



開始使用 Cloud Data Sense

NetApp
May 16, 2022

This PDF was generated from <https://docs.netapp.com/zh-tw/cloud-manager-data-sense/concept-cloud-compliance.html> on May 16, 2022. Always check docs.netapp.com for the latest.

目錄

開始使用	1
深入瞭解Cloud Data Sense	1
部署Cloud Data Sense	6
啟動資料來源的掃描	23
將Active Directory與Cloud Data Sense整合	61
設定Cloud Data Sense授權	64
有關Cloud Data Sense的常見問題集	69

開始使用

深入瞭解Cloud Data Sense

Cloud Data Sense是適用於Cloud Manager的資料治理服務、可掃描企業內部部署與雲端資料來源及工作環境、以對應及分類資料、並識別私有資訊。這有助於降低安全性與法規遵循風險、降低儲存成本、並協助您執行資料移轉專案。

["瞭解Cloud Data Sense的使用案例"](#)。

功能

Cloud Data Sense提供多種工具、可協助您達成法規遵循目標。您可以使用Data Sense：

- 識別個人識別資訊（PII）
- 根據 GDPR、CCPA、PCI 及 HIPAA 隱私權法規的要求、識別廣泛的敏感資訊
- 回應資料主體存取要求（DSAR）
- 當檔案包含特定PII時、透過電子郵件通知Cloud Manager使用者（您使用定義此條件 ["原則"](#)）
- 檢視及修改 ["Azure資訊保護（AIP）標籤"](#) 在您的檔案中
- 將自訂標記新增至檔案（例如「需要搬移」）、並指派Cloud Manager使用者、讓該人員擁有檔案的更新
- 複製、移動及刪除檔案

Cloud Data Sense也提供各種工具、協助您善用治理方式。您可以使用Cloud Data Sense：

- 識別系統中過時的資料、非商業資料、重複的檔案、具有開放權限的檔案、以及非常大的檔案。

您可以使用此資訊來決定是否要將某些檔案移至較便宜的物件儲存設備、刪除或分層處理。

- 在移動資料之前、請先檢視資料大小、以及是否有任何資料包含敏感資訊。

如果您打算將資料從內部部署位置移轉至雲端、這項功能就很實用。

支援的工作環境和資料來源

Cloud Data Sense可掃描下列工作環境和資料來源類型的資料：

工作環境：

- （部署於AWS、Azure或GCP）Cloud Volumes ONTAP
- 內部部署 ONTAP 的叢集
- Azure NetApp Files
- Amazon FSX for ONTAP
- Amazon S3

資料來源：

- 非NetApp檔案共用
- 物件儲存（使用S3傳輸協定）
- 資料庫
- OneDrive 帳戶
- SharePoint帳戶
- Google雲端硬碟帳戶

Data Sense支援NFS 3.x、4.0及4.1版、以及CIFS 1.x、2.0、2.1及3.0版。

成本

- 使用Cloud Data Sense的成本取決於您要掃描的資料量。Data Sense在Cloud Manager工作區中掃描的前1 TB資料是免費的。這包括所有工作環境和資料來源的所有資料。必須訂閱AWS、Azure或GCP Marketplace、或NetApp的BYOL授權、才能在該點之後繼續掃描資料。請參閱 ["定價"](#) 以取得詳細資料。

["瞭解如何取得Cloud Data Sense授權"](#)。

- 若要在雲端上安裝Cloud Data Sense、必須部署雲端執行個體、這會導致雲端供應商在部署雲端執行個體時收取費用。請參閱 [為每個雲端供應商部署的執行個體類型](#)。如果您在內部部署系統上安裝Data Sense、則不需支付任何費用。
- Cloud Data Sense需要部署Cloud Manager Connector。在許多情況下、由於 Cloud Manager 中使用的其他儲存設備和服務、您已經擁有 Connector。連接器執行個體會從部署該執行個體的雲端供應商收取費用。請參閱 ["為每個雲端供應商部署的執行個體類型"](#)。如果您將連接器安裝在內部部署系統上、則無需支付任何費用。

資料傳輸成本

資料傳輸成本取決於您的設定。如果Cloud Data Sense執行個體和資料來源位於相同的可用度區域和區域、則不會產生資料傳輸成本。但是如果Cloud Volumes ONTAP 資料來源（例如、不支援的系統或S3時段）位於不同可用度區域或區域、則您的雲端供應商會向您收取資料傳輸成本。如需詳細資料、請參閱以下連結：

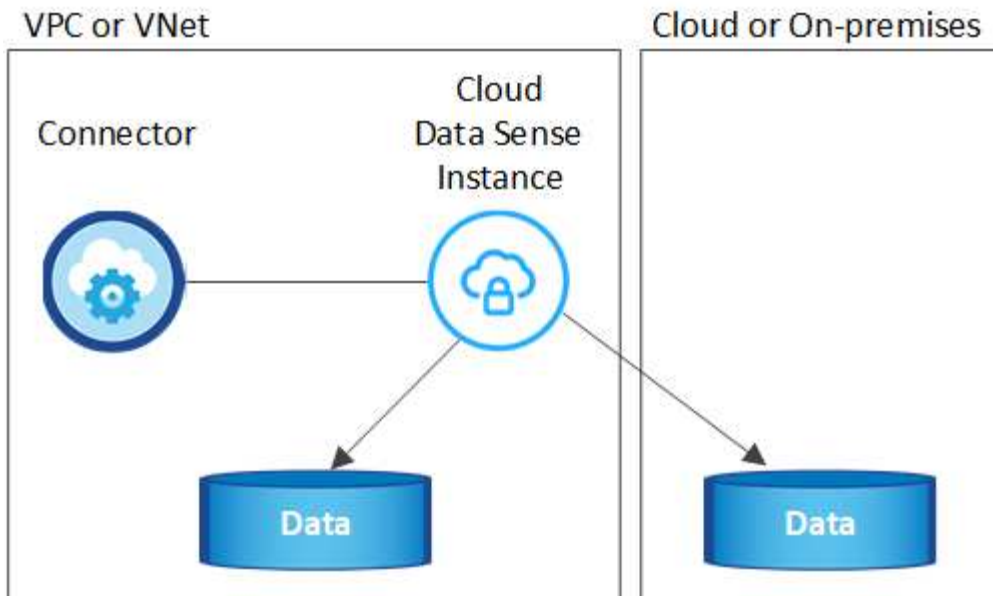
- ["AWS：Amazon EC2 定價"](#)
- ["Microsoft Azure：頻寬定價詳細資料"](#)
- ["Google Cloud：儲存傳輸服務定價"](#)

Cloud Data Sense執行個體

當您在雲端部署Data Sense時、Cloud Manager會將執行個體部署在連接器所在的同一子網路中。 ["深入瞭解連接器。"](#)



如果連接器安裝在內部環境中、它會在Cloud Volumes ONTAP 要求中的第一個支援系統相同VPC或vnet中部署Cloud Data Sense執行個體。您也可以內部安裝Data Sense。



請注意下列關於預設執行個體的資訊：

- 在AWS中、Cloud Data Sense可在上執行 "[m5.4xLarge 執行個體](#)" 使用 500 GB GP2 磁碟。作業系統映像是Amazon Linux 2 (Red Hat 7.3.1)。

在無法使用m5.4xLarge的區域中、Data Sense會改為在m4.4xLarge執行個體上執行。

- 在Azure中、Cloud Data Sense可在上執行 "[Standard_D16s_v3 VM](#)" 使用 512 GB 磁碟。作業系統映像是CentOS 7.8。
- 在GCP中、Cloud Data Sense可在上執行 "[n2-Standard-16 VM](#)" 使用512 GB標準持續磁碟。作業系統映像是CentOS 7.9。

在無法使用n2-Standard-16的區域中、Data Sense會改為在n2d-Standard-16或n1-Standard-16 VM上執行。

- 此執行個體的名稱為 `CloudCompliance_`、並以產生的雜湊 (`UUID`) 串聯在其中。例如：
`_CloudCompliance -16bb6564-38ad-4080-9a92-36f5fd2f71c7`
- 每個連接器只部署一個Data Sense執行個體。
- 只要執行個體能夠存取網際網路、就會自動升級Data Sense軟體。



由於Cloud Data Sense會持續掃描資料、因此執行個體應隨時保持執行狀態。

使用較小的執行個體類型

您可以在CPU較少、RAM較少的系統上部署Data Sense、但使用這些功能較不強大的系統時會有一些限制。

系統大小	規格	限制
超大 (預設)	16個CPU、64 GB RAM 、500 GB SSD	無
中	8個CPU、32 GB RAM 、200 GB SSD	掃描速度較慢、最多只能掃描100萬個檔案。

系統大小	規格	限制
小	8個CPU、16 GB RAM 、100 GB SSD	與「中」相同的限制、加上識別能力 "資料主旨名稱" 內部檔案已停用。

在雲端部署Data Sense時、如果您想要使用其中一個較小的系統、請寄送電子郵件至ng-contact-data-sense@netapp.com尋求協助。我們需要與您合作、以部署這些較小型的雲端組態。

在內部部署Data Sense時、只需使用規格較小的Linux主機即可。您不需要聯絡NetApp尋求協助。

Cloud Data Sense的運作方式

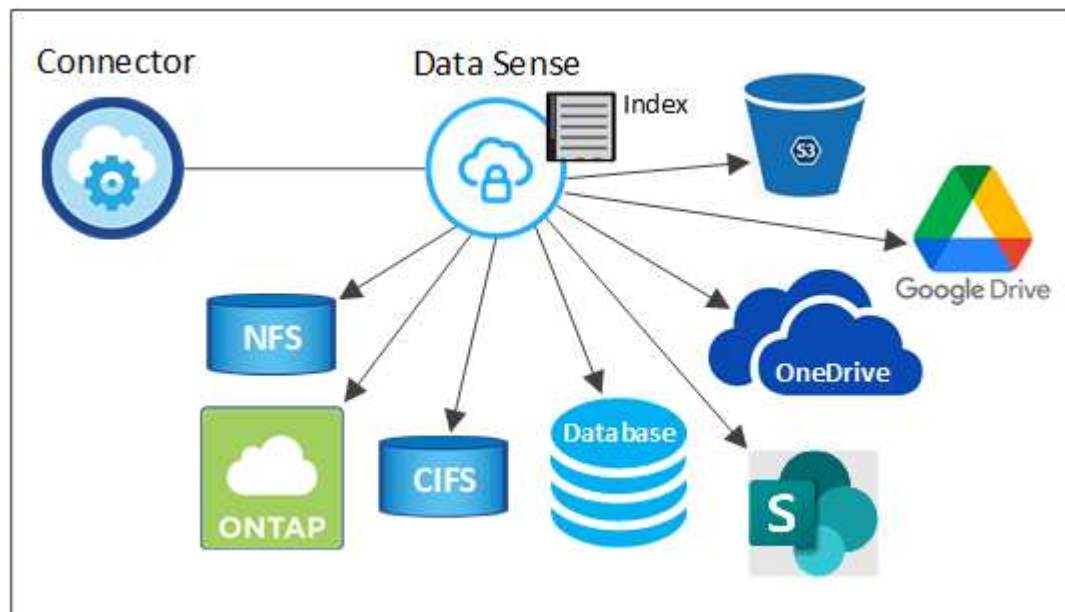
在高層級、Cloud Data Sense的運作方式如下：

1. 您可以在Cloud Manager中部署Data Sense執行個體。
2. 您可以在一或多個工作環境或資料來源上啟用高層對應或深度層級掃描。
3. Data Sense會使用AI學習程序掃描資料。
4. 您可以使用所提供的儀表板和報告工具、協助您達成法規遵循與治理目標。

掃描的運作方式

啟用Cloud Data Sense並選取您要掃描的磁碟區、儲存區、資料庫架構、OneDrive或SharePoint使用者資料之後、它會立即開始掃描資料、以識別個人和敏感資料。它會對應您的組織資料、分類每個檔案、並識別及擷取資料中的實體和預先定義的模式。掃描結果是個人資訊、敏感個人資訊、資料類別和檔案類型的索引。

Data Sense可掛載NFS和CIFS磁碟區、如同任何其他用戶端一樣連線至資料。NFS 磁碟區會自動以唯讀方式存取、而您需要提供 Active Directory 認證來掃描 CIFS 磁碟區。



在初始掃描之後、Data Sense會持續掃描您的資料、以偵測遞增變更（這也是為何務必保持執行個體的重要性）。

您可以在磁碟區層級、儲存庫層級、資料庫架構層級、OneDrive使用者層級和SharePoint網站層級啟用和停用

掃描。

對應掃描與分類掃描之間有何差異

Cloud Data Sense可讓您在選定的工作環境和資料來源上執行一般的「對應」掃描。對應只提供資料的高層級總覽、而分類則提供資料的深度層級掃描。您可以很快在資料來源上完成對應、因為它不會存取檔案來查看內部資料。

許多使用者之所以喜歡這項功能、是因為他們想要快速掃描資料、找出需要更多研究的資料來源、然後只能針對需要的資料來源或磁碟區進行分類掃描。

下表顯示部分差異：

功能	分類	對應
掃描速度	慢	快速
檔案類型和已用容量的清單	是的	是的
檔案數量和已用容量	是的	是的
檔案的存留時間和大小	是的	是的
執行的能力 "資料對應報告"	是的	是的
「資料調查」頁面可檢視檔案詳細資料	是的	否
在檔案中搜尋名稱	是的	否
建立 "原則" 提供自訂搜尋結果	是的	否
使用AIP標籤和狀態標籤來分類資料	是的	否
複製、刪除及移動來源檔案	是的	否
執行其他報告的能力	是的	否

Cloud Data Sense索引的資訊

Data Sense會收集、索引及指派類別給您的資料（檔案）。Data Sense索引的資料包括下列項目：

標準中繼資料

Cloud Data Sense會收集有關檔案的標準中繼資料：檔案類型、檔案大小、建立和修改日期等。

個人資料

個人識別資訊、例如電子郵件地址、識別號碼或信用卡號碼。 ["深入瞭解個人資料"](#)。

敏感的個人資料

GDPR 及其他隱私權法規所定義的特殊敏感資訊類型、例如健康資料、族群來源或政治見解。 ["深入瞭解敏感的個人資料"](#)。

類別

Cloud Data Sense會將掃描的資料分成不同類型的類別。類別是以 AI 分析每個檔案的內容和中繼資料為基礎的主題。 ["深入瞭解類別"](#)。

類型

Cloud Data Sense會將掃描的資料取走、並依檔案類型加以細分。 "[深入瞭解類型](#)"。

名稱實體辨識

Cloud Data Sense使用AI從文件中擷取天然人士的姓名。 "[瞭解如何回應資料主體存取要求](#)"。

網路總覽

Cloud Manager部署Cloud Data Sense執行個體時、其安全群組可從Connector執行個體啟用傳入HTTP連線。

在SaaS模式下使用Cloud Manager時、Cloud Manager連線會透過HTTPS提供、而在瀏覽器和Data Sense執行個體之間傳送的私有資料則會以端點對端點加密來保護、這表示NetApp和第三方無法讀取。

傳出規則已完全開啟。需要存取網際網路、才能安裝及升級Data Sense軟體、並傳送使用量標準。

如果您有嚴格的網路需求、 "[深入瞭解Cloud Data意義上的端點](#)"。

使用者存取法規遵循資訊

指派給每位使用者的角色、可在Cloud Manager內及Cloud Data範圍內提供不同的功能：

- *帳戶管理員*可管理所有工作環境的法規遵循設定及檢視法規遵循資訊。
- *工作區管理*只能管理具有存取權限的系統的法規遵循設定及檢視法規遵循資訊。如果Workspace管理程式無法在Cloud Manager中存取工作環境、他們就無法在「Data Sense（資料感測）」索引標籤中看到工作環境的任何法規遵循資訊。
- 具有* Compliance Viewer*角色的使用者只能檢視法規遵循資訊、並針對擁有存取權限的系統產生報告。這些使用者無法啟用 / 停用掃描磁碟區、儲存區或資料庫架構。這些使用者也無法複製、移動或刪除檔案。

"[深入瞭解 Cloud Manager 角色](#)" 以及使用方法 "[新增具有特定角色的使用者](#)"。

部署Cloud Data Sense

在雲端部署Cloud Data Sense

完成幾個步驟、在雲端部署Cloud Data Sense。

請注意、您也可以 "[在可存取網際網路的Linux主機上部署Data Sense](#)"。如果您偏好使用ONTAP 內部部署的Data Sense執行個體來掃描內部部署的支援系統、安裝類型可能是個不錯的選擇、但這並不是必要的。無論您選擇哪種安裝方法、軟體的運作方式都完全相同。

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。

如果您還沒有連接器、請立即建立連接器。請參閱 "[在 AWS 中建立連接器](#)"、 "[在 Azure 中建立 Connector](#)"或 "[在GCP中建立連接器](#)"。

您也可以 "[在內部部署連接器](#)" 在網路或雲端的Linux主機上。

確保您的環境符合先決條件。這包括執行個體的傳出網際網路存取、連接器與Cloud Data Sense之間透過連接埠443的連線等。請參閱完整清單。

預設組態需要16個vCPU用於Cloud Data Sense執行個體。請參閱 "執行個體類型的詳細資料"。

啟動安裝精靈、在雲端部署Cloud Data Sense執行個體。

Cloud Data Sense在Cloud Manager中掃描的前1 TB資料是免費的。您必須透過雲端供應商Marketplace訂閱Cloud Manager、或取得NetApp BYOL授權、才能在該時間點之後繼續掃描資料。

建立連接器

如果您還沒有Connector、請在雲端供應商中建立Connector。請參閱 "在 AWS 中建立連接器" 或 "在 Azure 中建立 Connector"或 "在GCP中建立連接器"。在大多數情況下、您可能會先設定Connector、然後才嘗試啟動Cloud Data Sense、因為大多數情況都是如此 "Cloud Manager 功能需要連接器"但有些情況下您需要立即設定一個。

有些情況下、您必須使用部署在特定雲端供應商中的Connector：

- 在Cloud Volumes ONTAP AWS、Amazon FSX for ONTAP S2或AWS S3儲存區中掃描資料時、您會在AWS中使用連接器。
- 在 Cloud Volumes ONTAP Azure 或 Azure NetApp Files 以不一樣的方式掃描資料時、您需要使用 Azure 中的連接器。
- 在Cloud Volumes ONTAP GCP中掃描資料時、請使用GCP中的Connector。

使用ONTAP 上述任何雲端連接器時、均可掃描內部系統、非NetApp檔案共用、一般S3物件儲存設備、資料庫、OneDrive資料夾、SharePoint帳戶及Google雲端磁碟帳戶。

請注意、您也可以 "在內部部署連接器" 在網路或雲端的Linux主機上。有些打算在內部安裝Data Sense的使用者也可能選擇在內部安裝Connector。

如您所見、您可能需要使用某些情況 "多個連接器"。



如果您計畫掃描Azure NetApp Files Sure Volume、則必須確保部署的區域與您想要掃描的Volume相同。

檢閱先決條件

在雲端部署Cloud Data Sense之前、請先檢閱下列先決條件、確定您擁有支援的組態。

從Cloud Data Sense啟用傳出網際網路存取

Cloud Data Sense需要傳出網際網路存取。如果您的虛擬或實體網路使用Proxy伺服器進行網際網路存取、請確定Data Sense執行個體具有傳出網際網路存取權限、以聯絡下列端點。當您在雲端部署Data Sense時、它與Connector位於同一個子網路中。

根據您是在AWS、Azure或GCP中部署Cloud Data Sense、請檢閱下方適當的表格。

- AWS 部署所需的端點： *

端點	目的
https://cloudmanager.cloud.netapp.com	與Cloud Manager服務（包括NetApp帳戶）進行通訊。

端點	目的
https://netapp-cloud-account.auth0.com https://auth0.com	與 NetApp Cloud Central 通訊、以進行集中式使用者驗證。
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srrn.cloudfront.net/ https://production.cloudflare.docker.com/	提供軟體映像、資訊清單和範本的存取權限。
https://kinesis.us-east-1.amazonaws.com	讓 NetApp 能夠從稽核記錄串流資料。
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://user-feedback-store-prod.s3.us-west-2.amazonaws.com https://customer-data-production.s3.us-west-2.amazonaws.com	讓 Cloud Data Sense 能夠存取及下載資訊清單和範本、並傳送記錄和數據。

- Azure與GCP部署所需的端點：*

端點	目的
https://cloudmanager.cloud.netapp.com	與 Cloud Manager 服務（包括 NetApp 帳戶）進行通訊。
https://netapp-cloud-account.auth0.com https://auth0.com	與 NetApp Cloud Central 通訊、以進行集中式使用者驗證。
https://support.compliance.cloudmanager.cloud.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srrn.cloudfront.net/ https://production.cloudflare.docker.com/	提供軟體映像、資訊清單、範本的存取、以及傳送記錄和度量資料的功能。
https://support.compliance.cloudmanager.cloud.netapp.com/	讓 NetApp 能夠從稽核記錄串流資料。

確保 Cloud Manager 擁有所需的權限

確保 Cloud Manager 擁有部署資源的權限、並為 Cloud Data Sense 執行個體建立安全群組。您可以在中找到最新的 Cloud Manager 權限 ["NetApp 提供的原則"](#)。

檢查 vCPU 的限制

確保雲端供應商的 vCPU 限制允許部署 16 個核心的執行個體。您需要驗證 Cloud Manager 所在區域中相關執行個體系列的 vCPU 限制。 ["請參閱所需的執行個體類型"](#)。

如需 vCPU 限制的詳細資料、請參閱下列連結：

- ["AWS 文件：Amazon EC2 服務配額"](#)
- ["Azure 文件：虛擬機器 vCPU 配額"](#)
- ["Google Cloud 文件：資源配額"](#)

請注意、您可以在CPU較少、RAM較少的系統上部署Data Sense、但使用這些系統時仍有限制。請參閱["使用較小的執行個體類型"](#)以取得詳細資料。

確保Cloud Manager Connector能夠存取Cloud Data Sense

確保Connector與Cloud Data Sense執行個體之間的連線能力。連接器的安全性群組必須允許傳入和傳出經由連接埠443的流量進出Data Sense執行個體。此連線可部署Data Sense執行個體、並可讓您在「Compliance and Governance（法規遵循與治理）」索引標籤中檢視資訊。AWS和Azure的政府區域均支援Cloud Data Sense。

AWS和AWS GovCloud部署需要額外的傳入和傳出規則。請參閱["AWS 中 Connector 的規則"](#)以取得詳細資料。

Azure和Azure政府部署需要額外的傳入和傳出規則。請參閱["Azure 中的 Connector 規則"](#)以取得詳細資料。

確保雲端資料認證能夠持續運作

Cloud Data Sense執行個體必須持續運作、才能持續掃描資料。

確保網頁瀏覽器連線至Cloud Data Sense

啟用Cloud Data Sense之後、請確保使用者從連線至Data Sense執行個體的主機存取Cloud Manager介面。

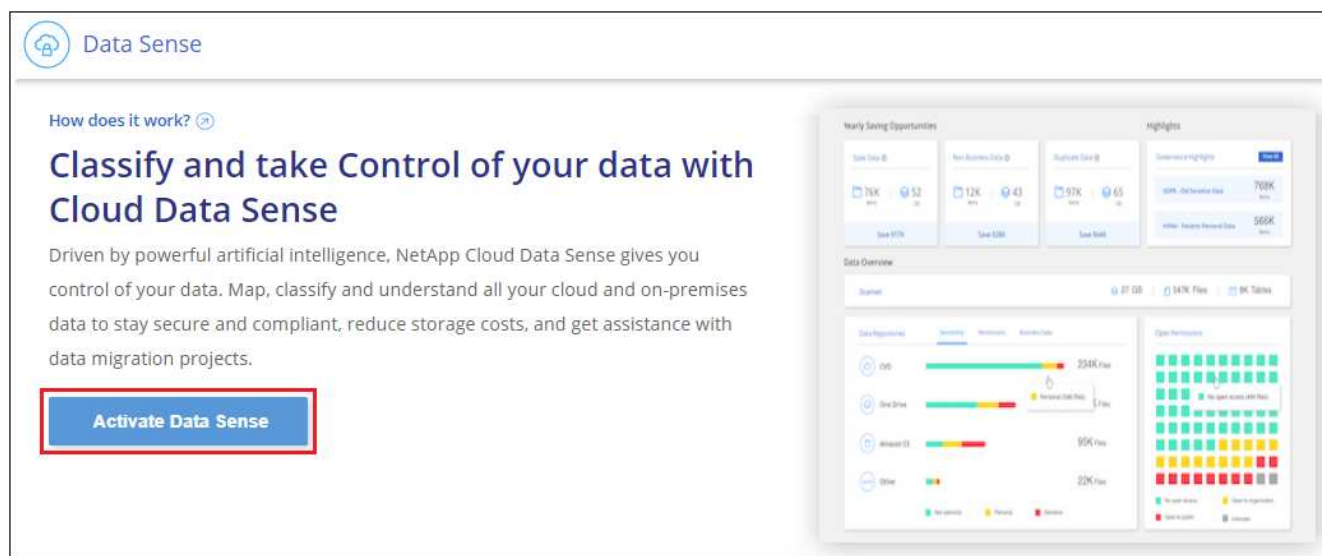
Data Sense執行個體使用私有IP位址、確保索引資料無法存取網際網路。因此、您用來存取 Cloud Manager的網頁瀏覽器必須連線至該私有 IP 位址。這種連線可能來自直接連線至雲端供應商（例如VPN）、或來自與Data Sense執行個體位於同一個網路內的主機。

在雲端部署Data Sense

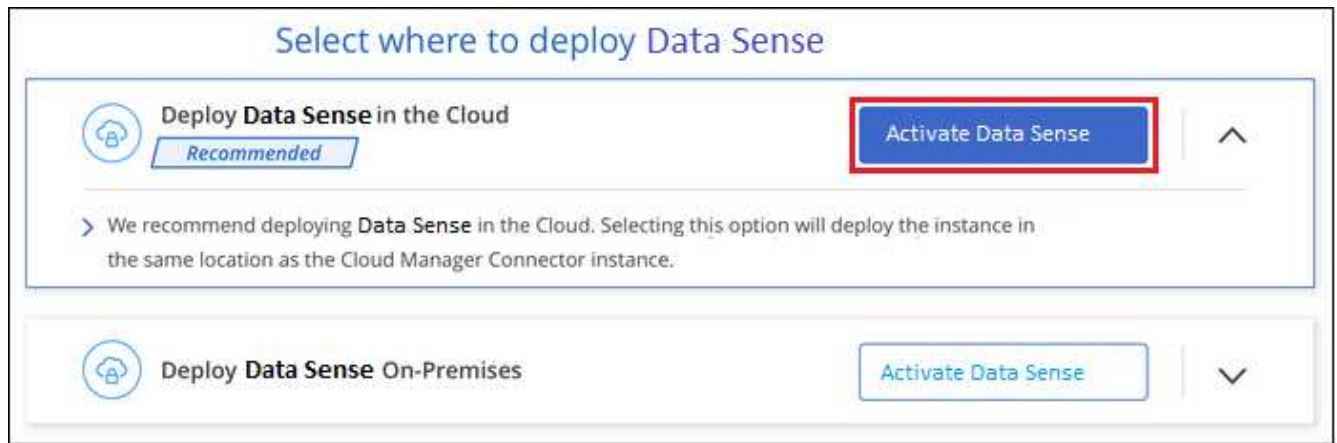
請遵循下列步驟、在雲端部署Cloud Data Sense執行個體。

步驟

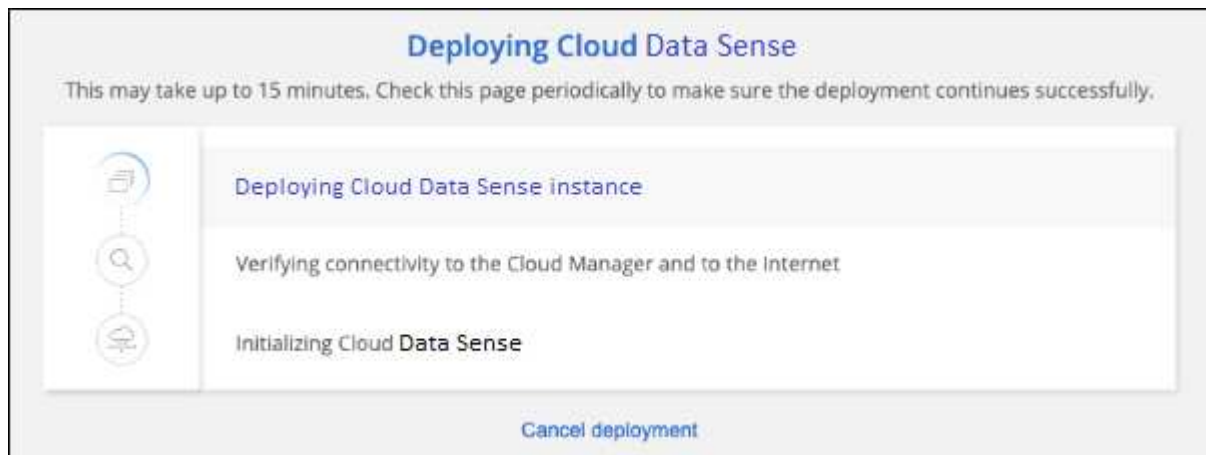
1. 在Cloud Manager中、按一下* Data Sense *。
2. 按一下「啟動資料感應」。



3. 按一下「啟動資料感應」以啟動雲端部署精靈。



4. 精靈會在執行部署步驟時顯示進度。如果遇到任何問題、它將會停止並徵求意見。



5. 部署執行個體後、按一下*繼續進行組態*以移至「_Configuration」頁面。

Cloud Manager可在雲端供應商中部署Cloud Data Sense執行個體。

您可以從「組態」頁面選取要掃描的資料來源。

您也可以 ["設定Cloud Data Sense授權"](#) 目前。在資料量超過 1 TB 之前、您將不會付費。

在可存取網際網路的Linux主機上部署Cloud Data Sense

完成幾個步驟、即可在網路或雲端上可存取網際網路的Linux主機上部署Cloud Data Sense。

如果您偏好使用ONTAP 內部部署的Data Sense執行個體來掃描內部部署的支援系統、則內部安裝可能是個不錯的選擇、但這並非必要。無論您選擇哪種安裝方法、軟體的運作方式都完全相同。

請注意、您也可以 ["在無法存取網際網路的內部部署網站上部署Data Sense"](#) 完全安全的網站。

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。

如果您還沒有連接器、請立即建立連接器。請參閱 ["在 AWS 中建立連接器"](#)、["在 Azure 中建立 Connector"](#)或 "

在GCP中建立連接器"。

您也可以 "在內部部署連接器" 在網路或雲端的Linux主機上。

確保您的環境符合先決條件。這包括執行個體的傳出網際網路存取、連接器與Cloud Data Sense之間透過連接埠443的連線等。請參閱完整清單。

您也需要符合的Linux系統 符合下列需求。

從NetApp支援網站下載Cloud Data Sense軟體、並將安裝程式檔案複製到您打算使用的Linux主機。然後啟動安裝精靈、並依照提示部署Data Sense執行個體。

Cloud Data Sense在Cloud Manager中掃描的前1 TB資料是免費的。您必須向雲端供應商Marketplace訂閱、或向NetApp訂購BYOL授權、才能在該時間點之後繼續掃描資料。

建立連接器

如果您還沒有Connector、請在雲端供應商中建立Connector。請參閱 "在 AWS 中建立連接器" 或 "在 Azure 中建立 Connector"或 "在GCP中建立連接器"。在大多數情況下、您可能會先設定Connector、然後才嘗試啟動Cloud Data Sense、因為大多數情況都是如此 "Cloud Manager 功能需要連接器"但有些情況下您需要立即設定一個。

有些情況下、您必須使用部署在特定雲端供應商中的Connector：

- 在Cloud Volumes ONTAP AWS、Amazon FSX for ONTAP S2或AWS S3儲存區中掃描資料時、您會在AWS中使用連接器。
- 在 Cloud Volumes ONTAP Azure 或 Azure NetApp Files 以不一樣的方式掃描資料時、您需要使用 Azure 中的連接器。
- 在Cloud Volumes ONTAP GCP中掃描資料時、請使用GCP中的連接器。

內部ONTAP 系統、非NetApp檔案共用、一般S3物件儲存、資料庫、OneDrive資料夾、SharePoint帳戶及Google雲端硬碟帳戶均可使用下列任何一種Cloud Connector進行掃描。

請注意、您也可以 "在內部部署連接器" 在網路或雲端的Linux主機上。有些打算在內部安裝Data Sense的使用者也可能選擇在內部安裝Connector。

如您所見、您可能需要使用某些情況 "多個連接器"。



如果您計畫掃描Azure NetApp Files Sure Volume、則必須確保部署的區域與您想要掃描的Volume相同。

準備Linux主機系統

資料感應軟體必須在符合特定作業系統需求、RAM需求、軟體需求等的主機上執行。與其他應用程式共用的主機不支援Data Sense、主機必須是專屬主機。

- 作業系統： Red Hat Enterprise Linux 或 CentOS 8.0 或 8.1 版
 - 作業系統必須能夠安裝 Docker 引擎（例如、視需要停用 *firewalld* 服務）
- 磁碟：SSD搭載500 GiB、可在/、或上使用
 - 100 GiB可在/op

- 400 GiB可在/var
- 5 GiB、位於/tmp
- RAM：64 GB（交換記憶體必須在主機上停用）
- CPU：16核心

請注意、您可以在CPU較少、RAM較少的系統上部署Data Sense、但使用這些系統時仍有限制。請參閱 ["使用較小的執行個體類型"](#) 以取得詳細資料。

- Red Hat Enterprise Linux 系統必須在 Red Hat 訂購管理中註冊。如果未註冊、系統將無法在安裝期間存取儲存庫來更新所需的協力廠商軟體。
- 主機上必須安裝下列軟體。如果主機上尚未存在、安裝程式會為您安裝軟體：
 - Docker Engine 19版或更新版本。 ["檢視安裝指示"](#)。
 - Python 3版本3.6或更新版本。 ["檢視安裝指示"](#)。

驗證Cloud Manager和Data Sense必要條件

在Linux系統上部署Cloud Data Sense之前、請先檢閱下列先決條件、確定您擁有支援的組態。

從Cloud Data Sense啟用傳出網際網路存取

Cloud Data Sense需要傳出網際網路存取。如果您的虛擬或實體網路使用Proxy伺服器進行網際網路存取、請確定Data Sense執行個體具有傳出網際網路存取權限、以聯絡下列端點。

端點	目的
https://cloudmanager.cloud.netapp.com	與Cloud Manager服務（包括NetApp帳戶）進行通訊。
https://netapp-cloud-account.auth0.com https://auth0.com	與 NetApp Cloud Central 通訊、以進行集中式使用者驗證。
https://support.compliance.cloudmanager.cloud.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	提供軟體映像、資訊清單、範本的存取、以及傳送記錄和度量資料的功能。
https://support.compliance.cloudmanager.cloud.netapp.com/	讓 NetApp 能夠從稽核記錄串流資料。
https://github.com/docker https://download.docker.com http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	提供安裝所需的必要套件。

確保 Cloud Manager 擁有所需的權限

確保Cloud Manager擁有部署資源的權限、並為Cloud Data Sense執行個體建立安全群組。您可以在中找到最新的 Cloud Manager 權限 ["NetApp 提供的原則"](#)。

確保Cloud Manager Connector能夠存取Cloud Data Sense

確保Connector與Cloud Data Sense執行個體之間的連線能力。連接器的安全性群組必須允許傳入和傳出經由連接埠443的流量進出Data Sense執行個體。

此連線可部署Data Sense執行個體、並可讓您在「Compliance and Governance（法規遵循與治理）」索引標籤中檢視資訊。

請確定連接埠 8080 已開啟、以便在 Cloud Manager 中查看安裝進度。

確保雲端資料認證能夠持續運作

Cloud Data Sense執行個體必須持續運作、才能持續掃描資料。

確保網頁瀏覽器連線至Cloud Data Sense

啟用Cloud Data Sense之後、請確保使用者從連線至Data Sense執行個體的主機存取Cloud Manager介面。

Data Sense執行個體使用私有IP位址、確保索引資料無法存取網際網路。因此、您用來存取 Cloud Manager 的網頁瀏覽器必須連線至該私有 IP 位址。這種連線可能來自直接連線至雲端供應商（例如VPN）、或來自與Data Sense執行個體位於同一個網路內的主機。

在內部部署部署Data Sense

對於一般組態、您將在單一主機系統上安裝軟體。 [請參閱此處的步驟](#)。

對於掃描PB資料的大型組態、您可以納入多個主機、以提供額外的處理能力。 [請參閱此處的步驟](#)。

請參閱 [準備Linux主機系統](#) 和 [檢閱先決條件](#) 以取得部署Cloud Data Sense之前的完整需求清單。

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。



當Azure NetApp Files 軟體安裝在內部部署環境中時、Cloud Data Sense目前無法掃描S3儲存區、功能區、或FSXfor ONTAP the Sf2。在這種情況下、您需要在雲端和部署獨立的Connector和Data Sense執行個體 "[在連接器之間切換](#)" 適用於不同的資料來源。

一般組態的單一主機安裝

在單一內部部署主機上安裝Data Sense軟體時、請遵循下列步驟。

您需要的是 **#8217** ；需要的是什麼

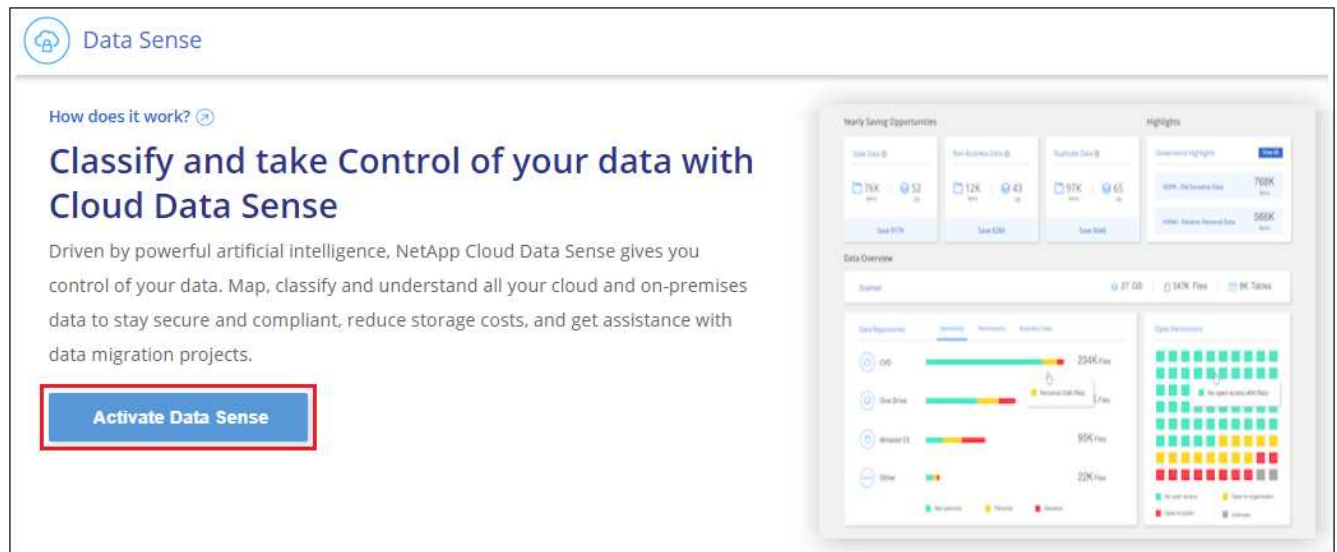
- 確認您的Linux系統符合 [主機需求](#)。
- （選用）確認系統已安裝兩個必要的軟體套件（Docker Engine和Python 3）。如果此軟體尚未安裝在系統上、安裝程式將會安裝此軟體。
- 請確定您擁有Linux系統的root權限。
- 如果您使用的是Proxy、而且它正在執行TLS攔截、則必須知道Data Sense Linux系統上儲存TLS CA憑證的路徑。
- 確認您的離線環境符合所需 [權限與連線能力](#)。

步驟

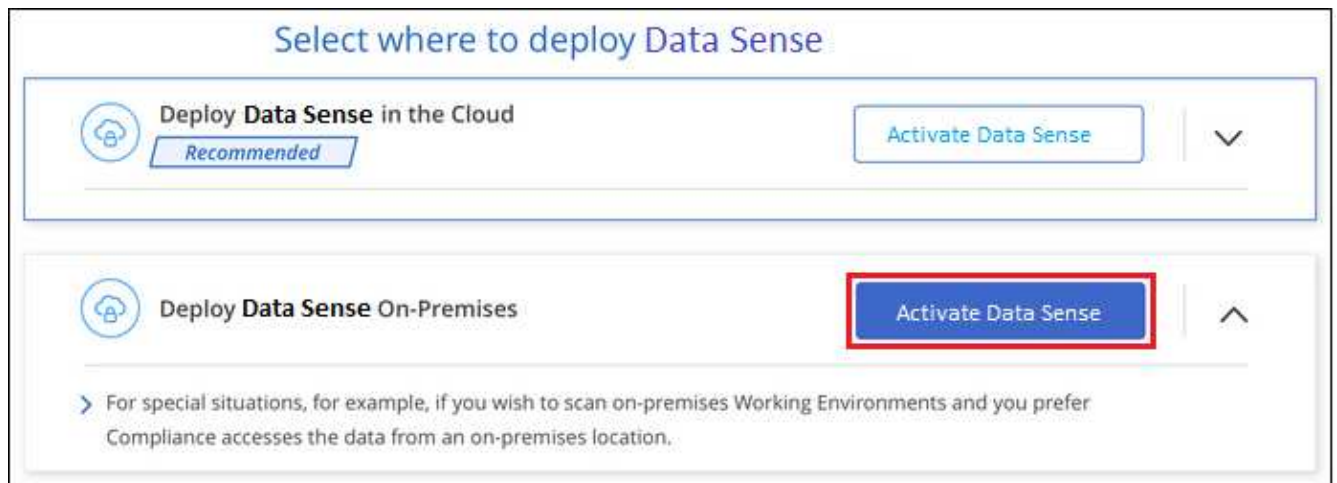
1. 從下載Cloud Data Sense軟體 "[NetApp 支援網站](#)"。您應該選取的檔案名稱為*

cc_OnPrem_installer_.tar.gz*。

2. 將安裝程式檔案複製到您打算使用的 Linux 主機（使用「XCP」或其他方法）。
3. 在Cloud Manager中、按一下* Data Sense *。
4. 按一下「啟動資料感應」。



5. 按一下「啟動資料感應」以啟動內部部署精靈。



6. 在_部署內部部署資料感測_對話方塊中、複製所提供的命令並貼到文字檔中、以便稍後使用、然後按一下*關閉*。例如：

```
「Udo ./install.sh -a 12345 -c 27AG75 -t 2198qq」
```

7. 在主機上解壓縮安裝程式檔案、例如：

```
tar -xzf cc_onprem_installer_1.10.0.tar.gz
```

8. 當安裝程式提示時、您可以在一系列提示中輸入所需的值、或是將所需的參數作為命令列引數提供給安裝程式：

根據提示輸入參數：	輸入完整命令：
<p>a. 貼上您從步驟6複製的資訊：「Udo ./install.sh -a <account_id>-c <agent_id>-t <token>」</p> <p>b. 輸入Data Sense主機機器的IP位址或主機名稱、以便連接器執行個體存取。</p> <p>c. 輸入Cloud Manager Connector主機機器的IP位址或主機名稱、以便Data Sense執行個體存取。</p> <p>d. 根據提示輸入 Proxy 詳細資料。如果您的Cloud Manager已使用Proxy、則不需要在此輸入此資訊、因為Data Sense會自動使用Cloud Manager所使用的Proxy。</p>	<p>或者、您也可以事先建立整個命令、提供必要的主機和Proxy參數：「Udo ./install.sh -A <account_id>-c <agent_id>-t <token>-host <ds_host>-manager-host <cm_host>-proxy_host <proxy_host>--proxy-port <proxy_port>-cert-proxy_proxy_proxy_proxy><key><key_proxy_proxy_user-proxy_proxy>-tese></p>

變數值：

- *Account_id* = NetApp 帳戶 ID
- *agent_id* = 連接器 ID
- *token* = JWT 使用者權杖
- *DS_host* = Data Sense Linux系統的IP位址或主機名稱。
- *cm_host* = Cloud Manager Connector系統的IP位址或主機名稱。
- *proxy_host* = 代理伺服器的 IP 或主機名稱（如果主機位於 Proxy 伺服器之後）。
- *proxy_port* = 連接到 Proxy 伺服器的連接埠（預設值 80 ）。
- *proxy_schap* = 連線配置：HTTPS或http（預設http）。
- *proxy_user* = 驗證的使用者、如果需要基本驗證、則可連線至 Proxy 伺服器。
- *proxy_password* = 您指定之使用者名稱的密碼。
- *ca_cert_dir* = Data Sense Linux系統上包含額外TLS CA憑證套件的路徑。僅當Proxy執行TLS攔截時才需要。

Cloud Data Sense安裝程式會安裝套件、安裝泊塢視窗、註冊安裝、以及安裝Data Sense。安裝可能需要 10 到 20 分鐘。

如果主機與連接器執行個體之間有連接埠8080的連線、您會在Cloud Manager的Data Sense（資料感測）索引標籤中看到安裝進度。

您可以從「組態」頁面選取要掃描的資料來源。

您也可以 ["設定Cloud Data Sense授權"](#) 目前。在資料量超過 1 TB 之前、您將不會付費。

適用於大型組態的多主機安裝

對於掃描PB資料的大型組態、您可以納入多個主機、以提供額外的處理能力。使用多個主機系統時、主要系統稱為 `_Manager節點_`、而提供額外處理能力的其他系統稱為 `_scaliple nodes _`。

在多部內部部署主機上安裝Data Sense軟體時、請遵循下列步驟。

您需要的是 **#8217** ；需要的是什麼

- 確認Manager和掃描儀節點的所有Linux系統都符合 [主機需求](#)。
- （選用）確認系統已安裝兩個必要的軟體套件（Docker Engine和Python 3）。如果系統上尚未安裝此軟體、安裝程式將會安裝此軟體。
- 請確定您擁有Linux系統的root權限。
- 確認您的環境符合所需 [權限與連線能力](#)。
- 您必須擁有要使用的掃描器節點主機的IP位址。
- 必須在所有主機上啟用下列連接埠和傳輸協定：

連接埠	通訊協定	說明
2377	TCP	叢集管理通訊
7946	TCP、udp	節點間通訊
4789	UDP	重疊網路流量
50	電子穩定程序	加密的IPsec覆疊網路（ESP）流量
111.	TCP、udp	NFS伺服器、用於在主機之間共用檔案（從每個掃描儀節點到管理器節點都需要）
2049	TCP、udp	NFS伺服器、用於在主機之間共用檔案（從每個掃描儀節點到管理器節點都需要）

步驟

1. 請依照中的步驟1至7進行 [單一主機安裝](#) 在管理器節點上。
2. 如步驟8所示、當安裝程式提示時、您可以在一系列提示中輸入所需的值、也可以將所需的參數作為命令列引數提供給安裝程式。

除了可用於單一主機安裝的變數之外、還會使用新的選項*- n <node_ip>*來指定掃描儀節點的IP位址。多個掃描儀節點IP之間以一個逗號分隔。

例如、此命令會新增3個掃描儀節點：「Udo ./install.sh -a <account_id>-c <agent_id>-t <token>-host <ds_host>-manager-host <cm_host>*-n <node_ip1>、<node_ip2>、<node_ip3>*-proxy-host <proxy_proxy_proxy_proxy_proxy_proxy_proxy_user-proxy_proxy>*

3. 在管理器節點安裝完成之前、會有一個對話方塊顯示掃描儀節點所需的安裝命令。複製命令並將其儲存在文字檔中。例如：

「Udo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212」

4. 在*每個*掃描儀節點主機上：
 - a. 將Data Sense安裝程式檔案（* cc_OnPrem_installer_<版本>.tar.gz*）複製到主機（使用「scp」或其他方法）。
 - b. 解壓縮安裝程式檔案。
 - c. 貼上並執行您在步驟3中複製的命令。

在所有掃描儀節點上完成安裝、並已加入管理器節點之後、管理器節點的安裝也會完成。

Cloud Data Sense安裝程式會完成套件、Docker的安裝、並登錄安裝。安裝可能需要 10 到 20 分鐘。

您可以從「組態」頁面選取要掃描的資料來源。

您也可以 "[設定Cloud Data Sense授權](#)" 目前。在資料量超過 1 TB 之前、您將不會付費。

在內部部署Cloud Data Sense、無需存取網際網路

請完成幾個步驟、在內部部署站台的主機上部署Cloud Data Sense、但該站台無法存取網際網路。這類安裝最適合安全的站台。

請注意、您也可以 "[將Data Sense部署在可存取網際網路的內部部署站台](#)"。

支援的資料來源

以這種方式安裝（有時稱為「離線」或「暗」站台）時、Data Sense只能掃描內部部署站台上本機資料來源的資料。此時、Data Sense可掃描下列本機資料來源：

- 內部部署ONTAP 的作業系統
- 資料庫架構
- 非NetApp NFS或CIFS檔案共用
- 使用簡易儲存服務（S3）傳輸協定的物件儲存設備

如果您需要非常安全的Cloud Manager安裝、但又想要從OneDrive帳戶或SharePoint帳戶掃描本機資料、則可以使用Data Sense離線安裝程式、並提供網際網路存取功能給少數幾個選定的端點。請參閱 [SharePoint和OneDrive的特殊需求](#) 以取得詳細資料。

當Data Sense部署在黑暗的站台時、目前不支援掃描Cloud Volumes ONTAP 功能的支援功能包括：適用於Azure NetApp Files 下列項目的功能：適用於ONTAP 支援功能的功能：

限制

大多數的Data Sense功能都能在部署於無法存取網際網路的站台上運作。不過、某些需要網際網路存取的功能則不受支援、例如：

- 管理Microsoft Azure資訊保護（AIP）標籤
- 當某些關鍵原則傳回結果時、會傳送電子郵件警示給Cloud Manager使用者
- 為不同使用者設定Cloud Manager角色（例如、Account Admin或Compliance Viewer）
- 使用Cloud Sync 還原複製與同步來源檔案
- 接收使用者意見反應
- 從Cloud Manager自動升級軟體

Cloud Manager Connector和Data Sense都需要定期手動升級、才能啟用新功能。您可以在Data Sense UI 頁面底部看到Data Sense版本。請檢查 "[Cloud Data Sense版本說明](#)" 查看每個版本的新功能、以及您是否想要這些功能。然後您可以依照下列步驟進行 [升級您的Data Sense軟體](#)。

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。

如果您的離線內部部署站台上尚未安裝Connector、"[部署Connector](#)" 現在就在Linux主機上。

確保您的Linux系統符合 [主機需求](#)、並已安裝所有必要的軟體、而且您的離線環境符合所需 [權限與連線能力](#)。

從NetApp支援網站下載Cloud Data Sense軟體、並將安裝程式檔案複製到您打算使用的Linux主機。然後啟動安裝精靈、並依照提示部署Cloud Data Sense執行個體。

Cloud Data Sense在Cloud Manager中掃描的前1 TB資料是免費的。NetApp需要BYOL授權、才能在該點之後繼續掃描資料。

安裝Cloud Manager Connector

如果您的離線內部部署站台上尚未安裝Cloud Manager Connector、"[部署Connector](#)" 在離線站台的Linux主機上。

準備Linux主機系統

資料感應軟體必須在符合特定作業系統需求、RAM需求、軟體需求等的主機上執行。與其他應用程式共用的主機不支援Data Sense、主機必須是專屬主機。

- 作業系統：Red Hat Enterprise Linux 或 CentOS 8.0 或 8.1 版
 - 作業系統必須能夠安裝Docker Engine（例如、視需要停用_firewalld_服務）
- 磁碟：SSD搭載500 GiB、可在/、或上使用
 - 100 GiB可在/op
 - 400 GiB可在/var
 - 5 GiB、位於/tmp
- RAM：64 GB（交換記憶體必須在主機上停用）
- CPU：16核心

請注意、您可以在CPU較少、RAM較少的系統上部署Data Sense、但使用這些系統時仍有限制。請參閱 "[使用較小的執行個體類型](#)" 以取得詳細資料。

在安裝Data Sense之前、您必須先在主機上安裝下列軟體：

- Docker Engine 19版或更新版本。"[檢視安裝指示](#)"。
- Python 3版本3.6或更新版本。"[檢視安裝指示](#)"。

驗證Cloud Manager和Data Sense必要條件

在部署Cloud Data Sense之前、請先檢閱下列先決條件、確定您擁有支援的組態。

- 確保Cloud Manager擁有部署資源的權限、並為Cloud Data Sense執行個體建立安全群組。
- 確保Cloud Manager Connector可以存取Data Sense執行個體。連接器的安全性群組必須允許傳入和傳出經由連接埠443的流量進出Data Sense執行個體。

此連線可部署Data Sense執行個體、並可讓您檢視法規遵循與治理資訊。

請確定連接埠 8080 已開啟、以便在 Cloud Manager 中查看安裝進度。

- 確保雲端資料認證能夠持續運作。Cloud Data Sense執行個體必須持續運作、才能持續掃描資料。
- 確保網頁瀏覽器連線至Cloud Data Sense。啟用Cloud Data Sense之後、請確保使用者從連線至Data Sense執行個體的主機存取Cloud Manager介面。

Data Sense執行個體使用私有IP位址、確保其他人無法存取索引資料。因此、您用來存取 Cloud Manager 的網頁瀏覽器必須連線至該私有 IP 位址。該連線可能來自與Data Sense執行個體位於同一個網路內的主機。

SharePoint和OneDrive的特殊需求

當Cloud Manager和Data Sense部署於無法存取網際網路的網站時、您可以透過網際網路存取部分選定端點、來掃描SharePoint和OneDrive帳戶中的本機檔案。

端點	目的
\login.microsoft.com \graph.microsoft.com	與Microsoft伺服器通訊、以登入所選的線上服務。
https://cloudmanager.cloud.netapp.com	與Cloud Manager服務（包括NetApp帳戶）進行通訊。

只有在初始連線至這些外部服務時、才需要存取_cloudmanager.cloud.netapp.com_。

部署資料感測

對於一般組態、您將在單一主機系統上安裝軟體。"請參閱此處的步驟"。

對於掃描PB資料的大型組態、您可以納入多個主機、以提供額外的處理能力。"請參閱此處的步驟"。

一般組態的單一主機安裝

在離線環境中的單一內部部署主機上安裝Data Sense軟體時、請遵循下列步驟。

您需要的是 **#8217** ；需要的是什麼

- 確認您的Linux系統符合 [主機需求](#)。
- 確認您已安裝兩個必要的軟體套件（Docker Engine和Python 3）。
- 請確定您擁有Linux系統的root權限。
- 確認您的離線環境符合所需 [權限與連線能力](#)。

步驟

1. 在網際網路設定的系統上、從下載Cloud Data Sense軟體 "[NetApp 支援網站](#)"。您應該選取的檔案名稱為*DataSense-offline bund-<版本>.tar.gz*。
2. 將安裝程式套件複製到您打算在黑暗站台中使用的Linux主機。
3. 在主機上解壓縮安裝程式套件、例如：

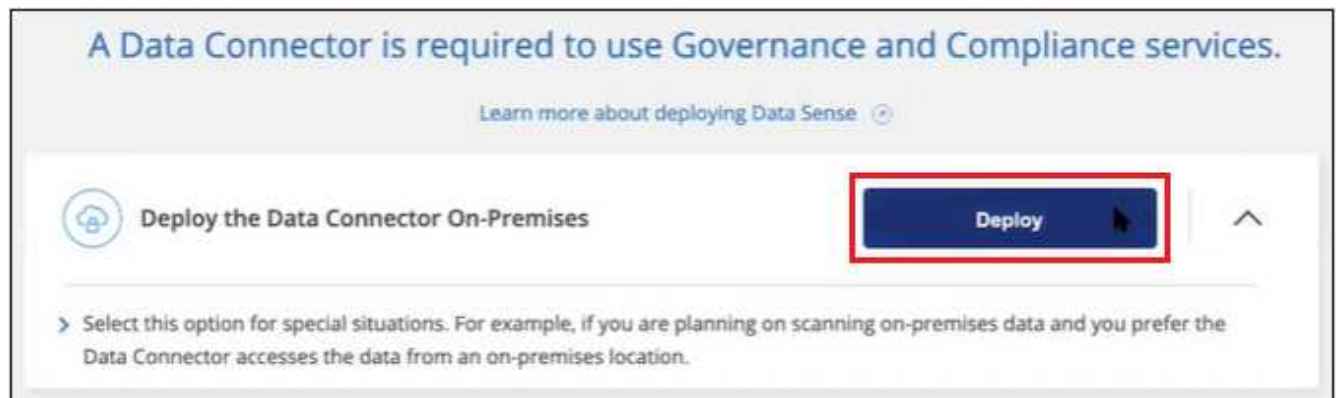
```
tar -xzf DataSense-offline-bundle-v1.10.0.tar.gz
```

這會擷取所需的軟體和實際安裝檔案* cc_OnPrem_installer_*.tar.gz*。

4. 啟動Cloud Manager、然後按一下* Data Sense *（資料感測）索引標籤。
5. 按一下「啟動資料感應」。



6. 按一下「部署」以啟動內部部署精靈。



7. 在_部署內部部署資料感測_對話方塊中、複製所提供的命令並貼到文字檔中、以便稍後使用、然後按一下* 關閉*。例如：

「Udo ./install.sh -a 12345 -c 27AG75 -t 2198qq --暗房」

8. 在主機上解壓縮安裝檔案、例如：

```
tar -xzf cc_onprem_installer_1.10.0.tar.gz
```

9. 當安裝程式提示時、您可以在一系列提示中輸入所需的值、或是將所需的參數作為命令列引數提供給安裝程式：

根據提示輸入參數：	輸入完整命令：
a. 貼上您從步驟7複製的資訊：「Udo ./install.sh -a <account_id>-c <agent_id>-t <token>--lidsite」 b. 輸入Data Sense主機機器的IP位址或主機名稱、以便連接器執行個體存取。 c. 輸入Cloud Manager Connector主機機器的IP位址或主機名稱、以便Data Sense執行個體存取。	或者、您也可以事先建立整個命令、提供必要的主機參數：「Udo ./install.sh -A <account_id>-c <agent_id>-t <token>-host <ds_host>--manager-host <cm_host>--ne-proxy—dimsite」

變數值：

- *Account_id* = NetApp 帳戶 ID
- *agent_id* = 連接器 ID
- *token* = JWT 使用者權杖
- *DS_host* = Data Sense Linux系統的IP位址或主機名稱。
- *cm_host* = Cloud Manager Connector系統的IP位址或主機名稱。

Data Sense安裝程式會安裝套件、登錄安裝、並安裝Data Sense。安裝可能需要 10 到 20 分鐘。

如果主機與連接器執行個體之間有連接埠8080的連線、您會在Cloud Manager的Data Sense（資料感測）索引標籤中看到安裝進度。

在「組態」頁面中、您可以選取本機 **"內部ONTAP 部署的叢集"** 和 **"資料庫"** 您想要掃描的。

您也可以 **"設定Cloud Data Sense的BYOL授權"** 現在請從「數位錢包」頁面。在資料量超過 1 TB 之前、您將不會付費。

適用於大型組態的多主機安裝

對於掃描PB資料的大型組態、您可以納入多個主機、以提供額外的處理能力。使用多個主機系統時、主要系統稱為 *_Manager節點_*、而提供額外處理能力的其他系統稱為 *_scaliple nodes _*。

在離線環境中的多部內部部署主機上安裝Data Sense軟體時、請遵循下列步驟。

您需要的是 **#8217** ；需要的是什麼

- 確認Manager和掃描儀節點的所有Linux系統都符合 **主機需求**。
- 確認您已安裝兩個必要的軟體套件（Docker Engine和Python 3）。
- 請確定您擁有Linux系統的root權限。
- 確認您的離線環境符合所需 **權限與連線能力**。
- 您必須擁有要使用的掃描器節點主機的IP位址。
- 必須在所有主機上啟用下列連接埠和傳輸協定：

連接埠	通訊協定	說明
2377	TCP	叢集管理通訊

連接埠	通訊協定	說明
7946	TCP、udp	節點間通訊
4789	UDP	重疊網路流量
50	電子穩定程序	加密的IPsec覆疊網路（ESP）流量
111.	TCP、udp	NFS伺服器、用於在主機之間共用檔案（從每個掃描儀節點到管理器節點都需要）
2049	TCP、udp	NFS伺服器、用於在主機之間共用檔案（從每個掃描儀節點到管理器節點都需要）

步驟

1. 請依照中的步驟1至8進行 **"單一主機安裝"** 在管理器節點上。
2. 如步驟9所示、當安裝程式提示時、您可以在一系列提示中輸入所需的值、也可以將所需的參數作為命令列引數提供給安裝程式。

除了可用於單一主機安裝的變數之外、還會使用新的選項 `-n <node_ip>` 來指定掃描儀節點的IP位址。多個節點IP之間以一個逗號分隔。

例如、此命令會新增3個掃描儀節點：「Udo ./install.sh -A <account_id>-c <agent_id>-t <token>-host <ds_host>--manager-host <cm_host>*-n <node_IP1>、<node_IP2>、<node_IP3>--ne-proxy-site。

3. 在管理器節點安裝完成之前、會有一個對話方塊顯示掃描儀節點所需的安裝命令。複製命令並將其儲存在文字檔中。例如：

```
「Udo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212」
```

4. 在*每個*掃描儀節點主機上：
 - a. 將Data Sense安裝程式檔案（* cc_OnPrem_installer_<版本>.tar.gz*）複製到主機機器。
 - b. 解壓縮安裝程式檔案。
 - c. 貼上並執行您在步驟3中複製的命令。

在所有掃描儀節點上完成安裝、並已加入管理器節點之後、管理器節點的安裝也會完成。

Cloud Data Sense安裝程式會完成安裝套件、並登錄安裝。安裝可能需要15至25分鐘。

在「組態」頁面中、您可以選取本機 **"內部ONTAP 部署的叢集"** 和本機 **"資料庫"** 您想要掃描的。

您也可以 **"設定Cloud Data Sense的BYOL授權"** 現在請從「數位錢包」頁面。在資料量超過 1 TB 之前、您將不會付費。

升級Data Sense軟體

由於Data Sense軟體會定期更新新功能、因此您應該定期檢查新版本、以確保使用最新的軟體和功能。您需要手動升級Data Sense軟體、因為沒有網際網路連線功能可自動執行升級。

開始之前

- Data Sense軟體一次可升級一個主要版本。例如、如果您已安裝1.9.x版、則只能升級至1.10.x如果您落後幾

個主要版本、就必須多次升級軟體。

- 確認您的內部部署Connector軟體已升級至最新版本。"請參閱連接器升級步驟"。

步驟

1. 在網際網路設定的系統上、從下載Cloud Data Sense軟體 "[NetApp 支援網站](#)"。您應該選取的檔案名稱為* DataSense-offline bund-<版本>.tar.gz*。
2. 將軟體套裝組合複製到安裝Data Sense的Linux主機、
3. 將主機上的軟體套裝組合解壓縮、例如：

```
tar -xvf DataSense-offline-bundle-v1.10.0.tar.gz
```

這會擷取安裝檔案* cc_OnPrem_installer_.tar.gz*。

4. 在主機上解壓縮安裝檔案、例如：

```
tar -xzf cc_onprem_installer_1.10.0.tar.gz
```

這會擷取升級指令碼* start_dimite_upgrade.sh*和任何必要的協力廠商軟體。

5. 在主機上執行升級指令碼、例如：

```
start_darksite_upgrade.sh
```

Data Sense軟體會在您的主機上進行升級。更新可能需要5到10分鐘的時間。

請注意、如果您已在多個主機系統上部署Data Sense來掃描非常大型的組態、則不需要在掃描器節點上進行升級。

您可以檢查Data Sense UI頁面底部的版本、確認軟體是否已更新。

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](#)"。

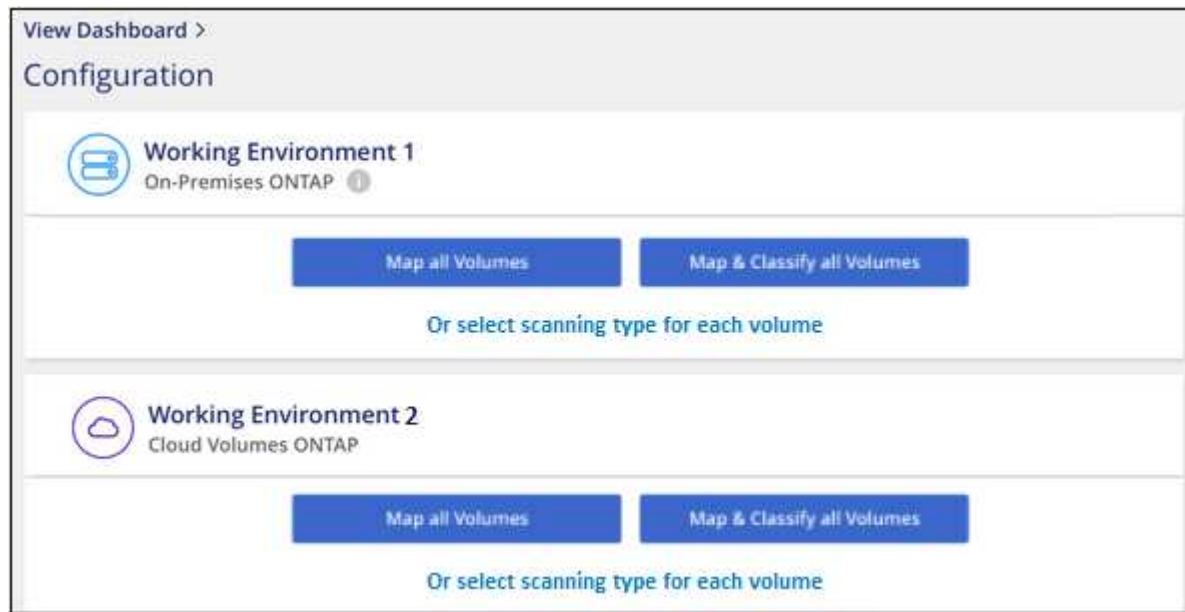
如果您正在掃描ONTAP 安裝在沒有網際網路連線的黑暗站台上的內部部署的資訊系統、您需要 "[在無法存取網際網路的同一個內部部署位置部署Cloud Data Sense](#)"。這也需要將Cloud Manager Connector部署在同一個內部部署位置。

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。

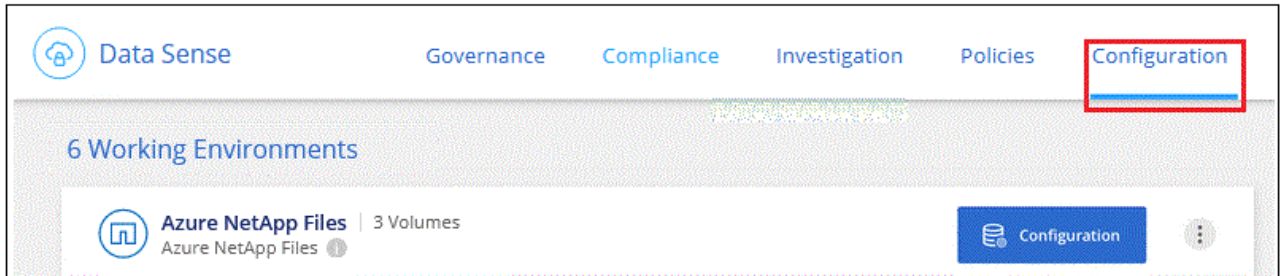
3. 確認下列連接埠已開放給Data Sense執行個體：

- 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。

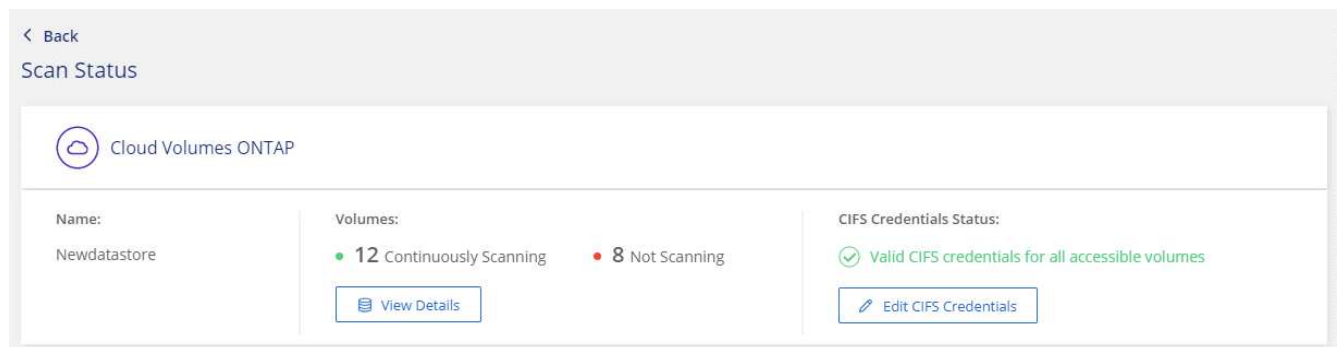
- 在Cloud Manager頂端、按一下* Data Sense *
- 單擊 * Configuration (配置) * 選項卡。



- 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。

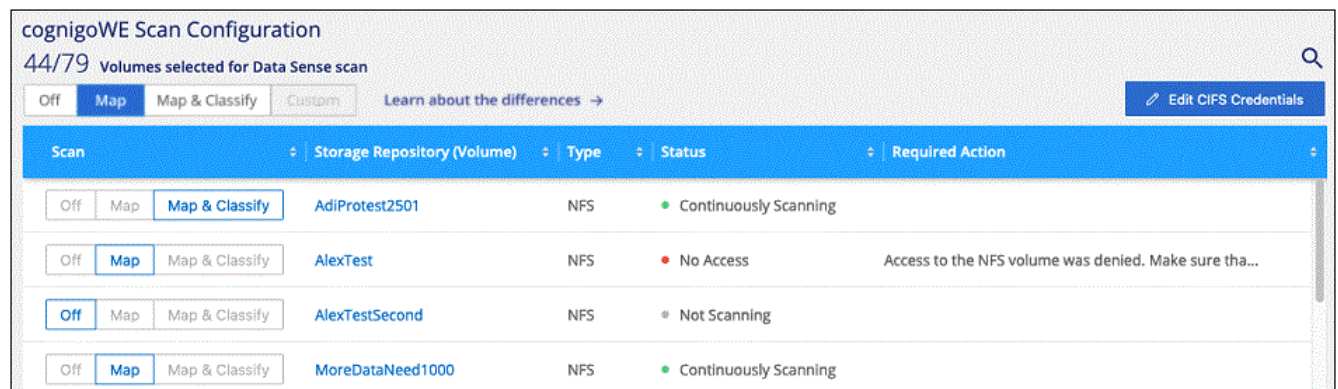
認證資料可以是唯讀的、但提供管理認證可確保Data Sense能夠讀取任何需要提升權限的資料。認證資料儲存在Cloud Data Sense執行個體上。

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。



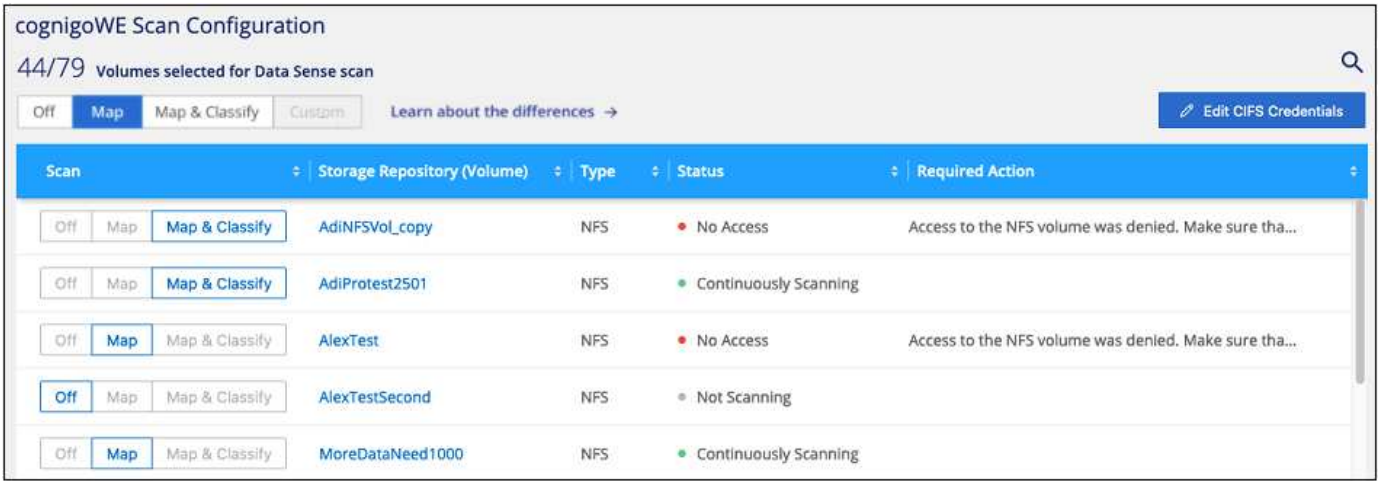
6. 在「_Configuration」頁面上、按一下「檢視詳細資料」以檢閱每個CIFS和NFS磁碟區的狀態、並修正任何錯誤。

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。



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 。



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

Enable Access to DP Volumes [Edit CIFS Credentials](#)

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：

- 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）」*。
 - 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

- 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

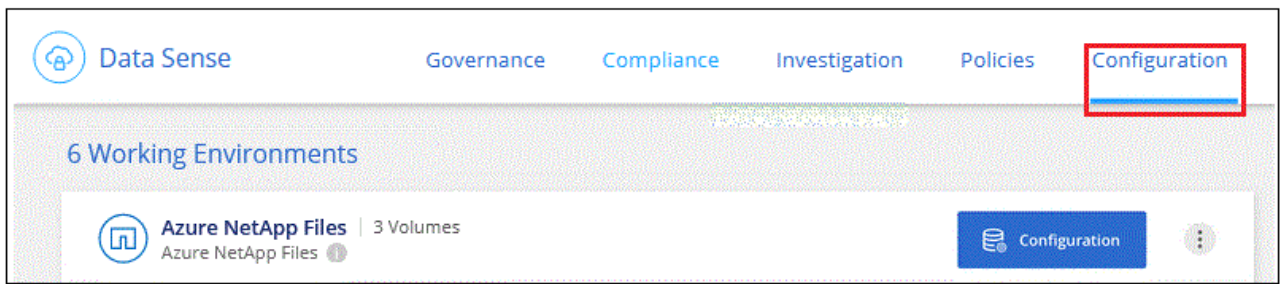
2. 確認下列連接埠已開放給Data Sense執行個體：

- 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。

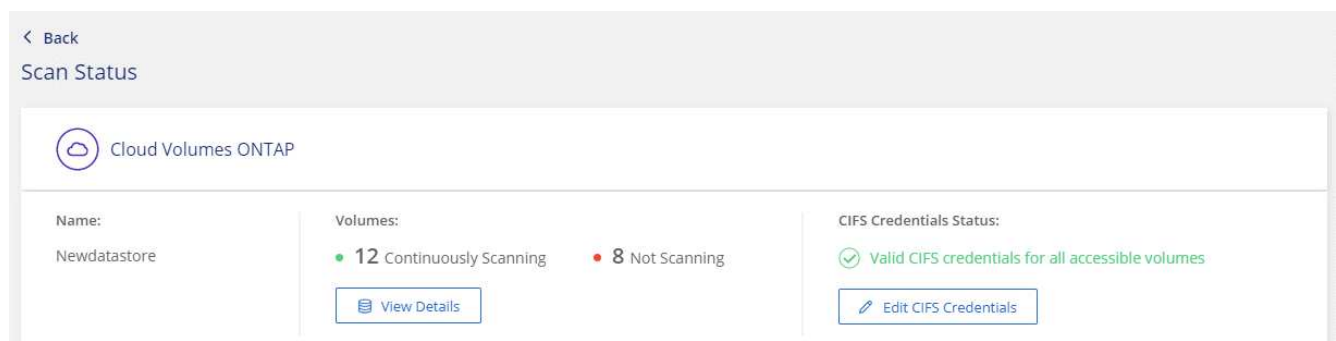
- a. 在Cloud Manager頂端、按一下* Data Sense *。
- b. 單擊 * Configuration （配置） * 選項卡。



- 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。

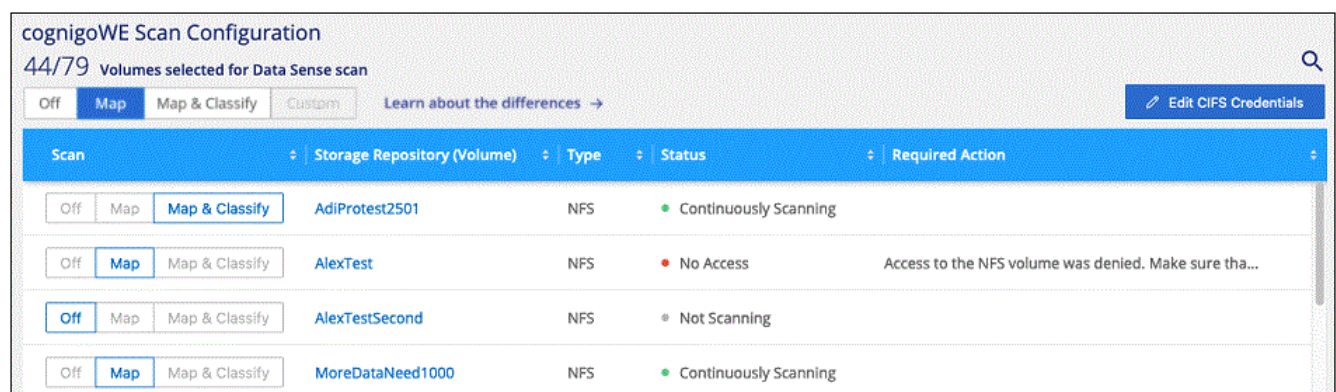
認證資料可以是唯讀的、但提供管理認證可確保Data Sense能夠讀取任何需要提升權限的資料。認證資料儲存在Cloud Data Sense執行個體上。

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。



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。

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 Sffile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。

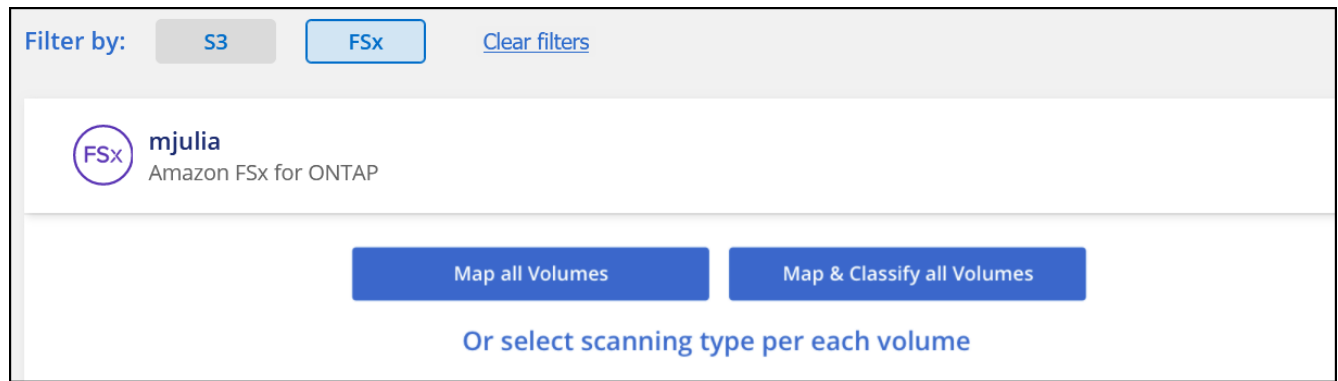
*附註：*掃描FSX Volume時、目前不支援在內部部署位置部署Cloud Data Sense。

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 Sf6 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
Off Map Map & Classify	jrmclone	NFS	● No Access	Check network connectivity between the Data Sense ...

2. 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。

3. 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。

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。

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 。

The screenshot displays the 'cognigoWE Scan Configuration' page. At the top, it indicates '44/79 Volumes selected for Data Sense scan'. Below this are tabs for 'Off', 'Map', 'Map & Classify', and 'Custom', along with a link to 'Learn about the differences'. A button for 'Edit CIFS Credentials' is also present. The main table lists several volumes: 'AdiNFSVol_copy', 'AdiProtest2501', 'AlexTest', 'AlexTestSecond', and 'MoreDataNeed1000'. Each row shows the current scan mode, the volume name, its type (NFS), its status (e.g., 'No Access', 'Continuously Scanning'), and a required action if there's an issue.

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*

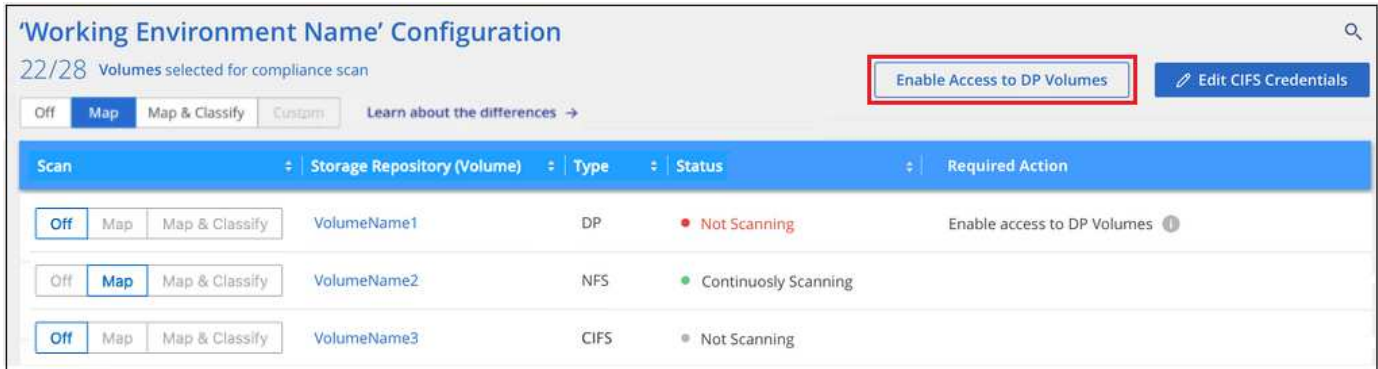


只有在標題區域中設定了*地圖*或*地圖與分類*設定之後、才會自動掃描新增至工作環境的磁碟區。在標題區域中設為*自訂*或*關閉*時、您必須在工作環境中新增的每個新磁碟區上啟動對應和/或完整掃描。

正在掃描資料保護磁碟區

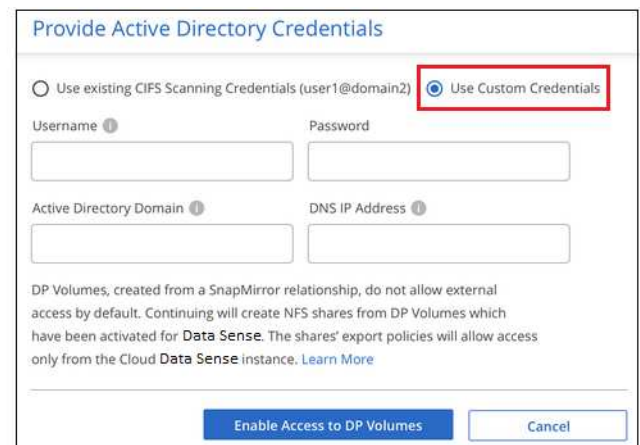
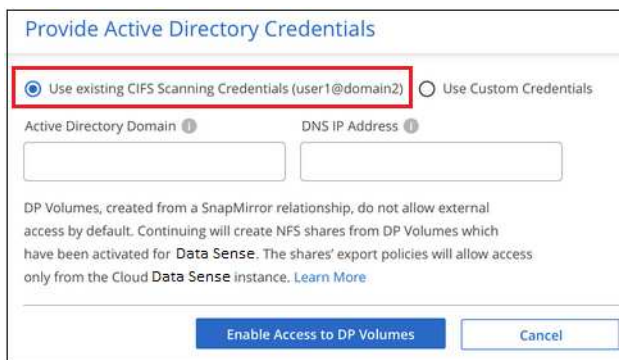
根據預設、不會掃描資料保護（DP）磁碟區、因為這些磁碟區並未對外公開、而且Cloud Data Sense無法存取它們。這些是來自FSXfor ONTAP Sfor the Sffile系統的SnapMirror作業目的地Volume。

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）。



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）」*。
 - 最初在來源FSXfor ONTAP the Sfor the Sffile系統中建立為NFS Volume的Volume將會啟用。
 - 最初在來源FSXfor ONTAP the Sffile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。

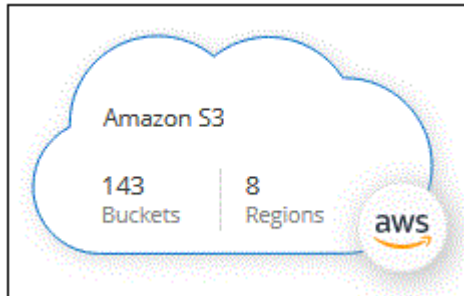
只要執行個體具備網際網路連線、就會自動升級至Data Sense軟體。

在S3工作環境中啟動Data Sense

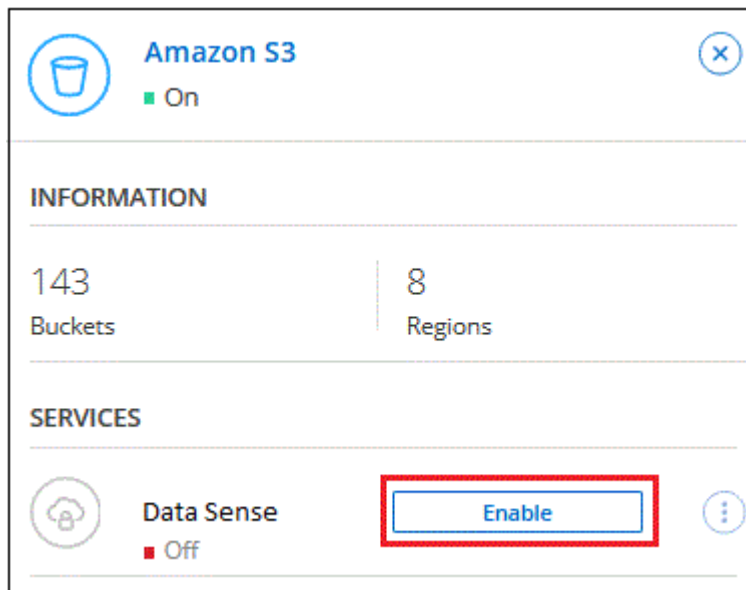
驗證先決條件之後、請在Amazon S3上啟用Cloud Data Sense。

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

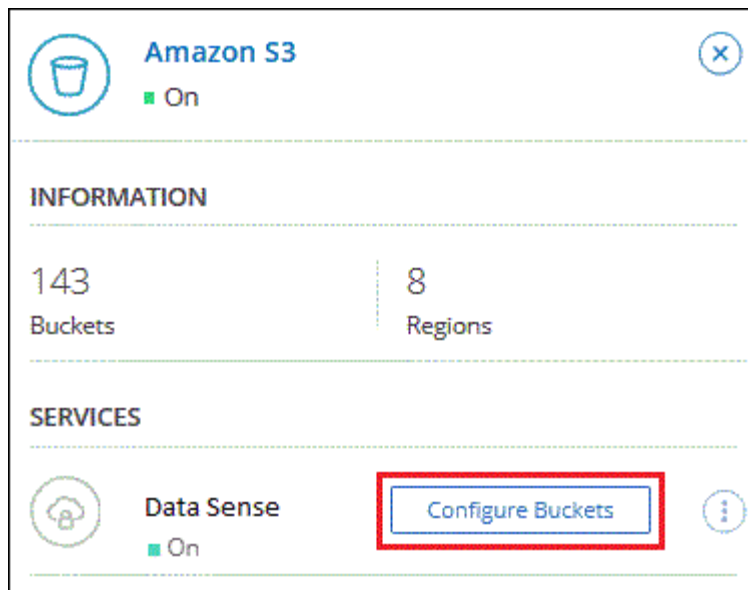
Cloud Manager在Amazon S3上啟用Cloud Data Sense之後、下一步是設定您要掃描的儲存區。

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。

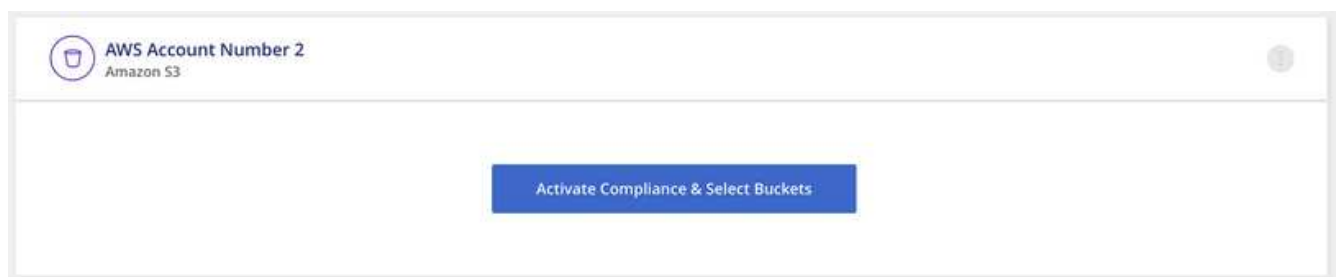
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

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"。

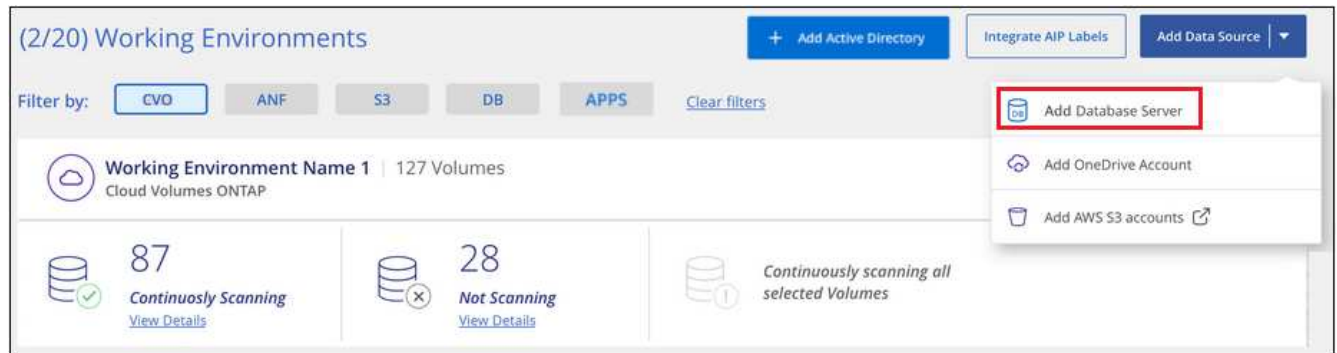
如果您要掃描安裝在無法存取網際網路的暗點中的資料庫架構、則必須執行 "在無法存取網際網路的同一個內部部署位置部署Cloud Data Sense"。這也需要將Cloud Manager Connector部署在同一個內部部署位置。

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

Port Service Name

Credentials

Username Password

資料庫會新增至工作環境清單。

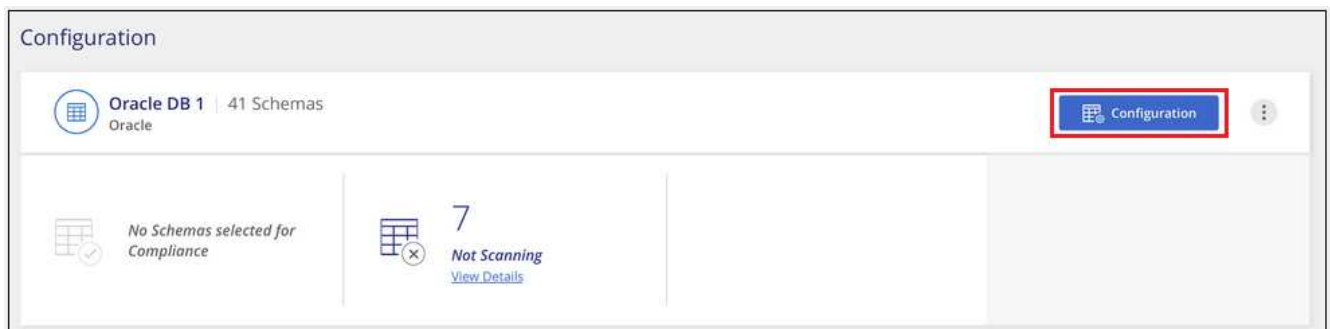
啟用及停用資料庫架構的法規遵循掃描

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		Edit Credentials	
Scan	Schema Name	Status	Required Action
<input 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	

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。

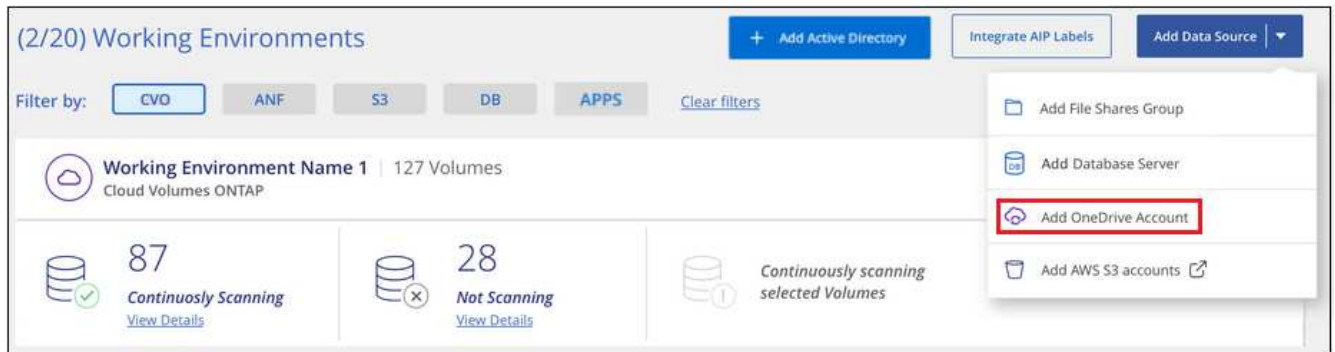
資料感測也可以是 "部署在沒有網際網路存取的內部部署位置"。不過、您必須提供網際網路存取功能、才能存取數個選定的端點、以掃描本機OneDrive檔案。"請參閱此處的必要端點清單"。

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

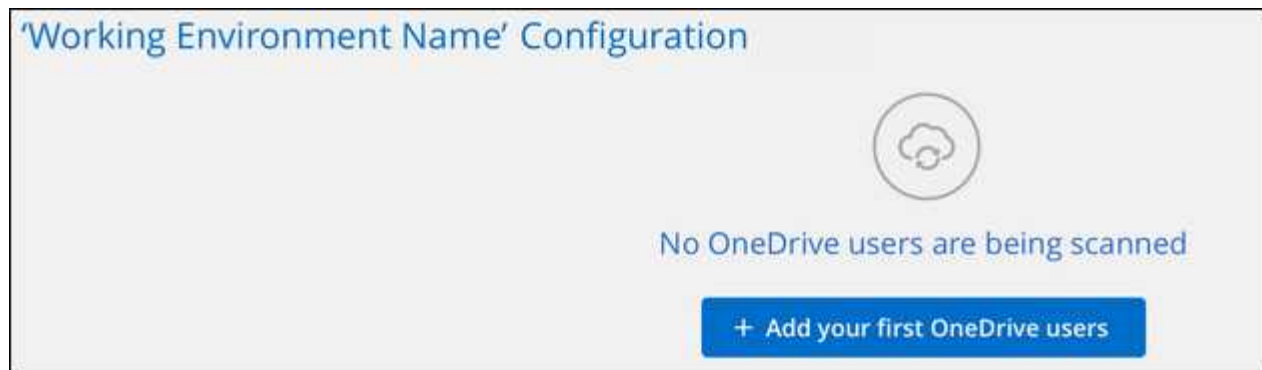
您可以新增個別OneDrive使用者或所有OneDrive使用者、以便Cloud Data Sense掃描他們的檔案。

步驟

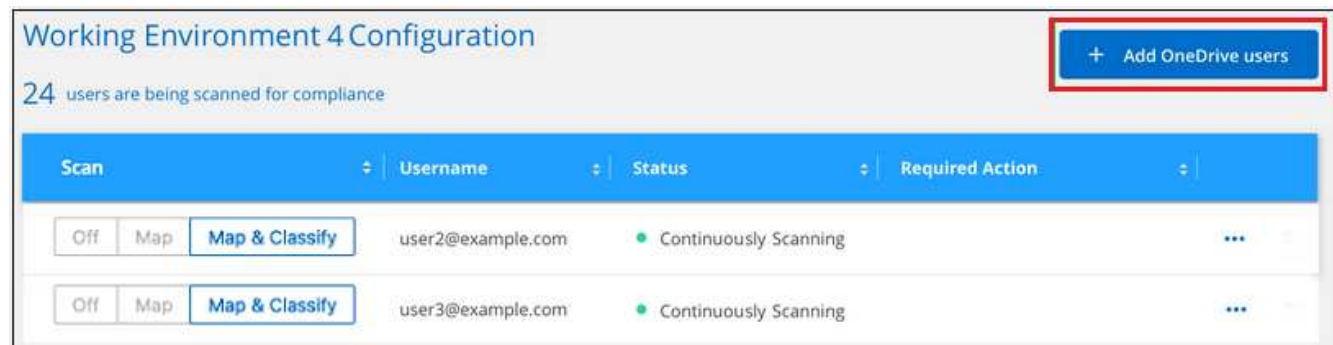
1. 在「_Configuration」頁面中、按一下OneDrive帳戶的*組態*按鈕。



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。

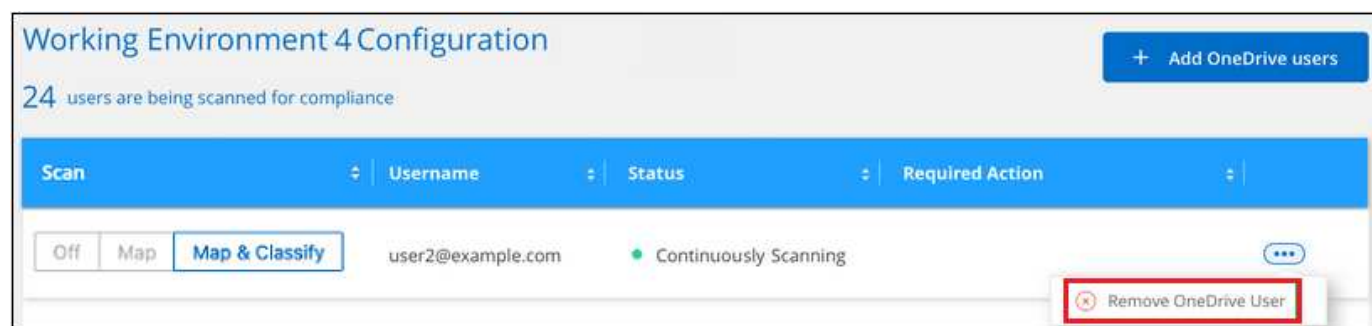
4. 啟用使用者檔案的純對應掃描、或對應與分類掃描。

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。

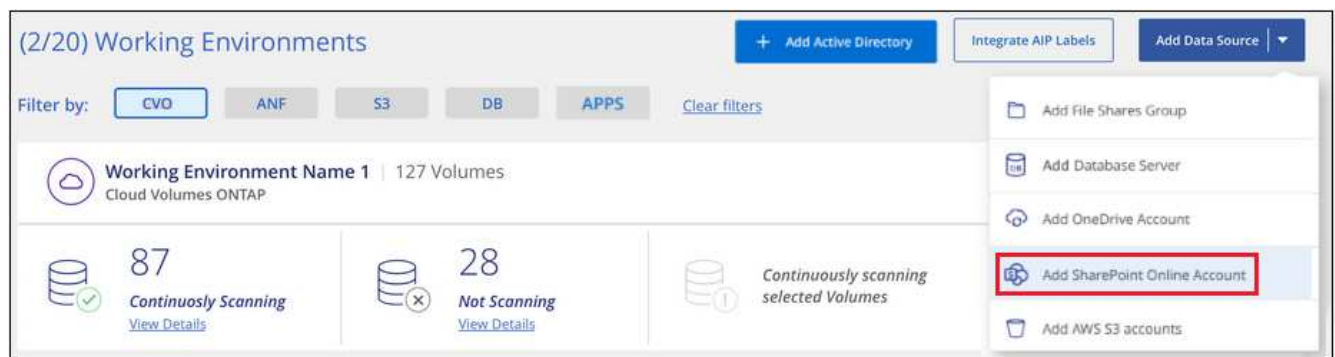
資料感測也可以是 "部署在沒有網際網路存取的內部部署位置"。不過、您必須提供網際網路存取功能、才能存取數個選定的端點、以掃描您的本機SharePoint檔案。"請參閱此處的必要端點清單"。

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

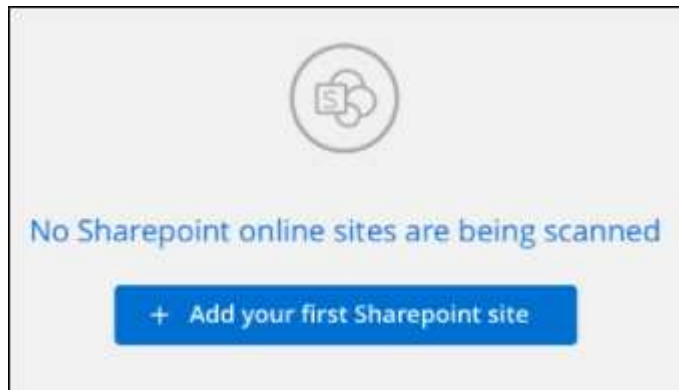
您可以新增個別SharePoint網站或帳戶中的所有SharePoint網站、以便Cloud Data Sense掃描相關檔案。

步驟

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



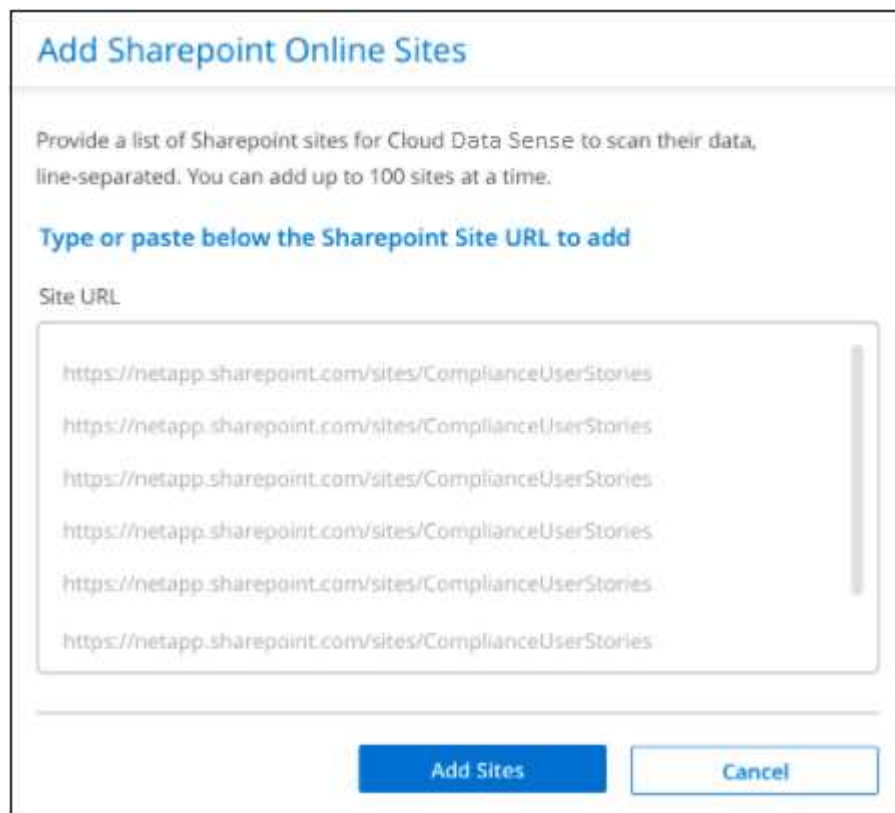
2. 如果這是第一次新增此SharePoint帳戶的網站、請按一下*「新增您的第一個SharePoint網站」*。



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）*。



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。

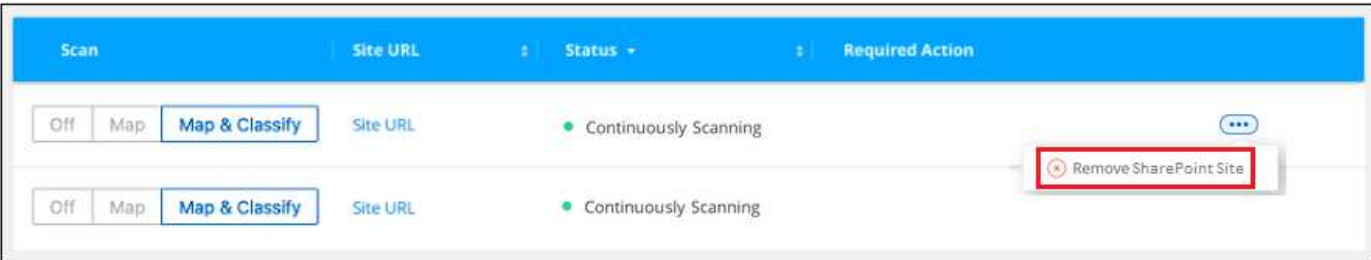
4. 在SharePoint網站的檔案上啟用純對應掃描、或對應及分類掃描。

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。



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"。

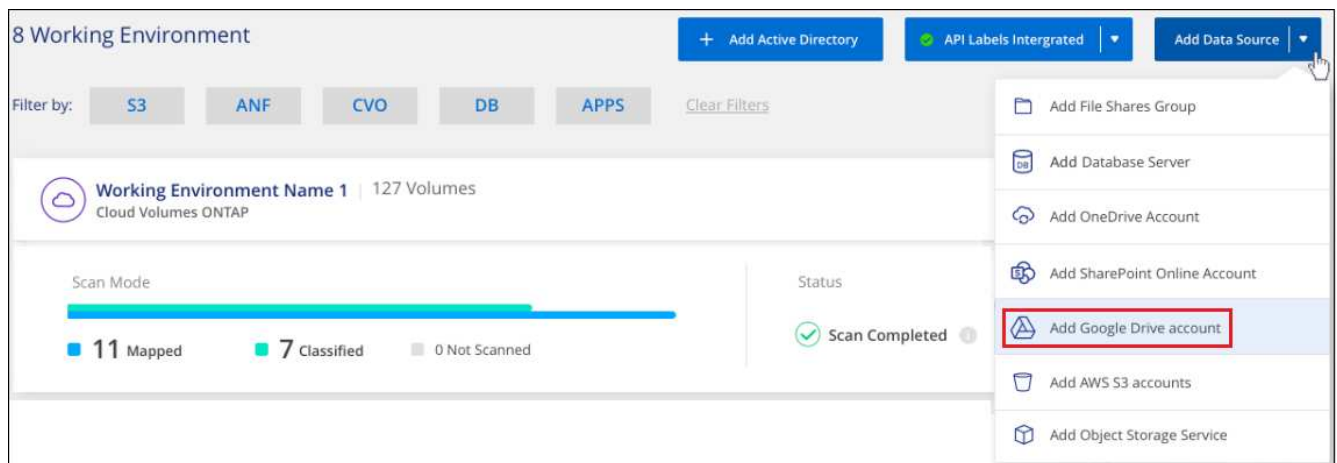
只要執行個體具備網際網路連線、就會自動升級至Data Sense軟體。

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。

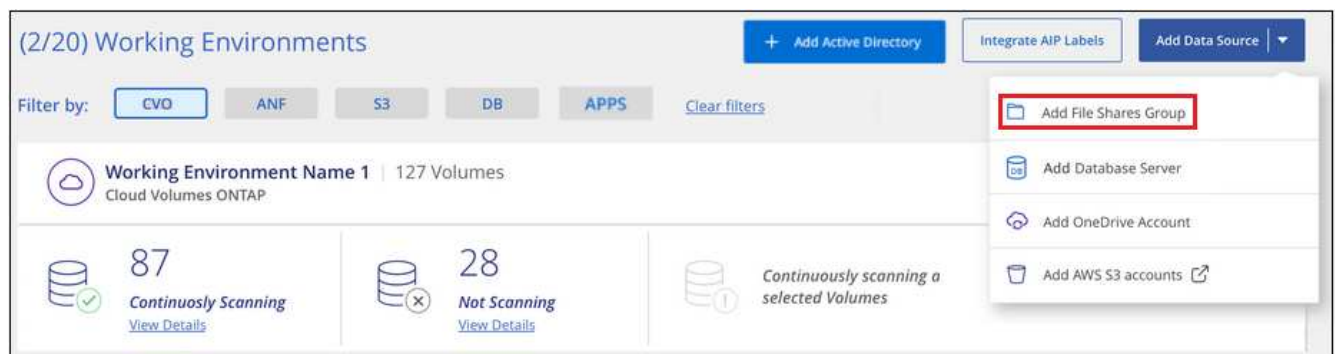
建立檔案共用的群組

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。

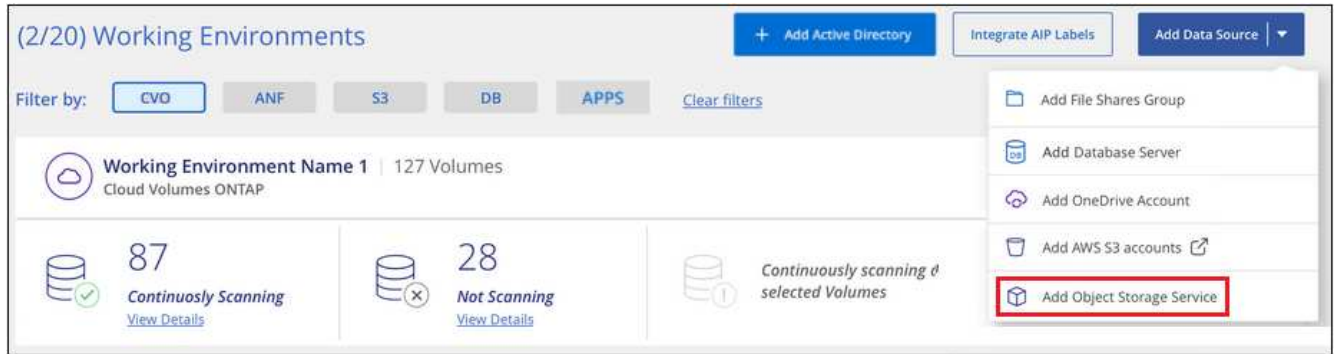
只要執行個體具備網際網路連線、就會自動升級至Data Sense軟體。

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="AJUKD0574NDJG86795"/>	<input type="password" value="....."/>

ContinueCancel

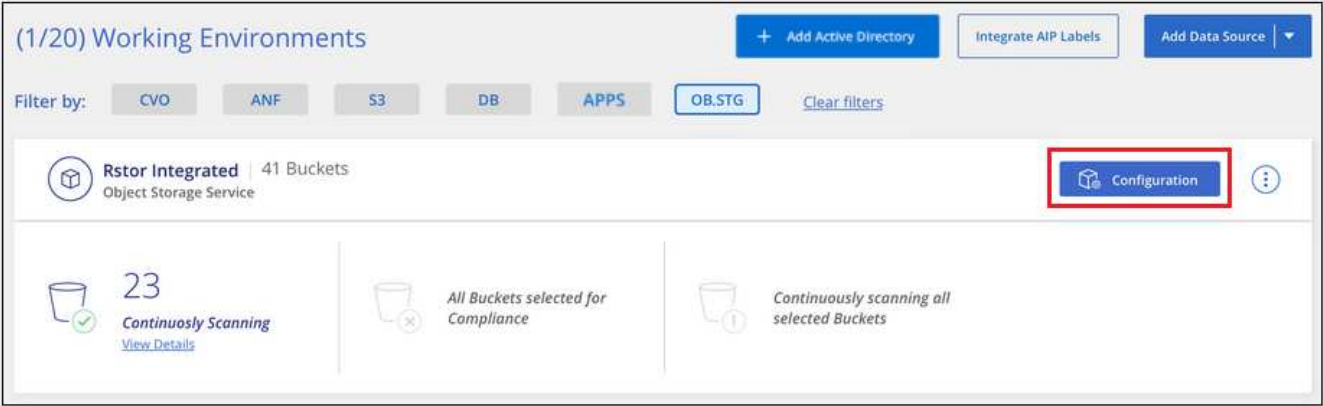
新的物件儲存服務會新增至工作環境清單。

啟用及停用物件儲存桶上的法規遵循掃描

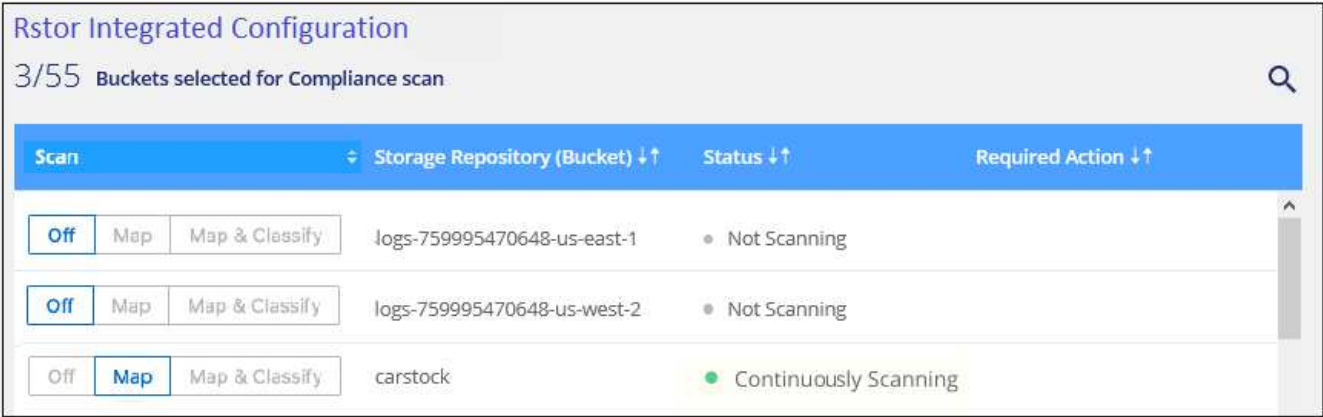
在物件儲存服務上啟用Cloud Data Sense之後、下一步是設定您要掃描的儲存區。Data Sense會探索這些儲存區、並在您所建立的工作環境中顯示這些儲存區。

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。



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。

將Active Directory與Cloud Data Sense整合

您可以將全域Active Directory與Cloud Data Sense整合、以增強Data Sense針對檔案擁有者及哪些使用者和群組有權存取您檔案的結果。

當您設定特定資料來源（如下所列）時、您需要輸入Active Directory認證資料、以便Data Sense能夠掃描CIFS磁碟區。這項整合提供資料認知功能、可讓檔案擁有者和這些資料來源中資料的權限詳細資料。針對這些資料來源輸入的Active Directory可能與您在此輸入的全域Active Directory認證不同。Data Sense會在所有整合式Active Directory中尋找使用者與權限詳細資料。

此整合可在Data意義上於下列位置提供額外資訊：

- 您可以使用「檔案擁有者」 **"篩選器"** 並在「調查」窗格中查看檔案中繼資料中的結果。與其包含SID（安全性識別碼）的檔案擁有者、會填入實際的使用者名稱。
- 您可以看到 **"完整檔案權限"** 按一下「檢視所有權限」按鈕即可檢視每個檔案。
- 在中 **"治理儀表板"**、「開啟權限」面板會顯示更多資料的詳細資料。



來自未知網域的本機使用者SID和SID不會轉譯為實際的使用者名稱。

支援的資料來源

Active Directory與Cloud Data Sense的整合可識別下列資料來源中的資料：

- 內部部署ONTAP 的作業系統
- Cloud Volumes ONTAP
- Azure NetApp Files
- FSX ONTAP
- 非NetApp CIFS檔案共用（非NFS檔案共用）

不支援從資料庫架構、OneDrive帳戶、SharePoint帳戶、Google雲端硬碟帳戶、Amazon S3帳戶、或使用簡易儲存服務（S3）傳輸協定的物件儲存設備。

連線至Active Directory伺服器

在您部署Data Sense並啟動資料來源掃描之後、就可以將Data Sense與Active Directory整合。Active Directory可使用DNS伺服器IP位址或LDAP伺服器IP位址來存取。

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

需求

- 您必須已為公司中的使用者設定Active Directory。
- 您必須擁有Active Directory的資訊：

- DNS伺服器IP位址或多個IP位址

或

LDAP伺服器IP位址或多個IP位址

- 存取伺服器的使用者名稱和密碼
 - 網域名稱（Active Directory名稱）
 - 無論您是否使用安全LDAP（LDAPS）
 - LDAP伺服器連接埠（LDAP一般為389、安全LDAP一般為636）
- Data Sense執行個體必須開啟下列連接埠、才能進行傳出通訊：

傳輸協定	連接埠	目的地	目的
TCP 與 UDP	389	Active Directory	LDAP
TCP	636	Active Directory	LDAP over SSL
TCP	3268/	Active Directory	全球目錄
TCP	3269	Active Directory	全球目錄（透過SSL）

步驟

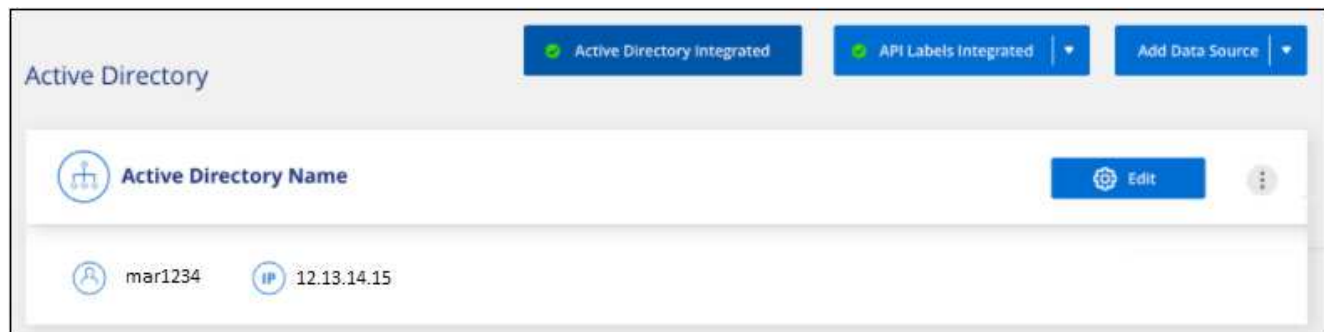
1. 在「Cloud Data Sense Configuration」（雲端資料感測組態）頁面中、按一下「* Add Active Directory」（



2. 在「連線至Active Directory」對話方塊中、輸入Active Directory詳細資料、然後按一下「連線」。


如有需要、您可以按一下*「Add IP*（新增IP*）」來新增多個IP位址。

Data Sense與Active Directory整合、並在「組態」頁面中新增一節。



管理Active Directory整合

如果您需要修改Active Directory整合中的任何值、請按一下*編輯*按鈕進行變更。

如果不再需要整合、您也可以按一下來刪除整合  按鈕、然後*移除Active Directory*。

設定Cloud Data Sense授權

Cloud Data Sense在Cloud Manager工作區中掃描的前1 TB資料是免費的。NetApp的BYOL授權或雲端供應商市場的Cloud Manager訂閱、必須在該點之後繼續掃描資料。

在閱讀更多內容之前、請先提供幾個附註：

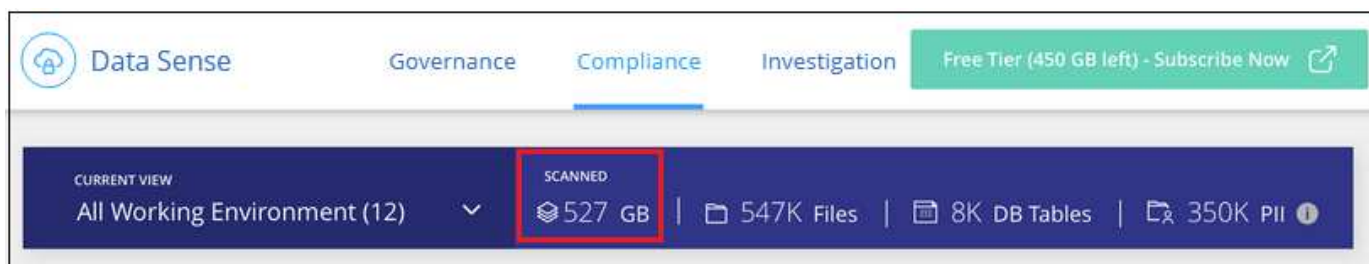
- 如果您已在雲端供應商的市場訂閱Cloud Manager隨用隨付（PAYGO）、您也會自動訂閱Cloud Data Sense。您不需要再次訂閱。
- Cloud Data Sense自帶授權（BYOL）是一個_浮_點型授權、您可以在您計畫掃描的工作環境和資料來源中使用。您會在Digital Wallet中看到使用中的訂閱內容。

["深入瞭解Cloud Data Sense的授權與成本"](#)。

使用Cloud Data Sense PAYGO訂閱

雲端供應商市場的隨用隨付訂閱可讓您授權使用Cloud Volumes ONTAP 多方面的系統及雲端資料服務、例如Cloud Data Sense。

您可以隨時訂閱、而且在資料量超過 1 TB 之前、將不會向您收取費用。您可以隨時從Data Sense儀表板查看要掃描的資料總量。而且「立即訂閱」按鈕可讓您在準備就緒時輕鬆訂閱。



這些步驟必須由擁有 *Account Admin* 角色的使用者完成。

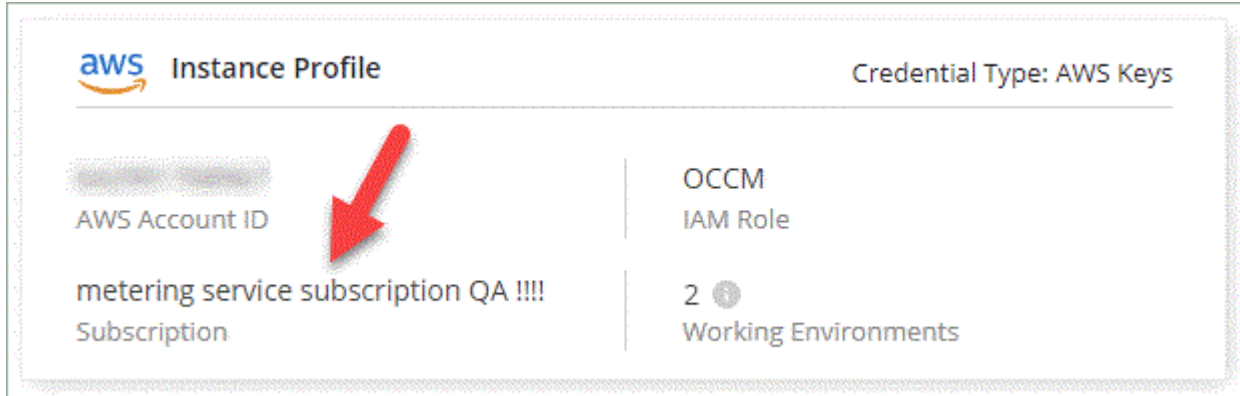
1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 * 認證 * 。



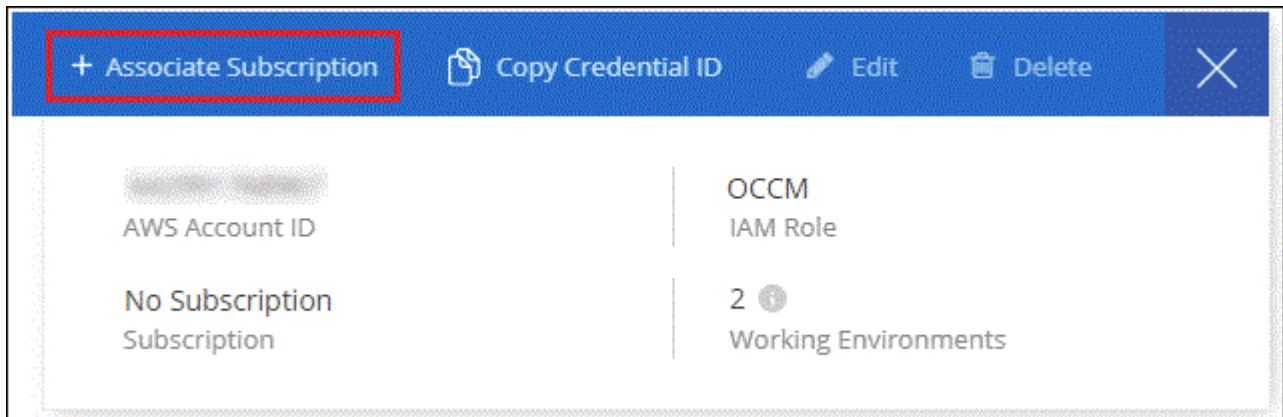
2. 尋找AWS執行個體設定檔、Azure託管服務身分識別或Google Project的認證資料。

訂閱必須新增至執行個體設定檔、託管服務識別或Google Project。否則無法充電。

如果您已經訂閱（如下所示）、就表示您已完成設定、沒有其他需要做的事。



3. 如果您尚未訂閱、請將游標移至認證上方、按一下動作功能表、然後按一下*建立訂閱關聯*。



4. 選取現有的訂閱、然後按一下「經銷」、或按一下「新增訂閱」、然後依照步驟進行。

下列影片說明如何建立關聯 "AWS Marketplace" 訂閱AWS訂閱：

► https://docs.netapp.com/zh-tw/cloud-manager-data-sense//media/video_subscribing_aws.mp4 (video)

下列影片說明如何建立關聯 "Azure Marketplace" 訂閱Azure：

► https://docs.netapp.com/zh-tw/cloud-manager-data-sense//media/video_subscribing_azure.mp4 (video)

下列影片說明如何建立關聯 "GCP 市場" 訂購GCP：

► https://docs.netapp.com/zh-tw/cloud-manager-data-sense//media/video_subscribing_gcp.mp4 (video)

使用Cloud Data Sense BYOL授權

NetApp自帶授權、提供1年、2年或3年期限。BYOL * Cloud Data Sense *授權是浮點型授權、可讓您的*全部*工作環境和資料來源共享總容量、讓初始授權和續約更輕鬆。

如果您沒有Cloud Data Sense授權、請聯絡我們以購買：

- mailto : ng-contact-data-sense@netapp.com ? Subject =授權[傳送電子郵件以購買授權]。
- 按一下Cloud Manager右下角的聊天圖示以申請授權。

或者、如果Cloud Volumes ONTAP 您擁有不使用的未指派節點型支援、您可以將其轉換成具有相同金額等同和相同到期日的Cloud Data Sense授權。"如需詳細資料、請前往此處"。

您可以使用Cloud Manager中的「Digital Wallet」頁面來管理Cloud Data Sense BYOL授權。您可以新增授權並更新現有授權。

取得Cloud Data Sense授權檔案

購買Cloud Data Sense授權後、您可以在Cloud Manager中輸入Cloud Data Sense序號和nss/帳戶、或上傳NLF授權檔案、以啟動授權。下列步驟說明如果您打算使用NLF授權檔案、該如何取得該檔案。

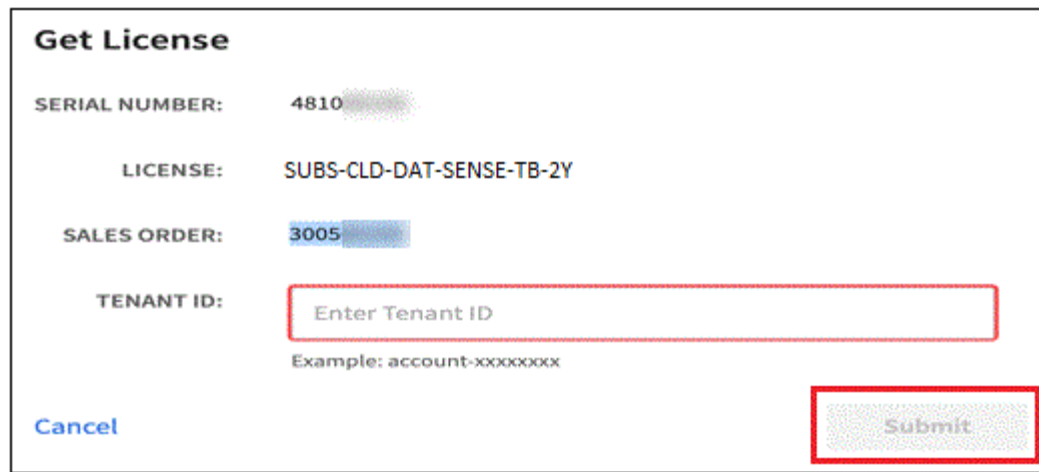
如果您已在內部部署站台的主機上部署Cloud Data Sense、但該站台無法存取網際網路、則必須從連線網際網路的系統取得授權檔案。無法使用序號和NSS帳戶啟動使用許可、進行暗色站台安裝。

步驟

1. 登入 "[NetApp 支援網站](#)" 然後按一下*系統>軟體授權*。
2. 輸入您的Cloud Data Sense授權序號。

Serial #	Cluster SN	License Name	License Key	Host ID	Value	End Date
4810		SUBS-CLD-DAT-SENSE-TB-2Y	Get NetApp License File		100	12/31/9998

3. 在*授權金鑰*下、按一下*取得NetApp授權檔案*。
4. 輸入您的Cloud Manager帳戶ID（在支援網站上稱為「租戶ID」）、然後按一下*提交*下載授權檔案。



Get License

SERIAL NUMBER: 4810

LICENSE: SUBS-CLD-DAT-SENSE-TB-2Y

SALES ORDER: 3005

TENANT ID:

Example: account-xxxxxxx

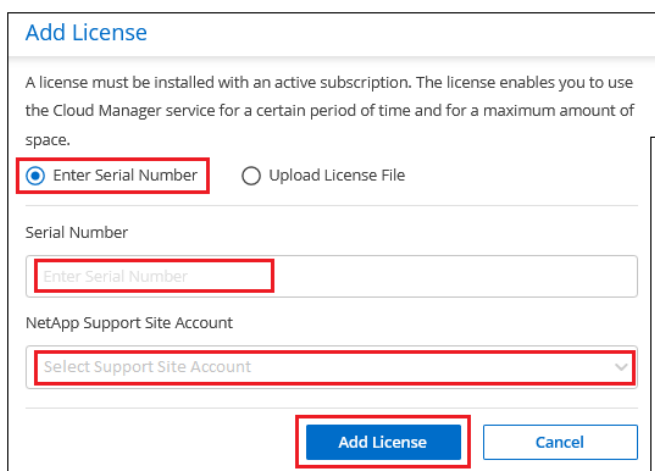
您可以從Cloud Manager頂端選取* Account*下拉式清單、然後按一下帳戶旁的* Manage Account*、即可找到Cloud Manager帳戶ID。您的帳戶ID位於「總覽」索引標籤。

將Cloud Data Sense BYOL授權新增至您的帳戶

購買Cloud Manager帳戶的Cloud Data Sense授權後、您必須將授權新增至Cloud Manager、才能使用Data Sense服務。

步驟

- 按一下「所有服務>數位錢包>資料服務授權」。
- 按一下「* 新增授權 *」。
- 在_新增授權_對話方塊中、輸入授權資訊、然後按一下*新增授權*：
 - 如果您擁有Data Sense授權序號並知道您的nss帳戶、請選取* Enter Serial Number*（輸入序號*）選項、然後輸入該資訊。
 - 如果您的NetApp支援網站帳戶無法從下拉式清單取得、["將新增至Cloud Manager的NSS帳戶"](#)。
 - 如果您有Data Sense授權檔案（安裝在暗處時需要）、請選取*上傳授權檔案*選項、然後依照提示附加檔案。



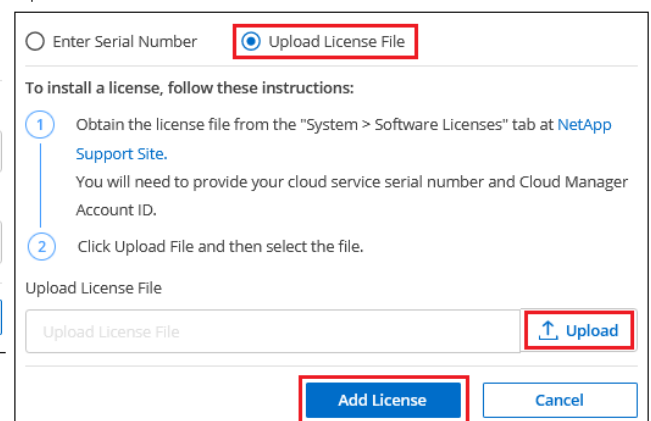
Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

☒ Enter Serial Number ☐ Upload License File

Serial Number

NetApp Support Site Account



☐ Enter Serial Number ☒ Upload License File

To install a license, follow these instructions:

- Obtain the license file from the "System > Software Licenses" tab at [NetApp Support Site](#). You will need to provide your cloud service serial number and Cloud Manager Account ID.
- Click Upload File and then select the file.

Upload License File

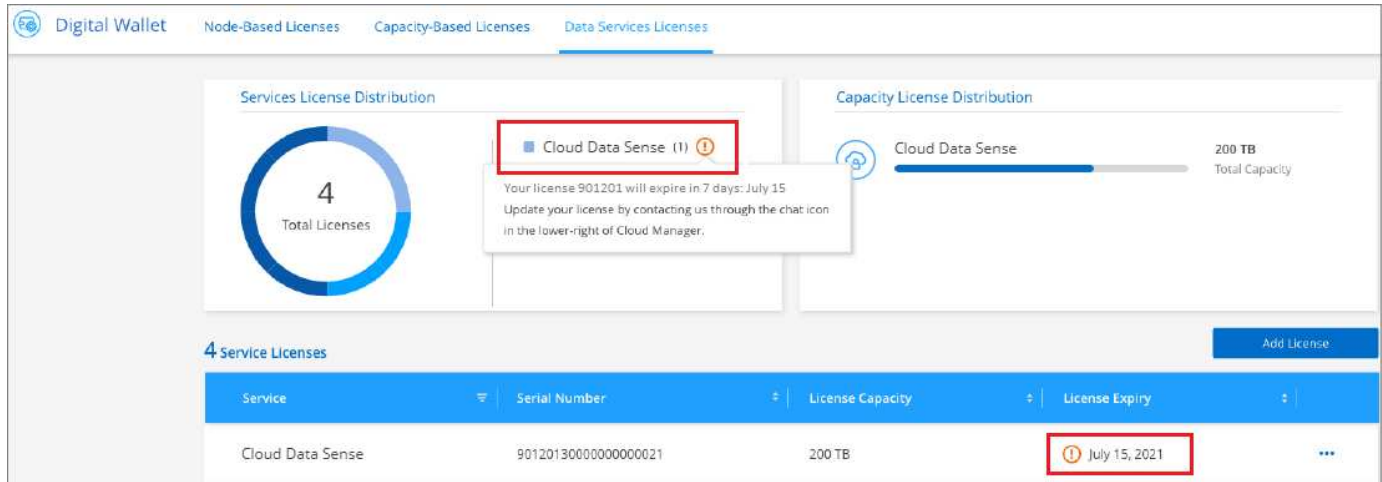
Cloud Manager會新增授權、讓您的Cloud Data Sense服務處於作用中狀態。

更新Cloud Data Sense BYOL授權

如果您的授權期限即將到期、或您的授權容量已達到上限、您將會收到Cloud Data傳感通知。



此狀態也會顯示在數位錢包中。



您可以在Cloud Data Sense授權到期之前更新、以確保存取掃描資料的能力不會中斷。

步驟

1. 按一下Cloud Manager右下角的聊天圖示、即可針對特定序號、要求將您的術語或額外容量擴充至Cloud Data Sense授權。您也可以傳送電子郵件至mailto: ng-contact-data-sense@netapp.com@Subject=Licensing[寄送電子郵件要求更新授權]。

在您支付授權費用並向NetApp支援網站註冊之後、Cloud Manager會自動更新Digital Wallet中的授權、而Data Services授權頁面將會在5到10分鐘內反映變更。

2. 如果Cloud Manager無法自動更新授權（例如、安裝在暗點）、則您需要手動上傳授權檔案。
 - a. 您可以 [從NetApp支援網站取得授權檔案](#)。
 - b. 在「資料服務授權」索引標籤的「數位錢包」頁面上、按一下 ... 如需您要更新的服務序號、請按一下*更新授權*。

4 Service Licenses				Add License
Service	Serial Number	License Capacity	License Expiry	
Cloud Tiering	90120130000000000021	300 TB	January 1, 2022	...
Cloud Data Sense	90120130000000000022	200 TB	January 1, 2022	<div> Update License Remove License </div>

c. 在「更新授權」頁面上傳授權檔案、然後按一下「更新授權」。

Cloud Manager會更新授權、讓您的Cloud Data Sense服務持續運作。

BYOL 授權考量

使用Cloud Data Sense BYOL授權時、當您掃描的所有資料大小接近容量限制或接近授權到期日時、Cloud Manager會在Data Sense UI和Digital Wallet UI中顯示警告。您會收到下列警告：

- 當您正在掃描的資料量達到授權容量的80%時、當您達到限制時、也會再次顯示
- 授權到期前 30 天、授權到期後再一次

當您看到這些警告時、請使用Cloud Manager介面右下角的聊天圖示來續約授權。

如果授權過期、Data Sense會繼續執行、但儀表板的存取會遭到封鎖、因此您無法檢視任何掃描資料的相關資訊。如果您想減少所掃描的磁碟區數量、使容量使用量可能低於授權限制、則只有「_Configuration」頁面可用。

續約BYOL授權之後、Cloud Manager會自動更新Digital Wallet中的授權、並提供所有儀表板的完整存取權限。如果Cloud Manager無法透過安全的網際網路連線存取授權檔案（例如、安裝在暗點）、您可以自行取得該檔案、然後手動將其上傳至Cloud Manager。如需相關指示、請參閱 [如何更新Cloud Data Sense授權](#)。



如果您使用的帳戶同時擁有BYOL授權和PAYGO訂閱、則當BYOL授權到期時、Data Sense _will 不會移轉至PAYGO訂閱。您必須續約BYOL授權。

有關Cloud Data Sense的常見問題集

如果您只是想要快速回答問題、這個常見問題集就能幫上忙。

雲端資料感應服務

下列問題可讓您大致瞭解Cloud Data Sense。

什麼是雲端資料意義？

Cloud Data Sense是一款雲端產品、採用人工智慧（AI）導向技術、可協助您瞭解資料內容、並識別儲存系統中的敏感資料。這些系統可以是您新增至Cloud Manager畫版的工作環境、以及Data Sense可透過網路存取的許多類型資料來源。 [請參閱下列完整清單](#)。

Cloud Data Sense提供預先定義的參數（例如敏感資訊類型和類別）、以因應資料隱私和敏感度的新資料法規遵循要求、例如GDPR、CCPA、HIPAA等。

為什麼我應該使用**Cloud Data Sense**？

Cloud Data Sense可協助您運用資料、協助您：

- 遵守資料法規遵循與隱私權法規。
- 將資料從舊系統移轉至雲端。
- 遵守資料保留政策。
- 根據 GDPR、CCPA、HIPAA 及其他資料隱私法規的要求、輕鬆找出特定資料並進行報告、以因應資料主題。

Cloud Data Sense的常見使用案例為何？

- 識別個人識別資訊（PII）。
- 根據 GDPR 和 CCPA 隱私權法規的要求、識別廣泛的敏感資訊。
- 遵守新的及即將推出的資料隱私權法規。

["深入瞭解Cloud Data Sense的使用案例"](#)。

雲端資料感測如何運作？

Cloud Data Sense可在Cloud Manager系統和儲存系統旁部署另一層人工智慧。然後掃描磁碟區、儲存區、資料庫及其他儲存帳戶上的資料、並為找到的資料洞見建立索引。Data Sense運用人工智慧和自然語言處理、而非以一般運算式和模式比對為基礎的替代解決方案。Cloud Data Sense使用AI來提供資料的關聯式瞭解、以利準確偵測和分類。它是由AI驅動、因為它是專為現代資料類型和規模所設計。它也瞭解資料內容、以便提供強大、準確的探索和分類功能。

["深入瞭解Cloud Data Sense的運作方式"](#)。

Cloud Data Sense多久掃描一次我的資料？

資料經常變更、因此Cloud Data Sense可持續掃描資料、不會對資料造成任何影響。雖然初次掃描資料可能需要較長時間、但後續掃描只會掃描遞增變更、如此可縮短系統掃描時間。

["瞭解掃描的運作方式"](#)。

資料掃描對儲存系統和資料的影響微乎其微。不過、如果您擔心影響極小、您可以設定「Data Sense」（資料感測）來執行「Slow」（慢速）掃描。["瞭解如何降低掃描速度"](#)。

Cloud Data Sense支援哪些部署模式？

Cloud Data Sense通常是使用SaaS模式來部署、在這種模式中、服務是透過Cloud Manager介面來啟用。Cloud Data Sense可部署在幾乎任何位置的系統上進行掃描和報告、包括內部部署、雲端和混合式環境。對於安全的安裝、Cloud Manager和Cloud Data Sense可部署在「暗站」模式中、此模式是以套件形式安裝在內部部署環境中、不需要外部網路連線。

是否有人能存取在我的瀏覽器和**Data Sense**之間傳送的私有資料？

不可以在瀏覽器與Data Sense執行個體之間傳送的私有資料、會以端點對端點加密加以保護、這表示NetApp與第三方無法讀取。除非您申請並核准存取、否則Data Sense不會與NetApp分享任何資料或結果。

Cloud Data Sense是否提供報告？

是的。Cloud Data Sense所提供的資訊可能與貴組織中的其他利害關係人有關、因此我們可讓您產生報告、以分享這些見解。下列報告適用於Data Sense：

隱私權風險評估報告

提供資料的隱私見解和隱私權風險分數。 ["深入瞭解"](#)。

資料主旨存取要求報告

可讓您擷取包含資料主旨特定名稱或個人識別碼相關資訊之所有檔案的報告。 ["深入瞭解"](#)。

PCI DSS 報告

協助您辨識信用卡資訊在檔案之間的發佈情形。 ["深入瞭解"](#)。

HIPAA 報告

協助您識別檔案之間的健全狀況資訊發佈。 ["深入瞭解"](#)。

資料對應報告

提供有關工作環境中檔案大小和數量的資訊。這包括使用容量、資料存留時間、資料大小和檔案類型。 ["深入瞭解"](#)。

報告特定資訊類型

報告中包含有關已識別檔案的詳細資料、這些檔案包含個人資料和敏感個人資料。您也可以查看依類別和檔案類型分類的檔案。 ["深入瞭解"](#)。

掃描效能是否有所差異？

掃描效能可能會因網路頻寬和環境中的平均檔案大小而有所不同。也可能取決於主機系統的大小特性（無論是雲端或內部部署）。請參閱 ["Cloud Data Sense執行個體"](#) 和 ["部署Cloud Data Sense"](#) 以取得更多資訊。

一開始新增資料來源時、您也可以選擇只執行「對應」掃描、而非完整的「分類」掃描。您可以很快在資料來源上完成對應、因為它不會存取檔案來查看內部資料。 ["瞭解對應與分類掃描之間的差異。"](#)

如何啟用雲端資料感測？

首先、您需要在Cloud Manager中部署Cloud Data Sense執行個體。執行個體之後、您可以從* Data Sense *標籤或選取特定工作環境、在現有的工作環境、資料庫及其他資料來源上啟用服務。

["瞭解如何開始使用"](#)。



在資料來源上啟動Cloud Data Sense會立即進行初始掃描。掃描結果會在不久後顯示。

如何停用**Cloud Data Sense**？

您可以從「Data Sense組態」頁面、停用「Cloud Data Sense」、從掃描個別工作環境、資料庫、檔案共用群

組、OneDrive帳戶或SharePoint帳戶。

["深入瞭解"](#)。



若要完全移除Cloud Data Sense執行個體、您可以從雲端供應商的入口網站或內部位置手動移除Data Sense執行個體。

如果在您的功能區上啟用資料分層、會發生什麼情況**ONTAP**？

您可能想要在ONTAP 將冷資料分層儲存至物件儲存的功能區系統上啟用Cloud Data Sense。如果啟用資料分層、Data Sense會掃描磁碟上的所有資料、並將冷資料階層化至物件儲存設備。

法規遵循掃描不會將冷資料加熱、而是維持冷態並分層至物件儲存設備。

Cloud Data Sense可以傳送通知給我的組織嗎？

是的。搭配原則功能、您可以在原則傳回結果時、將電子郵件警示傳送給Cloud Manager使用者（每日、每週或每月）、以便取得通知來保護資料。深入瞭解 ["原則"](#)。

您也可以從「治理」頁面和「調查」頁面下載狀態報告、以便在組織內部分享。

我可以根據組織的需求自訂服務嗎？

Cloud Data Sense可為您的資料提供隨裝即用的洞見。您可以擷取這些洞見、並將其用於貴組織的需求。

此外、您也可以使用* Data Fusion Seri*功能、根據您正在掃描之資料庫中特定欄位的條件、讓Data Sense掃描您的所有資料、基本上讓您自行建立自訂的個人資料類型。

["深入瞭解"](#)。

Cloud Data Sense是否能搭配我檔案內嵌的**AIP**標籤運作？

是的。您可以在Cloud Data Sense正在掃描的檔案中管理AIP標籤（若已訂閱） ["Azure資訊保護（AIP）"](#)。您可以檢視已指派給檔案的標籤、新增標籤至檔案、以及變更現有的標籤。

["深入瞭解"](#)。

我可以將**Cloud Data Sense**資訊限制在特定使用者身上嗎？

是的、Cloud Data Sense與Cloud Manager完全整合。Cloud Manager 使用者只能根據其工作區權限、查看其符合檢視資格的工作環境資訊。

此外、如果您想要讓特定使用者在不管理「資料感應」設定的情況下、只檢視「資料感應」掃描結果、您可以將「*Cloud Compliance Viewer*」角色指派給這些使用者。

["深入瞭解"](#)。

支援哪些雲端供應商？

Cloud Data Sense是Cloud Manager的一部分、可支援AWS、Azure和GCP。如此一來、您的組織便能在不同的雲端供應商之間統一化隱私權可見度。

來源系統和資料類型的類型

下列問題與可掃描的儲存設備類型及掃描的資料類型有關。

哪些資料來源可以透過**Data Sense**進行掃描？

Cloud Data Sense可掃描已新增至Cloud Manager畫版的工作環境中的資料、以及Data Sense可透過網路存取的多種資料來源。

工作環境：

- （部署於AWS、Azure或GCP）Cloud Volumes ONTAP
- 內部部署 ONTAP 的叢集
- Azure NetApp Files
- Amazon FSx for ONTAP
- Amazon S3

資料來源：

- 非NetApp檔案共用
- 物件儲存（使用S3傳輸協定）
- 資料庫（Amazon RDS、MongoDB、MySQL、Oracle、PostgreSQL、SAP HANA、SQL Server）
- OneDrive 帳戶
- SharePoint帳戶
- Google雲端硬碟帳戶

Data Sense支援NFS 3.x、4.0及4.1版、以及CIFS 1.x、2.0、2.1及3.0版。

如果我在沒有網際網路存取的網站上安裝**Data Sense**、我可以掃描哪些資料來源？

Data Sense只能掃描內部部署站台本機資料來源的資料。此時、Data Sense可掃描「暗」站台中的下列本機資料來源：

- 內部部署ONTAP 的作業系統
- 資料庫架構
- 非NetApp NFS或CIFS檔案共用
- 使用簡易儲存服務（S3）傳輸協定的物件儲存設備

支援哪些檔案類型？

Cloud Data Sense會掃描所有檔案以取得類別和中繼資料深入資訊、並在儀表板的「檔案類型」區段中顯示所有檔案類型。

當Data Sense偵測到個人識別資訊（PII）、或執行DSAR搜尋時、僅支援下列檔案格式：

Cloud Data Sense擷取哪些類型的資料和中繼資料？

CSV、.dcm、.dicom、.dDOC、.DOCX、.Json、.PDF、.PPTX、.RTF、.TXT、.XLS、.XLSX、文件、工作表及Slides +

Cloud Data Sense可讓您對資料來源執行一般的「對應」掃描或完整的「分類」掃描。對應只提供資料的高層級總覽、而分類則提供資料的深度層級掃描。您可以很快在資料來源上完成對應、因為它不會存取檔案來查看內部資料。

- 資料對應掃描：

Data Sense只會掃描中繼資料。這對整體資料管理與治理、快速專案範圍規劃、大型產業和優先順序都很有幫助。資料對應是以中繼資料為基礎、視為*快速*掃描。

快速掃描之後、您可以產生資料對應報告。本報告概述儲存在企業資料來源中的資料、協助您做出有關資源使用率、移轉、備份、安全性及法規遵循程序的決策。

- 資料分類（深度）掃描。

在客戶的整個環境中、使用標準傳輸協定和唯讀權限進行資料感應掃描。針對敏感的業務相關資料、私有資訊及勒索軟體相關問題、會開啟並掃描選取的檔案。

完整掃描之後、您可以將許多其他Data Sense功能套用至資料、例如在「Data Investigation」（資料調查）頁面中檢視及精簡資料、在檔案中搜尋名稱、複製、移動及刪除來源檔案等。

授權與成本

下列問題與使用Cloud Data Sense的授權和成本有關。

Cloud Data合理的成本是多少？

使用Cloud Data Sense的成本取決於您要掃描的資料量。Data Sense在Cloud Manager工作區中掃描的前1 TB資料是免費的。達到該限制後、您需要下列其中一項、才能繼續掃描超過1 TB的資料：

- 向您的雲端供應商訂購Cloud Manager Marketplace清單、或
- NetApp的自帶授權（BYOL）

請參閱 ["定價"](#) 以取得詳細資料。

如果我達到BYOL容量上限、會發生什麼事？

如果您達到BYOL容量限制、Data Sense會繼續執行、但儀表板的存取會遭到封鎖、因此您無法檢視任何已掃描資料的相關資訊。只有在您想要減少所掃描的磁碟區數量、使容量使用量可能低於授權限制時、才可使用「組態」頁面。您必須續約BYOL授權、才能重新取得Data Sense的完整存取權。

連接器部署

下列問題與Cloud Manager Connector有關。

什麼是Connector？

Connector是在雲端帳戶內或內部部署的運算執行個體上執行的軟體、可讓Cloud Manager安全地管理雲端資源。您必須部署Connector才能使用Cloud Data Sense。

連接器需要安裝在何處？

- 在Cloud Volumes ONTAP AWS、Amazon FSx for ONTAP S2或AWS S3儲存區中掃描資料時、您會在AWS中使用連接器。
- 在Cloud Volumes ONTAP Azure 或 Azure NetApp Files 以不一樣的方式掃描資料時、您需要使用 Azure 中的連接器。
- 在Cloud Volumes ONTAP GCP中掃描資料時、請使用GCP中的Connector。
- 在內部部署ONTAP 的支援系統、非NetApp檔案共用、一般S3物件儲存、資料庫、OneDrive資料夾、SharePoint帳戶及Google雲端磁碟帳戶中掃描資料時、您可以在這些雲端位置中使用連接器。

因此、如果您在這些位置中有許多資料、您可能需要使用 ["多個連接器"](#)。

我可以在自己的主機上部署Connector嗎？

是的。您可以 ["在內部部署連接器"](#) 在網路或雲端的Linux主機上。如果您打算在內部部署Data Sense、則可能也想在內部部署安裝Connector、但這不是必要的。

沒有網際網路存取的安全網站又如何？

是的、這也受到支援。您可以 ["在無法存取網際網路的內部部署Linux主機上部署Connector"](#)。然後您可以探索內部部署ONTAP 的叢集和其他本機資料來源、並使用Data Sense掃描資料。

資料感測部署

下列問題與個別的Data Sense執行個體有關。

Cloud Data Sense需要哪種類型的執行個體或VM？

何時 ["部署於雲端"](#)：

- 在AWS中、Cloud Data Sense可在具有500 GB GP2磁碟的m5.4x大型 執行個體上執行。
- 在Azure中、Cloud Data Sense可在具有512 GB磁碟的Standard_D16s_v3 VM上執行。
- 在GCP中、Cloud Data Sense可在具有512 GB標準持續磁碟的n2-Standard-16 VM上執行。

請注意、您可以在CPU較少、RAM較少的系統上部署Data Sense、但使用這些系統時仍有限制。請參閱 ["使用較小的執行個體類型"](#) 以取得詳細資料。

["深入瞭解Cloud Data Sense的運作方式"](#)。

我可以在自己的主機上部署Data Sense嗎？

是的。您可以將Data Sense軟體安裝在可在網路或雲端存取網際網路的Linux主機上。一切都一樣運作、您也可以透過 Cloud Manager 繼續管理掃描組態和結果。請參閱 ["在內部部署Cloud Data Sense"](#) 以取得系統需求和安裝詳細資料。

沒有網際網路存取的安全網站又如何？

是的、這也受到支援。您可以 ["在無法存取網際網路的內部部署網站上部署Data Sense"](#) 完全安全的網站。

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.