStories
 https://netapp.sharepoint.com/sites/ComplianceUserStories
 https://netapp.sharepoint.com/sites/ComplianceUserStories
 https://netapp.sharepoint.com/sites/ComplianceUserStories

Add Sites Cancel

確認對話方塊會顯示已新增的站台數量。

如果對話方塊列出任何無法新增的網站、請擷取此資訊、以便您解決問題。在某些情況下、您可以使用修正的URL重新新增網站。

4. 在SharePoint網站的檔案上啟用純對應掃描、或對應及分類掃描。

至：	請執行下列動作：
啟用檔案的純對應掃描	按一下*地圖*
啟用檔案的完整掃描	按一下*地圖與分類*
停用檔案掃描	按一下「關」

Cloud Data Sense會開始掃描您新增之SharePoint網站中的檔案、結果會顯示在儀表板和其他位置。

將SharePoint網站從法規遵循掃描中移除

如果您日後移除SharePoint網站、或決定不掃描SharePoint網站中的檔案、您可以隨時移除個別SharePoint網站的檔案掃描功能。只要按一下「組態」頁面中的「移除SharePoint Site」即可。

Scan	Site URL	Status	Required Action
Off Map Map & Classify	Site URL	Continuously Scanning	...
Off Map Map & Classify	Site URL	Continuously Scanning	Remove SharePoint Site

請注意、您可以 ["從Data Sense刪除整個SharePoint帳戶"](#) 如果您不想再從SharePoint帳戶掃描任何使用者資料。

正在掃描Google雲端硬碟帳戶

請完成幾個步驟、以Cloud Data Sense開始掃描Google雲端硬碟帳戶中的使用者檔案。

快速入門

請依照下列步驟快速入門、或向下捲動至其餘部分以取得完整詳細資料。

確認您擁有登入Google雲端硬碟帳戶的管理認證資料。

["部署Cloud Data Sense"](#) 如果尚未部署執行個體、

使用管理使用者認證、登入您要存取的Google雲端硬碟帳戶、將其新增為新的資料來源。

選取您要對使用者檔案執行的掃描類型；對應或對應及分類。

檢視Google雲端硬碟的需求

請檢閱下列先決條件、確定您已準備好在Google雲端磁碟機帳戶上啟用Cloud Data Sense。

- 您必須擁有Google雲端硬碟帳戶的管理員登入認證、才能提供使用者檔案的讀取存取權

目前限制

Google雲端硬碟檔案目前不支援下列Data Sense功能：

- 在「資料調查」頁面中檢視檔案時、按鈕列中的動作不會作用。您無法複製、移動、刪除等任何檔案。
- 無法在Google雲端硬碟的檔案中識別權限、因此「調查」頁面不會顯示任何權限資訊。

部署Cloud Data Sense

如果尚未部署執行個體、請部署Cloud Data Sense。

資料感測可以是 ["部署於雲端"](#) 或 ["位於內部部署位置、可存取網際網路"](#)。

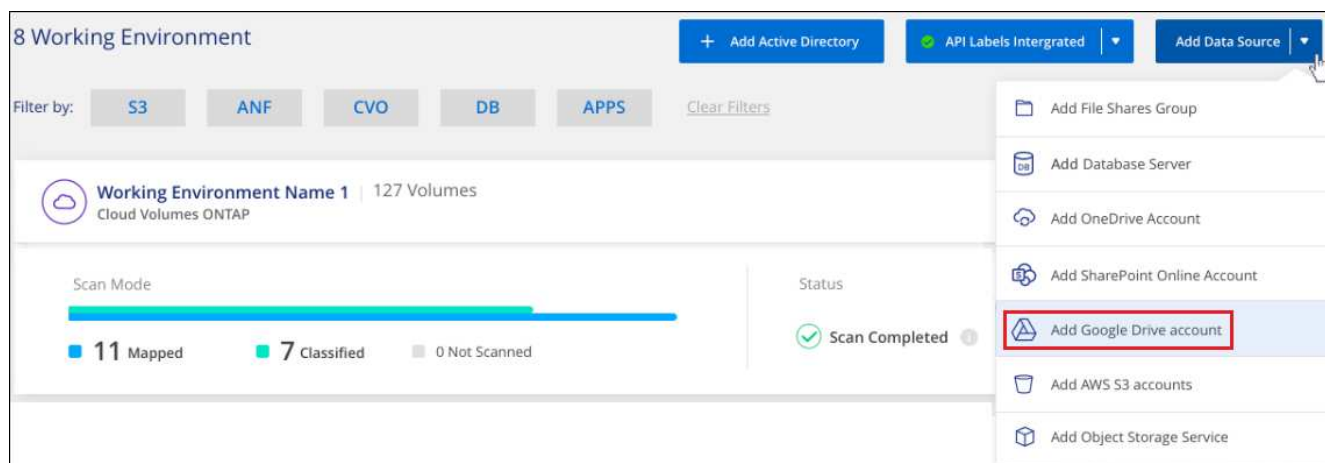
只要執行個體具備網際網路連線、就會自動升級至Data Sense軟體。

新增Google雲端硬碟帳戶

新增使用者檔案所在的Google雲端硬碟帳戶。如果您想要掃描多位使用者的檔案、您必須為每位使用者執行此步驟。

步驟

1. 在「工作環境組態」頁面中、按一下「新增資料來源」>「新增Google雲端硬碟帳戶」。



2. 在「新增Google雲端硬碟帳戶」對話方塊中、按一下*「登入Google雲端硬碟*」。
3. 在顯示的Google頁面中、選取Google雲端硬碟帳戶並輸入所需的管理使用者和密碼、然後按一下*接受*以允許Cloud Data Sense從這個帳戶讀取資料。

Google雲端硬碟帳戶會新增至工作環境清單。

選取使用者資料的掃描類型

選取Cloud Data Sense對使用者資料執行的掃描類型。

步驟

1. 在「_Configuration」頁面中、按一下Google雲端硬碟帳戶的*組態*按鈕。



2. 啟用Google雲端硬碟帳戶中檔案的純對應掃描、或是對應與分類掃描。



至：	請執行下列動作：
啟用檔案的純對應掃描	按一下*地圖*
啟用檔案的完整掃描	按一下*地圖與分類*
停用檔案掃描	按一下「關」

Cloud Data Sense會開始掃描所新增Google雲端硬碟帳戶中的檔案、結果會顯示在儀表板和其他位置。

從法規遵循掃描中移除Google雲端硬碟帳戶

由於單一Google雲端硬碟帳戶只有單一使用者的Google雲端硬碟檔案、因此如果您想要停止掃描使用者Google雲端硬碟帳戶的檔案、您應該這樣做 ["從Data Sense刪除Google雲端硬碟帳戶"](#)。

正在掃描檔案共用

請完成幾個步驟、直接掃描非NetApp NFS或CIFS檔案與Cloud Data Sense共享區。這些檔案共用區可位於內部部署或雲端。

快速入門

請依照下列步驟快速入門、或向下捲動至其餘部分以取得完整詳細資料。

若為CIFS（SMB）共用、請確定您擁有存取共用的認證資料。

["部署Cloud Data Sense"](#) 如果尚未部署執行個體、

此群組是您要掃描之檔案共用的容器、會做為這些檔案共用的工作環境名稱。

新增您要掃描的檔案共用清單、然後選取掃描類型。一次最多可新增100個檔案共用區。

檢閱檔案共用需求

請先檢閱下列先決條件、確定您擁有支援的組態、然後再啟用Cloud Data Sense。

- 共享區可在任何地方代管、包括雲端或內部部署。這些是位於非NetApp儲存系統上的檔案共用。
- Data Sense執行個體與共用區之間必須有網路連線。
- 請確定這些連接埠已開放給Data Sense執行個體：
 - NFS：連接埠111和2049。
 - 適用於CIFS：連接埠139和445。
- 您需要以「<host_name>//<share_path>'格式新增的共用清單。您可以個別輸入共用、也可以提供要掃描之檔案共用的行分隔清單。
- 若為CIFS（SMB）共用、請確定您擁有Active Directory認證、以提供共用的讀取存取權。如果Cloud Data Sense需要掃描任何需要提高權限的資料、則首選管理認證。

部署Cloud Data Sense執行個體

如果尚未部署執行個體、請部署Cloud Data Sense。

如果您要掃描可透過網際網路存取的非NetApp NFS或CIFS檔案共用、您可以 ["在雲端部署Cloud Data Sense"](#) 或 ["在內部部署位置部署Data Sense、並可存取網際網路"](#)。

如果您要掃描安裝在無法存取網際網路的暗點中的非NetApp NFS或CIFS檔案共用、您必須執行 ["在無法存取網際網路的同一個內部部署位置部署Cloud Data Sense"](#)。這也需要將Cloud Manager Connector部署在同一個內部部署位置。

只要執行個體具備網際網路連線、就會自動升級至Data Sense軟體。

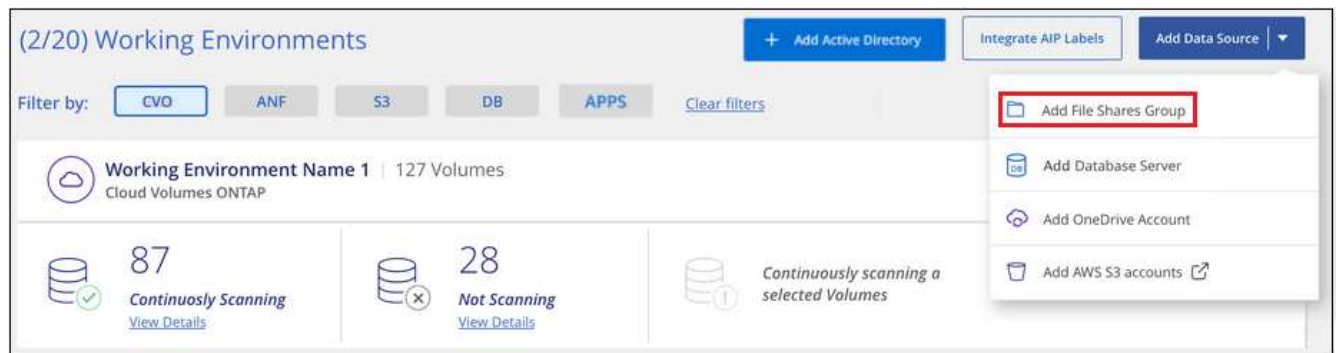
建立檔案共用的群組

您必須先新增共用「群組」的檔案、才能新增檔案共用。此群組是您要掃描之檔案共用的容器、群組名稱會做為這些檔案共用的工作環境名稱。

您可以混合使用同一個群組中的NFS和CIFS共用、不過群組中的所有CIFS檔案共用都必須使用相同的Active Directory認證。如果您打算新增使用不同認證的CIFS共用、則必須針對每組獨特的認證建立個別的群組。

步驟

1. 在「工作環境組態」頁面中、按一下「新增資料來源」>「新增檔案共用群組」。



2. 在「新增檔案共用群組」對話方塊中、輸入共用群組的名稱、然後按一下*繼續*。

新的「檔案共用群組」會新增至工作環境清單。

新增檔案共用至群組

您可以將檔案共用新增至檔案共用群組、以便Cloud Data Sense掃描這些共用中的檔案。您可以使用「<host_name>\\<share_path>」格式新增共用。

您可以新增個別檔案共用、也可以提供要掃描之檔案共用的行分隔清單。一次最多可新增100個共用。

在單一群組中同時新增NFS和CIFS共用時、您需要執行兩次程序、一次新增NFS共用、然後再次新增CIFS共用。

步驟

1. 在「工作環境」頁面中、按一下「檔案共用」群組的「組態」按鈕。



2. 如果這是第一次新增此檔案共用群組的檔案共用、請按一下*「Add Your First Shares」*（新增您的第一個共用）*。

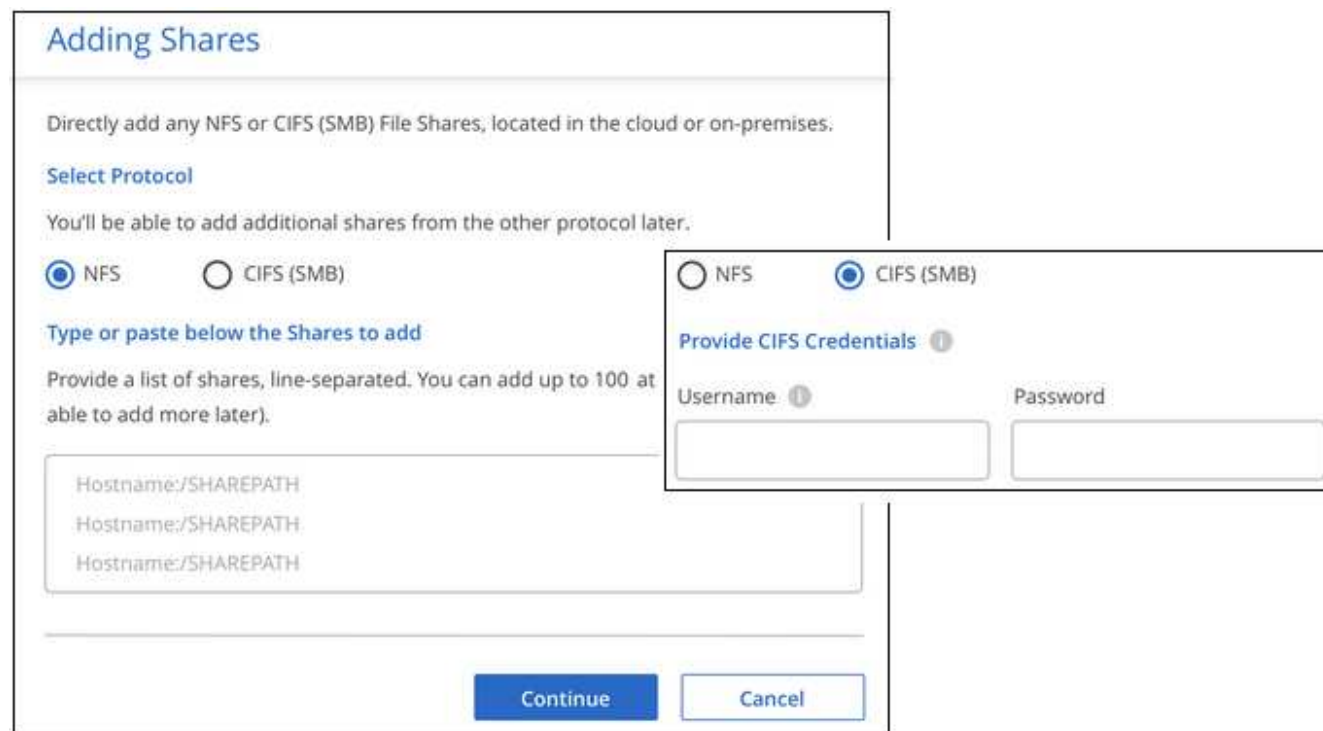


如果您要將檔案共用新增至現有群組、請按一下*「Add Shares」（新增共用）*。



3. 選取您要新增之檔案共用的傳輸協定、新增您要掃描的檔案共用區（每行一個檔案共用區）、然後按一下*繼續*。

新增CIFS（SMB）共用時、您必須輸入Active Directory認證、以提供共用的讀取存取權。首選管理認證。



確認對話方塊會顯示已新增的共用數。

如果對話方塊列出任何無法新增的共用、請擷取此資訊、以便您解決問題。在某些情況下、您可以使用修正後的主機名稱或共用名稱重新新增共用區。

4. 在每個檔案共用區上啟用純對應掃描、或是對應與分類掃描。

至：	請執行下列動作：
啟用檔案共用上的純對應掃描	按一下*地圖*
啟用檔案共用區的完整掃描	按一下*地圖與分類*
停用掃描檔案共用區	按一下「關」

Cloud Data Sense會開始掃描您新增檔案共用中的檔案、結果會顯示在儀表板和其他位置。

從法規遵循掃描移除檔案共用區

如果不再需要掃描特定檔案共用、您可以隨時將個別檔案共用區移除、使其檔案不再掃描。只要按一下「組態」頁面中的「移除共用」即可。



掃描使用S3傳輸協定的物件儲存設備

請完成幾個步驟、以Cloud Data Sense直接掃描物件儲存區內的資料。Data Sense可從任何使用簡易儲存服務（S3）傳輸協定的物件儲存服務掃描資料。其中包括NetApp StorageGRID 功能、IBM Cloud Object Store、Azure Blob（使用MinIO）、Linode、B2 Cloud Storage、Amazon S3等。

快速入門

請依照下列步驟快速入門、或向下捲動至其餘部分以取得完整詳細資料。

您需要有端點URL才能連線至物件儲存服務。

您需要從物件儲存供應商取得存取金鑰和秘密金鑰、以便Cloud Data Sense能夠存取儲存區。

"部署Cloud Data Sense" 如果尚未部署執行個體、

將物件儲存服務新增至Cloud Data Sense。

選取您要掃描的儲存區、Cloud Data Sense將開始掃描。

檢閱物件儲存需求

請先檢閱下列先決條件、確定您擁有支援的組態、然後再啟用Cloud Data Sense。

- 您需要有端點URL才能連線至物件儲存服務。
- 您需要從物件儲存供應商取得存取金鑰和秘密金鑰、以便讓Data Sense能夠存取儲存區。
- 若要支援Azure Blob、您必須使用 "[MinIO服務](#)"。

部署Cloud Data Sense執行個體

如果尚未部署執行個體、請部署Cloud Data Sense。

如果您要掃描S3物件儲存設備的資料、而且可以透過網際網路存取 "[在雲端部署Cloud Data Sense](#)" 或 "[在內部部署位置部署Data Sense](#)、並可存取網際網路"。

如果您要掃描安裝在無法存取網際網路之黑暗站台上的S3物件儲存設備資料、則必須執行 "[在無法存取網際網路的同一個內部部署位置部署Cloud Data Sense](#)"。這也需要將Cloud Manager Connector部署在同一個內部部署位置。

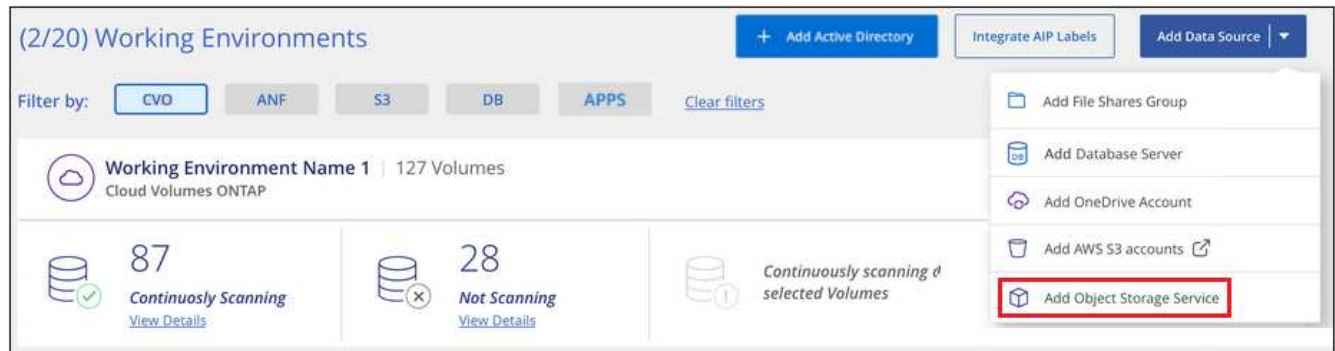
只要執行個體具備網際網路連線、就會自動升級至Data Sense軟體。

將物件儲存服務新增至Cloud Data Sense

新增物件儲存服務。

步驟

1. 在「工作環境組態」頁面中、按一下「新增資料來源」>「新增物件儲存服務」。



2. 在「新增物件儲存服務」對話方塊中、輸入物件儲存服務的詳細資料、然後按一下*繼續*。
 - a. 輸入您要用於工作環境的名稱。此名稱應反映您要連線的物件儲存服務名稱。
 - b. 輸入端點URL以存取物件儲存服務。
 - c. 輸入存取金鑰和秘密金鑰、讓Cloud Data Sense能夠存取物件儲存區中的儲存區。

Add Object Storage Service

Cloud Data Sense can scan data from any Object Storage service which uses the S3 protocol. This includes NetApp StorageGRID, IBM Object Store, and more.

To continue, enter the following information. In the next steps you'll need to select the buckets you want to scan.

Name the Working Environment	Endpoint URL
<input type="text" value="object_myIBM"/>	<input type="text" value="http://my.endpoint.com"/>
Access Key	Secret Key
<input type="text" value="AJUKDO574NDJG86795"/>	<input type="text" value="....."/>

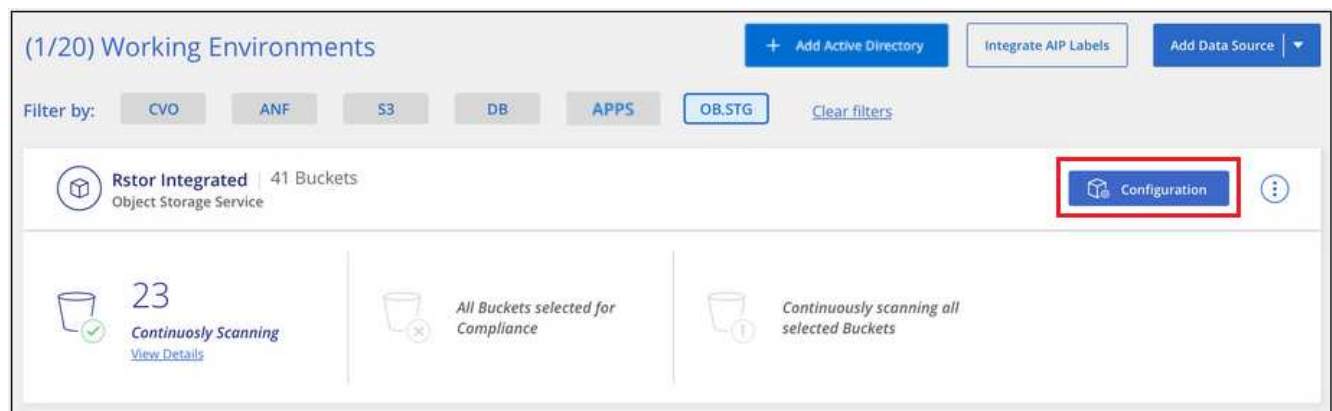
新的物件儲存服務會新增至工作環境清單。

啟用及停用物件儲存桶上的法規遵循掃描

在物件儲存服務上啟用Cloud Data Sense之後、下一步是設定您要掃描的儲存區。Data Sense會探索這些儲存區、並在您所建立的工作環境中顯示這些儲存區。

步驟

1. 在「組態」頁面中、按一下「物件儲存服務」工作環境中的*組態*。



2. 在您的庫位上啟用純對應掃描、或是對應和分類掃描。

Rstor Integrated Configuration			
3/55 Buckets selected for Compliance scan			
Scan	Storage Repository (Bucket) ↓↑	Status ↓↑	Required Action ↓↑
Off Map Map & Classify	logs-759995470648-us-east-1	● Not Scanning	
Off Map Map & Classify	logs-759995470648-us-west-2	● Not Scanning	
Off Map Map & Classify	carstock	● Continuously Scanning	

至：	請執行下列動作：
在儲存區上啟用僅對應掃描	按一下*地圖*
啟用庫位的完整掃描	按一下*地圖與分類*
停用儲存區上的掃描	按一下「關」

Cloud Data Sense會開始掃描您啟用的儲存區。如果有任何錯誤、它們會顯示在「Status（狀態）」欄中、以及修正錯誤所需的動作。

Copyright Information

Copyright © 2022 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.