深入瞭解資料隱私

Cloud Manager 3.7

NetApp
March 25, 2024

目錄

深入瞭解資料隱私 1
深入瞭解雲端法規遵循 1
Cloud Compliance for Cloud Volumes ONTAP NetApp入門 4
提高私有資料的可見度與控管能力 9
檢視隱私風險評估報告 16
回應資料主體存取要求 18
停用雲端法規遵循 19
雲端法規遵循的常見問題集 20

深入瞭解資料隱私

深入瞭解雲端法規遵循

Cloud Compliance是Cloud Volumes ONTAP 一套資料隱私與法規遵循服務、適用於AWS和Azure中的功能。Cloud Compliance採用人工智慧（AI）導向技術、可協助組織瞭解資料內容、並識別Cloud Volumes ONTAP 整個各個系統的敏感資料。

雲端法規遵循目前以受控的可用度版本提供。

"瞭解雲端法規遵循的使用案例"。

功能

Cloud Compliance 提供多種工具、可協助您達成法規遵循目標。您可以使用雲端法規遵循來：

- 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 ）

成本

Cloud Compliance是Cloud Volumes ONTAP NetApp提供的一套附加服務、無需額外付費。若要啟動Cloud Compliance、您必須部署雲端執行個體、雲端供應商會收取您的費用。資料不需支付進出的費用、因為資料不會在網路外流通。

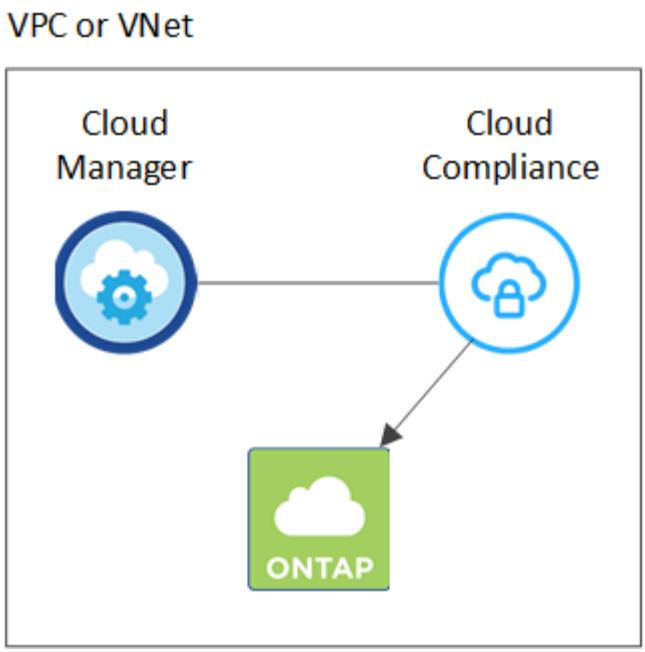
雲端法規遵循的運作方式

在高層級、 Cloud Compliance 的運作方式如下：

1. 您可以在一Cloud Volumes ONTAP 或多個支援雲端的系統上啟用Cloud Compliance。
2. Cloud Compliance 會使用 AI 學習程序掃描資料。
3. 在Cloud Manager中、您可以按一下* Compliance *、然後使用提供的儀表板和報告工具來協助您達成法規遵循目標。

Cloud Compliance 執行個體

當您在一Cloud Volumes ONTAP 或多個支援雲端的系統上啟用Cloud Compliance時、Cloud Manager會將Cloud Compliance執行個體部署在Cloud Volumes ONTAP 與要求中第一個支援的VPC或vnet相同的VPC或vnet上。



請注意下列關於執行個體的資訊：

- 在 Azure 中、 Cloud Compliance 可在標準磁碟機 D16s_v3 VM 上執行、磁碟容量為 512 GB 。
- 在AWS中、Cloud Compliance會在具有500 GB IO1磁碟的m5.4x大型 執行個體上執行。

  在無法使用 m5.4xLarge 的區域中、 Cloud Compliance 會改在 m4.4xLarge 執行個體上執行。

- 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Cloud Manager系統只部署一個Cloud Compliance執行個體。
- 雲端法規遵循軟體的升級是自動化的、您不需要擔心。

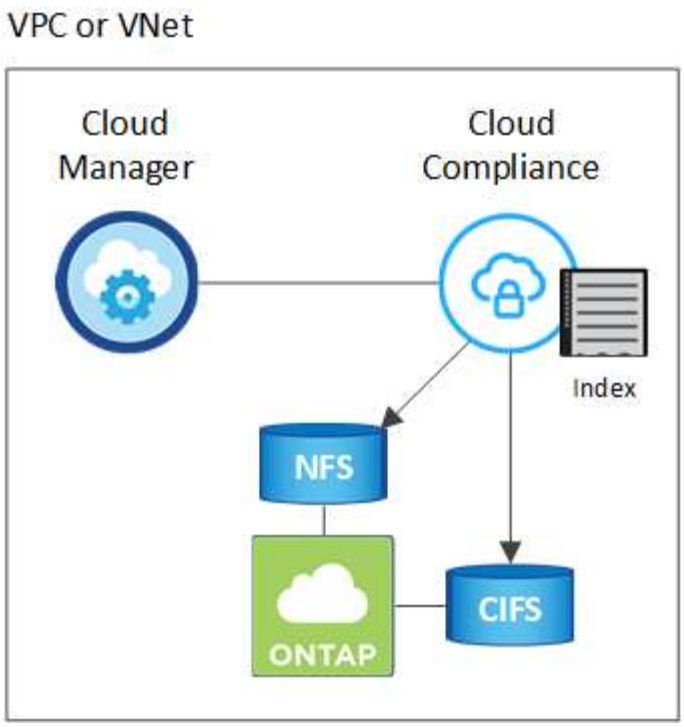
由於Cloud Compliance會持續掃描Cloud Volumes ONTAP 有關的資料、因此執行個體應隨時保持執行。

掃描的運作方式

啟用雲端法規遵循之後、IT會立即開始掃描資料、以識別個人和敏感資料。

Cloud Compliance Cloud Volumes ONTAP 可像任何其他用戶端一樣、透過掛載NFS和CIFS磁碟區來連線至功能不受限。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。

Cloud Compliance會掃描每個磁碟區上的非結構化資料、以取得各種個人資訊。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、敏感個人資訊和資料類別的索引。



在初始掃描之後、Cloud Compliance會持續掃描每個磁碟區、以偵測遞增變更（這也是為何務必讓執行個體持續執行的原因）。

您可以在工作環境層級開啟或關閉掃描、但不能在Volume層級開啟或關閉掃描。 "瞭解方法"。

Cloud Compliance 索引的資訊

Cloud Compliance會收集、索引及指派類別給非結構化資料（檔案）。Cloud Compliance 索引的資料包括：

標準中繼資料

Cloud Compliance 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 Compliance 會將掃描的資料分成不同類別、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"。

名稱實體辨識

Cloud Compliance 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 Compliance執行個體時會使用私有IP位址和安全群組、以便從Cloud Manager進行傳

入HTTP連線。此連線可讓您從Cloud Manager介面存取Cloud Compliance儀表板。

傳出規則已完全開啟。執行個體透過Cloud Volumes ONTAP Cloud Manager的Proxy連線至不穩定系統和網際網路。需要存取網際網路、才能升級Cloud Compliance軟體並傳送使用量標準。

如果您有嚴格的網路需求、 "瞭解 Cloud Compliance 所接觸的端點"。

> 索引資料絕不會離開Cloud Compliance執行個體、資料不會轉送到虛擬網路外部、也不會傳送到Cloud Manager。

使用者存取法規遵循資訊

Cloud Manager管理員可以檢視所有工作環境的法規遵循資訊。

Workspace系統管理員只能檢視具有存取權限的系統的法規遵循資訊。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「 Compliance 」（法規遵循）索引標籤中看到工作環境的任何法規遵循資訊。

"深入瞭解 Cloud Manager 角色"。

Cloud Compliance for Cloud Volumes ONTAP NetApp入門

完成幾個步驟、即可開始使用Cloud Volumes ONTAP AWS或Azure中的Cloud Compliance for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。

1 確認您的組態符合要求

- 確保Cloud Compliance執行個體可存取傳出的網際網路。

  Cloud Manager會將執行個體部署在Cloud Volumes ONTAP 要求中第一個的VPC或vnet上。

- 確保使用者可以從直接連線至AWS或Azure的主機、或是從與Cloud Compliance執行個體位於相同網路內的主機（執行個體將有私有IP位址）存取Cloud Manager介面。
- 確保雲端法規遵循執行個體持續運作。

2 在**Cloud Volumes ONTAP** 支援的基礎上實現雲端法規遵循

- 新的工作環境：建立工作環境（預設為啟用）時、請務必啟用雲端法規遵循。
- 現有工作環境：按一下* Compliance （符合法規）、編輯工作環境清單、然後按一下 Show Compliance Dashboard（顯示法規遵循儀表板）*。

3 確保能夠存取磁碟區

雲端法規遵循已啟用、請確保 IT 能夠存取磁碟區。

- Cloud Compliance執行個體需要網路連線至Cloud Volumes ONTAP 每個子網路。
- 適用於此功能的安全群組 Cloud Volumes ONTAP 必須允許來自 Cloud Compliance 執行個體的傳入連線。
- NFS Volume匯出原則必須允許從Cloud Compliance執行個體存取。
- Cloud Compliance 需要 Active Directory 認證資料才能掃描 CIFS Volume 。

  按一下「* Compliance **>** CIFS Scan Status **>** Edit CIFS Credentials*」、然後提供認證資料。認證資料可以是唯讀的、但提供管理認證可確保Cloud Compliance能夠讀取需要提升權限的資料。

4 確保**Cloud Manager**與**Cloud Compliance**之間的連線能力

- Cloud Manager的安全性群組必須允許來自連接埠80的傳入和傳出流量進出Cloud Compliance執行個體。
- 如果AWS網路未使用NAT或Proxy進行網際網路存取、Cloud Manager的安全性群組必須允許來自Cloud Compliance執行個體的TCP連接埠3128傳入流量。

檢閱先決條件

在啟用 Cloud Compliance 之前、請先檢閱下列先決條件、確定您擁有支援的組態。啟用雲端法規遵循之後、您必須確保元件之間的連線能力。內容涵蓋如下：

啟用傳出網際網路存取

雲端法規遵循需要外傳網際網路存取。如果您的虛擬網路使用Proxy伺服器進行網際網路存取、請確定Cloud Compliance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 Cloud Central 帳戶）進行通訊。
https://netapp-cloud-account.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-1.amazonaws.com https://hub.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	讓 Cloud Compliance 能夠存取及下載資訊清單和範本、並傳送記錄和指標。

驗證網路瀏覽器是否能連線至**Cloud Compliance**

Cloud Compliance 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。這種連線可能來自於 AWS 或 Azure （例如 VPN ）的直接連線、或來自與 Cloud Compliance 執行個體位於同一個網路內的主機。

如果您是從公有IP位址存取Cloud Manager、則您的網頁瀏覽器可能並未在網路內部的主機上執行。

持續執行雲端法規遵循

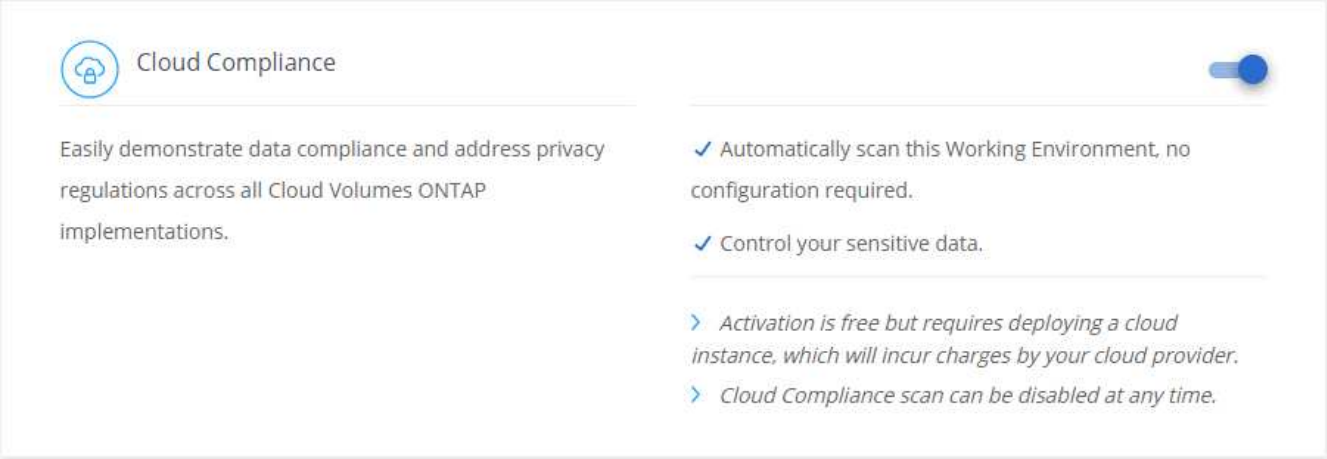
Cloud Compliance 執行個體必須持續執行、才能持續掃描資料。

在新的工作環境中實現雲端法規遵循

依預設、在工作環境精靈中會啟用「雲端法規遵循」。請務必保持啟用選項。

步驟

1. 按一下「 * 建立 Cloud Volumes ONTAP 參考 * 」。
2. 選取Amazon Web Services或Microsoft Azure做為雲端供應商、然後選擇單一節點或HA系統。
3. 填寫「詳細資料與認證」頁面。
4. 在「服務」頁面上、讓Cloud Compliance保持啟用狀態、然後按一下*繼續*。



5. 完成精靈中的頁面以部署系統。

   如需協助、請參閱 "在 Cloud Volumes ONTAP AWS 中啟動" 和 "在 Cloud Volumes ONTAP Azure 中啟動"。

結果

Cloud Compliance可在Cloud Volumes ONTAP 整個系統上啟用。如果這是您第一次啟用Cloud Compliance、Cloud Manager會在雲端供應商中部署Cloud Compliance執行個體。只要執行個體可用、就會在資料寫入您建立的每個磁碟區時開始掃描資料。

在現有的工作環境中實現雲端法規遵循

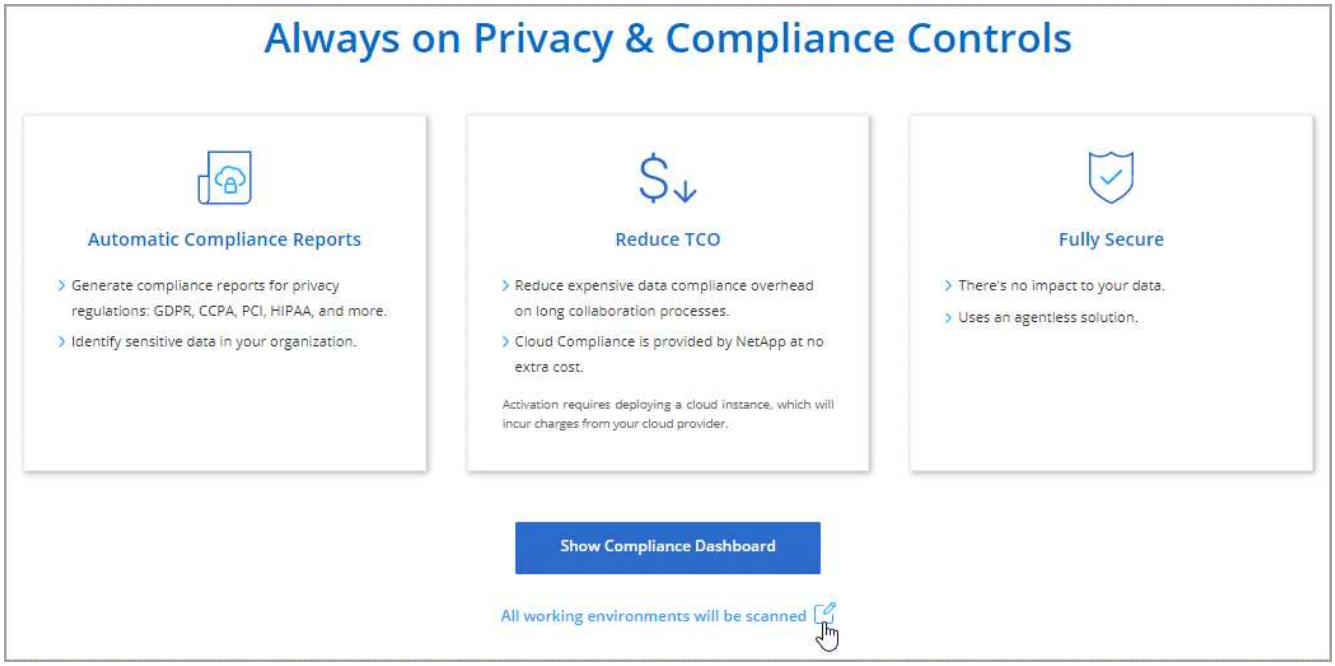
從Cloud Manager的* Compliance *（法規遵循）標籤、在現有Cloud Volumes ONTAP 的支援系統上啟用Cloud Compliance（雲端法規遵循）。

另一個選項是從*工作環境*索引標籤中個別選取每個工作環境、以啟用雲端法規遵循。除非您只有一個系統、否則需要更長的時間才能完成。

適用於多種工作環境的步驟

1. 在 Cloud Manager 頂端、按一下 * Compliance * 。
2. 如果您想在特定工作環境中啟用Cloud Compliance、請按一下編輯圖示。

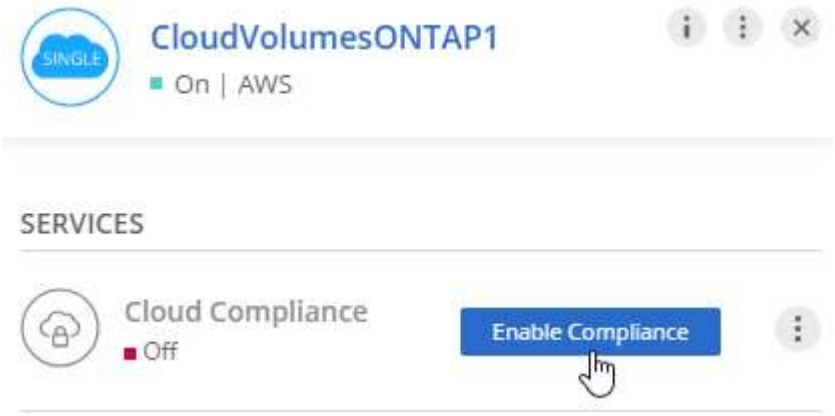
   否則、Cloud Manager會在您有權存取的所有工作環境中、啟用Cloud Compliance（雲端法規遵循）。



3. 按一下*顯示法規遵循儀表板*。

單一工作環境的步驟

1. 在Cloud Manager頂端、按一下*工作環境*。
2. 選取工作環境。
3. 在右側窗格中、按一下「 * 啟用相容性 * 」。



結果

如果這是您第一次啟用Cloud Compliance、Cloud Manager會在雲端供應商中部署Cloud Compliance執行個體。

Cloud Compliance會開始掃描每個工作環境中的資料。一旦Cloud Compliance完成初始掃描、資料就會出現在法規遵循儀表板中。所需時間取決於資料量、可能需要幾分鐘或幾小時。

確認 Cloud Compliance 可存取磁碟區

請檢查您的網路、安全群組和匯出原則、確保Cloud Compliance能夠存取Cloud Volumes ONTAP 位於Sure上的磁碟區。您必須提供符合雲端法規的 CIFS 認證資料、讓 IT 能夠存取 CIFS 磁碟區。

步驟

1. 確定Cloud Compliance執行個體與每Cloud Volumes ONTAP 個子網路之間都有網路連線。

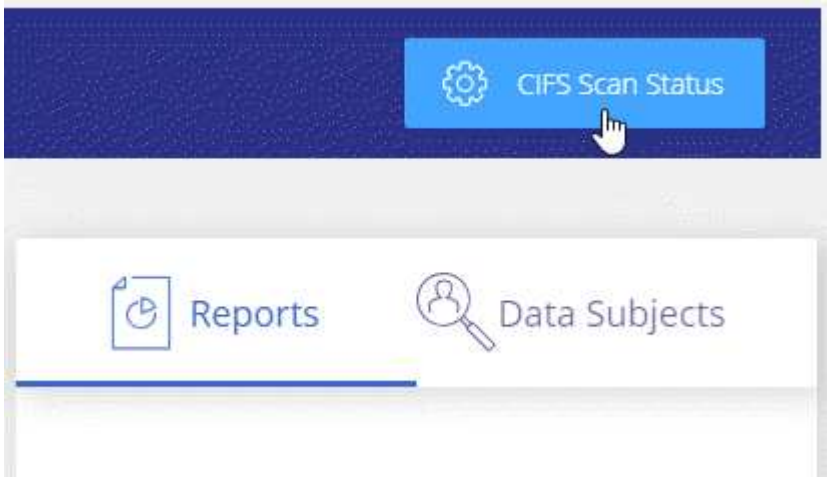
   Cloud Manager會將Cloud Compliance執行個體部署在Cloud Volumes ONTAP 與申請中第一個的版本相同的VPC或vnet上。因此、如果某些Cloud Volumes ONTAP 支援的系統位於不同的子網路或虛擬網路中、這個步驟就很重要。

2. 確保 Cloud Volumes ONTAP 適用於此功能的安全群組允許來自 Cloud Compliance 執行個體的傳入流量。

   您可以從 Cloud Compliance 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. 確保 NFS Volume 匯出原則包含 Cloud Compliance 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 Active Directory 認證的 Cloud Compliance 、以便掃描 CIFS Volume 。

   a. 在 Cloud Manager 頂端、按一下 * Compliance * 。
   b. 在右上角、按一下「* CIFS掃描狀態*」。



   c. 針對每Cloud Volumes ONTAP 個作業系統、按一下*編輯CIFS認證*、然後輸入Cloud Compliance存取系統上CIFS Volume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 Cloud Compliance 能夠讀取任何需要提高權限的資料。認證資料儲存在 Cloud Compliance 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。

驗證Cloud Manager是否可存取Cloud Compliance

確保Cloud Manager與Cloud Compliance之間的連線能力、讓您檢視Cloud Compliance所發現的法規遵循洞見。

步驟

1. 請確定Cloud Manager的安全性群組允許透過連接埠80往返Cloud Compliance執行個體的傳入和傳出流量。

   此連線可讓您在「Compliance」（符合性）索引標籤中檢視資訊。

2. 如果您的AWS網路未使用NAT或Proxy進行網際網路存取、請修改Cloud Manager的安全性群組、以允許來自Cloud Compliance執行個體的TCP連接埠3128傳入流量。

   這是必要的、因為Cloud Compliance執行個體使用Cloud Manager做為Proxy來存取網際網路。

   此連接埠預設會在所有新的Cloud Manager執行個體上開啟、從3.7.5版開始。它不會在該版本之前所建立的Cloud Manager執行個體上開啟。

提高私有資料的可見度與控管能力

檢視組織中個人資料和敏感個人資料的詳細資料、以掌控您的私有資料。您也可以檢閱資料中 Cloud Compliance 的類別和檔案類型、以獲得可見度。

個人資料

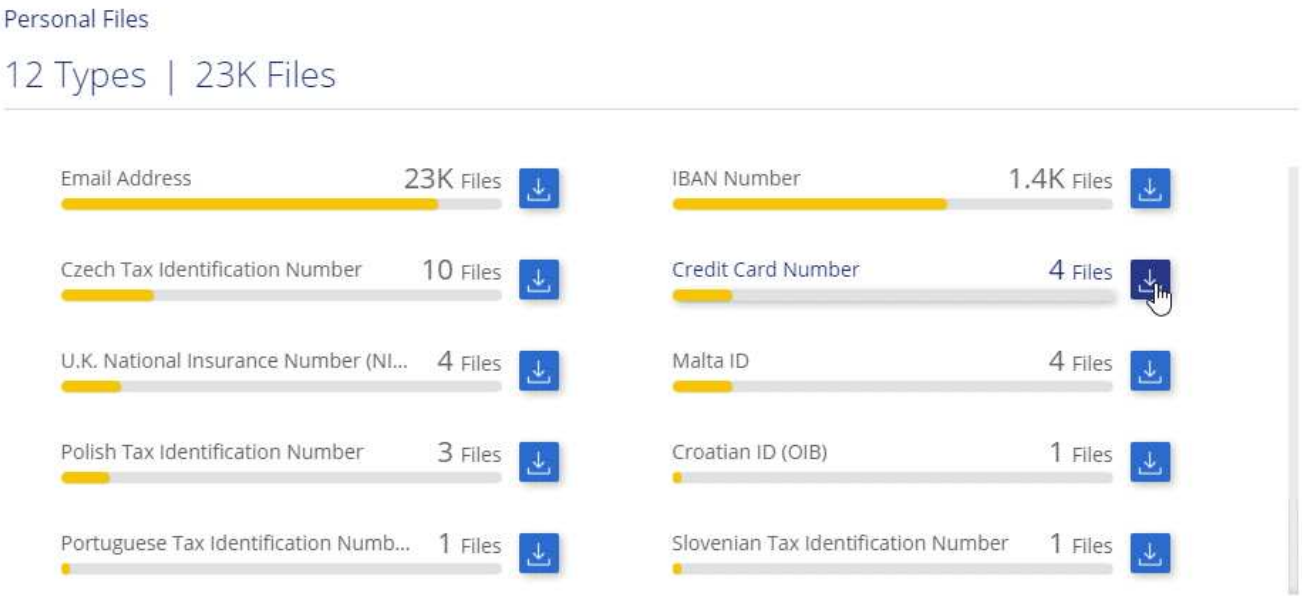
Cloud Compliance 會自動識別資料內部的特定字詞、字串和模式（ Regex ）。例如、個人識別資訊（ PII ）、信用卡號碼、社會安全號碼、銀行帳戶號碼等。 請參閱完整清單。

對於某些類型的個人資料、 Cloud Compliance 會使用 _ 近接驗證 _ 來驗證其發現結果。驗證的方式是在找到的個人資料附近尋找一或多個預先定義的關鍵字。例如、 Cloud Compliance 可識別美國社會安全號碼（ SSN ）若在 SSN 旁看到鄰近的詞彙、例如 *SSN* 或 _Social SECURITY 。 下表 顯示 Cloud Compliance 何時使用接近驗證。

檢視包含個人資料的檔案

步驟

1. 在 Cloud Manager 頂端、按一下 * Compliance * 。
2. 直接從主畫面下載前2大檔案類型的詳細資料、或按一下*檢視全部*、然後下載找到的任何個人資料類型清單。



個人資料類型

檔案中的個人資料可以是一般個人資料或國家識別碼。第三欄指出雲端法規遵循是否使用 鄰近驗證 驗證識別碼的發現。

類型	識別碼	鄰近驗證？
一般	電子郵件地址	否
	信用卡號碼	否
	IBAN 編號（國際銀行帳戶號碼）	否
	IP 位址	是的

類型	識別碼	鄰近驗證？
國家識別碼	比利時 ID （ Numero National ）	是的
	保加利亞文ID（統一化市民號碼）	是的
	塞浦路斯稅務識別編號（ TIC ）	是的
	丹麥稅務識別編號（CPR）	是的
	愛沙尼亞ID（Isikukood）	是的
	芬蘭文ID（henkilontnus）	是的
	法文稅務識別編號（ SPI ）	是的
	德國稅務識別編號（ Steuerlice 識別碼）	是的
	匈牙利稅務識別號碼（Adorazonos í t o jel）	是的
	愛爾蘭 ID （ PPS ）	是的
	以色列 ID	是的
	義大利文ID（Codice Fiscale）	是的
	拉脫維亞稅務識別編號	是的
	立陶宛ID（Asmen kodas）	是的
	盧森堡 ID	是的
	馬爾他ID	是的
	荷蘭ID（BSN）	是的
	波蘭稅務識別編號	是的
	葡萄牙稅務識別號碼（ NIF ）	是的
	羅馬尼亞稅務識別編號	是的
	斯洛伐克稅務識別編號	是的
	斯洛維尼亞稅務識別編號	是的
	南非 ID	是的
	西班牙稅務識別編號	是的
	瑞典稅務識別編號	是的
	英國國家保險號碼（Nino）	是的
	美國社會安全號碼（ SSN ）	是的

敏感的個人資料

Cloud Compliance 會自動識別特殊類型的敏感個人資訊、如隱私權法規所定義 "GDPR 第 9 和第 10 條"。例如、關於個人健康、族群或性取向的資訊。 請參閱完整清單。

Cloud Compliance 使用人工智慧（AI）、自然語言處理（NLP）、機器學習（ML）和認知運算（CC）來瞭解其掃描內容的意義、以便擷取實體並據此分類。

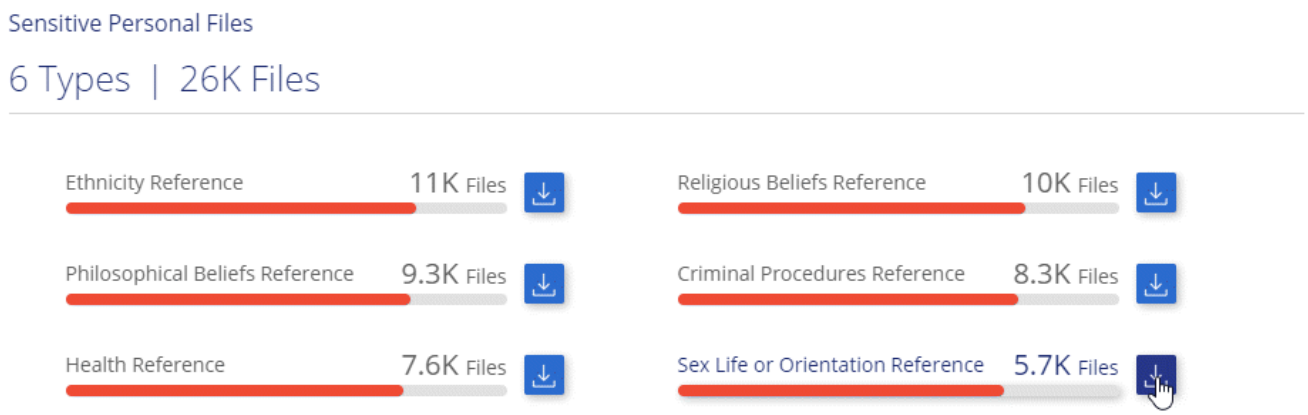
例如、一個敏感的 GDPR 資料類別是「族群」。由於 Cloud Compliance 的 NLP 能力、因此可以區分「George is 墨西哥」（表示 GDPR 第 9 條所述的敏感資料）與「George is Mexican ging」（George 正在吃墨西哥菜）這兩個句子的差異。

> 掃描敏感的個人資料時、僅支援英文。稍後將新增更多語言支援。

檢視含有敏感個人資料的檔案

步驟

1. 在 Cloud Manager 頂端、按一下 * Compliance * 。
2. 直接從主畫面下載前2大檔案類型的詳細資料、或按一下*檢視全部*、然後下載找到的任何敏感個人資料類型清單。



敏感個人資料的類型

Cloud Compliance 可在檔案中找到的敏感個人資料包括：

刑事訴訟程序參考資料
: 關於任何人的刑事定罪和犯罪的資料。

族群參考資料
: 關於一個人的種族或族裔來源的資料。

健全狀況參考資料
: 關於自然人健康的資料。

哲學理念參考資料
: 關於自然人哲學理念的資料。

《宗教信仰參考》
: 關於自然人的宗教信仰的資料。

性生活或取向參考資料
: 關於自然人性生活或性取向的資料。

類別

Cloud Compliance 會將掃描的資料分成不同類別、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。請參閱類別清單。

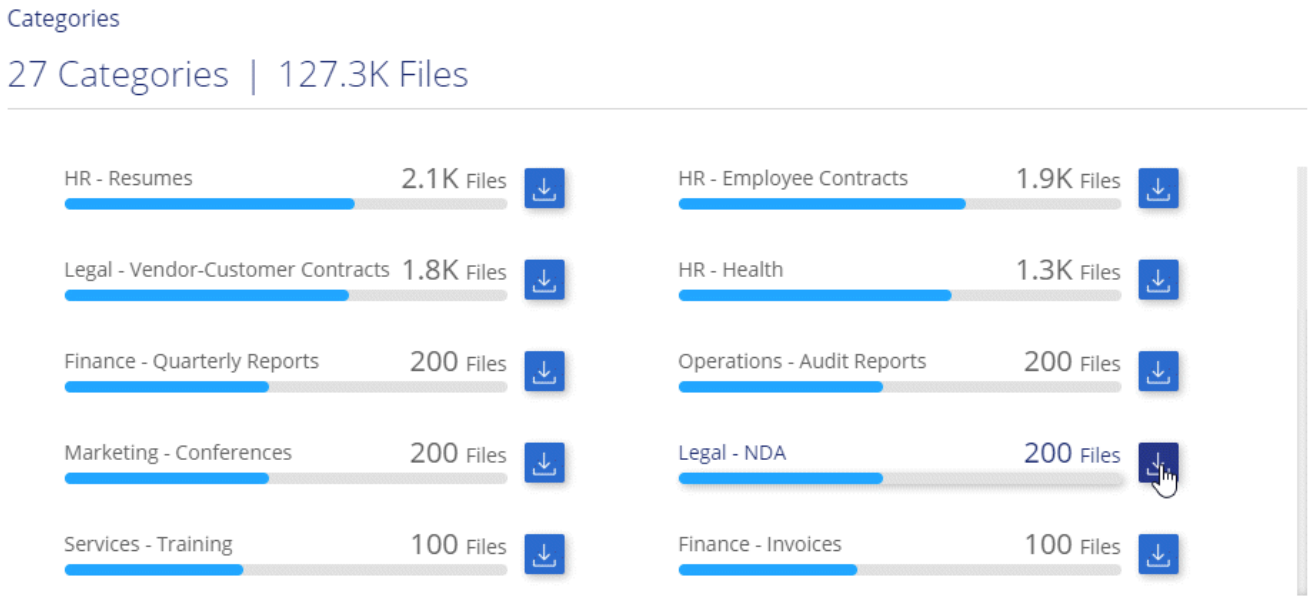
類別可顯示您擁有的資訊類型、協助您瞭解資料的現況。例如、簡歷或員工合約等類別可能包含敏感資料。下載CSV報告時、您可能會發現員工合約儲存在不安全的位置。然後您就可以修正該問題。

> 類別僅支援英文。稍後將新增更多語言支援。

依類別檢視檔案

步驟

1. 在 Cloud Manager 頂端、按一下 * Compliance * 。
2. 直接從主畫面下載前4大檔案類型的詳細資料、或按一下*檢視全部*、然後下載任何類別的清單。



類別類型

Cloud Compliance 將資料分類如下：

財務

- 平衡表
- 訂單
- 發票
- 季度報告

人力資源

- 背景檢查
- 補償計畫

- 員工合約
- 員工審查
- 健全狀況
- 恢復

合法

- NDA
- 廠商 - 客戶合約

行銷

- 行銷活動
- 會議

營運

- 稽核報告

銷售

- 銷售訂單

服務

- RFI
- RFP
- 訓練

支援

- 投訴與門票

其他

- 歸檔檔案
- 音訊
- CAD 檔案
- 程式碼
- 可執行檔
- 映像

檔案類型

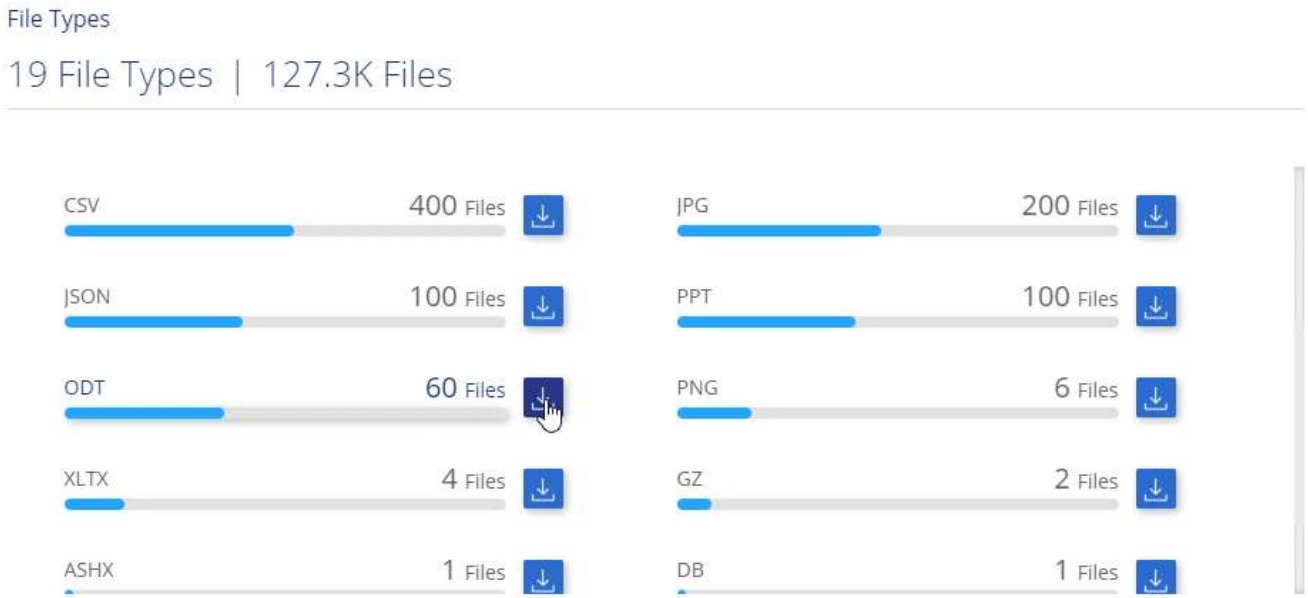
Cloud Compliance 會根據檔案類型來記錄掃描的資料、並將其細分。Cloud Compliance可顯示掃描中找到的所有檔案類型。

檢閱檔案類型有助於控制敏感資料、因為您可能會發現某些檔案類型儲存不正確。例如、您可能會儲存 CAD 檔案、其中包含有關組織的非常敏感資訊。如果機密資料不安全、您可以限制權限或將檔案移至其他位置、以取得機密資料的控制權。

檢視檔案類型

步驟

1. 在 Cloud Manager 頂端、按一下 * Compliance * 。
2. 直接從主畫面下載前4大檔案類型的詳細資料、或按一下*檢視全部*、然後下載任何檔案類型的清單。



找到資訊的準確度

NetApp 無法保證 Cloud Compliance 所識別的個人資料和敏感個人資料 100% 準確無誤。您應該一律檢閱資料來驗證資訊。

根據我們的測試結果、下表顯示 Cloud Compliance 找到的資訊準確度。我們將其細分為 _精密度 _ 和 _Recall _ ：

精確性

雲端法規遵循發現的可能性已正確識別。例如、 90% 的個人資料精準率表示、在 10 個被識別為包含個人資訊的檔案中、有 9 個檔案實際上包含個人資訊。10 個檔案中有 1 個是誤報的。

回收

雲端法規遵循的可能性。例如、個人資料的回收率為 70% 、表示 Cloud Compliance 可在組織內實際包含個人資訊的 10 個檔案中找出 7 個檔案。雲端法規遵循將會遺漏 30% 的資料、而且不會出現在儀表板中。

Cloud Compliance 是受控的可用度版本、我們持續改善結果的準確度。未來的 Cloud Compliance 版本將會自動提供這些改良功能。

類型	精確性	回收
個人資料 - 一般	90% 至 95%	60% 至 80%
個人資料 - 國家 / 地區識別碼	30% 至 60%	40% 至 60%
敏感的個人資料	80% 至 95%	20% 至 30%

類型	精確性	回收
類別	90% 至 97%	60% 至 80%

每份檔案清單報告中所包含的內容（ **CSV** 檔案）

儀表板可讓您下載檔案清單（CSV格式）、其中包含已識別檔案的詳細資料。如果結果超過10、000個、則只有前10、000個結果會出現在清單中（稍後會新增更多支援）。

每個檔案清單都包含下列資訊：

- 檔案名稱
- 位置類型
- 位置
- 檔案路徑
- 檔案類型
- 類別
- 個人資訊
- 敏感的個人資訊
- 刪除偵測日期

  刪除偵測日期可識別檔案刪除或移動的日期。這可讓您識別敏感檔案的移動時間。刪除的檔案不屬於儀表板中顯示的檔案編號數。這些檔案只會出現在 CSV 報告中。

檢視隱私風險評估報告

隱私權風險評估報告概述貴組織的隱私權風險狀態、如 GDPR 和 CCPA 等隱私權法規要求。

> NetApp 無法保證 Cloud Compliance 所識別的個人資料和敏感個人資料 100% 準確無誤。您應該一律檢閱資料來驗證資訊。

報告包含下列資訊：

法規遵循狀態

嚴重性分數（請參閱下方以瞭解更多詳細資料）以及資料的散佈、無論是不敏感、個人或敏感的個人資料。

評估總覽

所找到的個人資料類型及資料類別的明細。

本評估的資料主題

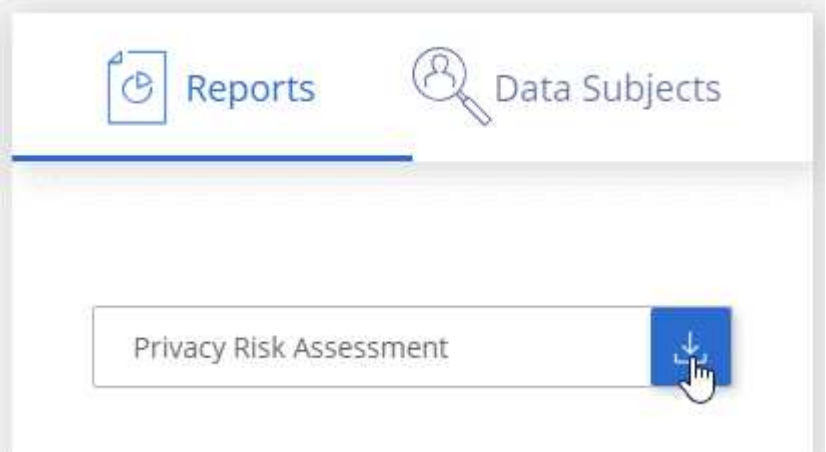
按地點列出找到國家識別碼的人數。

產生隱私風險評估報告

前往「 Compliance 」（法規遵循）索引標籤以產生報告。

步驟

1. 在 Cloud Manager 頂端、按一下 * Compliance * 。
2. 在「 * 報告 * 」下、按一下「 * 隱私風險評估 * 」旁的下載圖示。



結果

Cloud Compliance 會產生一份 PDF 報告、您可以視需要檢閱並傳送給其他群組。

嚴重性分數

Cloud Compliance 會根據三個變數來計算隱私風險評估報告的嚴重性分數：

- 所有資料中的個人資料百分比。
- 所有資料中敏感個人資料的百分比。
- 包含資料主體的檔案百分比、由國家識別碼、社會安全號碼及稅務 ID 等國家識別碼所決定。

用來判斷分數的邏輯如下：

嚴重性分數	邏輯
0	這三個變數都是 0%
1.	其中一個變數大於 0%
2.	其中一個變數大於 3%
3.	其中兩個變數大於 3%
4.	其中三個變數大於 3%
5.	其中一個變數較大6%
6.	其中兩個變數較大6%
7.	其中有三個變數較大6%

嚴重性分數	邏輯
8.	其中一個變數大於15%
9.	其中兩個變數較大15%
10.	其中有三個變數較大15%

回應資料主體存取要求

搜尋受試者的全名或已知識別碼（例如電子郵件地址）、然後下載報告、即可回應資料受試者存取要求（ DSAR ）。本報告旨在協助貴組織遵守 GDPR 或類似資料隱私權法律。

> NetApp 無法保證 Cloud Compliance 所識別的個人資料和敏感個人資料 100% 準確無誤。您應該一律檢閱資料來驗證資訊。

什麼是資料主體存取要求？

歐洲 GDPR 等隱私權法規賦予資料當事人（例如客戶或員工）存取其個人資料的權利。當資料主體要求此資訊時、這稱為 DSAR （資料主體存取要求）。組織必須在收到申請後一個月內、「不致發生不當延誤」地回應這些要求。

Cloud Compliance 如何協助您回應 DSAR ？

當您執行資料主旨搜尋時、Cloud Compliance會尋找其中含有該人員名稱或識別碼的所有檔案。Cloud Compliance 會檢查最新的預先索引資料、找出名稱或識別碼。它不會啟動新的掃描。

搜尋完成後、您就可以下載檔案清單或資料主旨存取要求報告。報告會彙總資料的深入見解、並將其納入法律條款、以便您寄回給該人員。

搜尋資料主題並下載報告

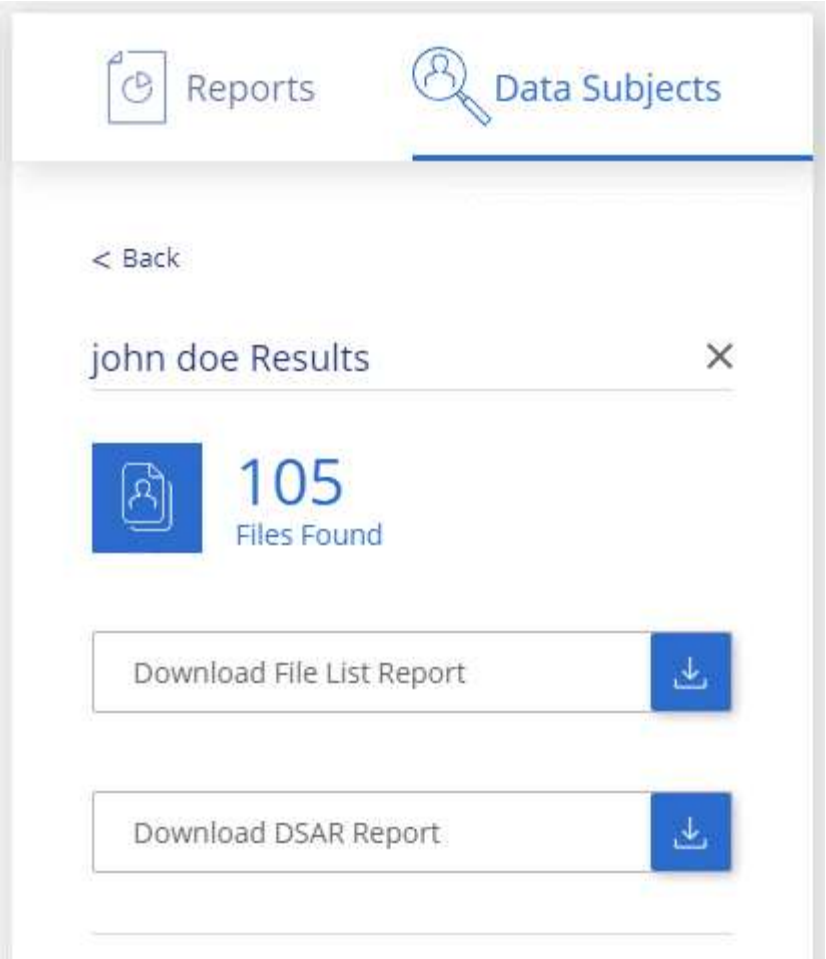
搜尋資料主旨的完整名稱或已知識別碼、然後下載檔案清單報告或 DSAR 報告。您可以搜尋 "任何個人資訊類型"。

> 搜尋資料主題名稱時、僅支援英文。稍後將新增更多語言支援。

步驟

1. 在 Cloud Manager 頂端、按一下 * Compliance * 。
2. 按一下 * 資料主題 * 。
3. 搜尋資料主旨的完整名稱或已知識別碼。

   以下範例顯示名稱 *John doe* 的搜尋：



4. 請選擇下列其中一個可用選項：
   - 下載檔案清單報告：包含資料主旨資訊的檔案清單。

     如果結果超過10、000項、則報告中只會顯示前10、000項（稍後將會新增更多支援）。

   - * 下載 DSAR 報告 * ：您可傳送至資料主旨的存取要求正式回應。此報告會根據在資料主題上找到的 Cloud Compliance 資料、自動產生資訊、並設計作為範本使用。您應先填寫表單並在內部審查、再將其傳送至資料主旨。

停用雲端法規遵循

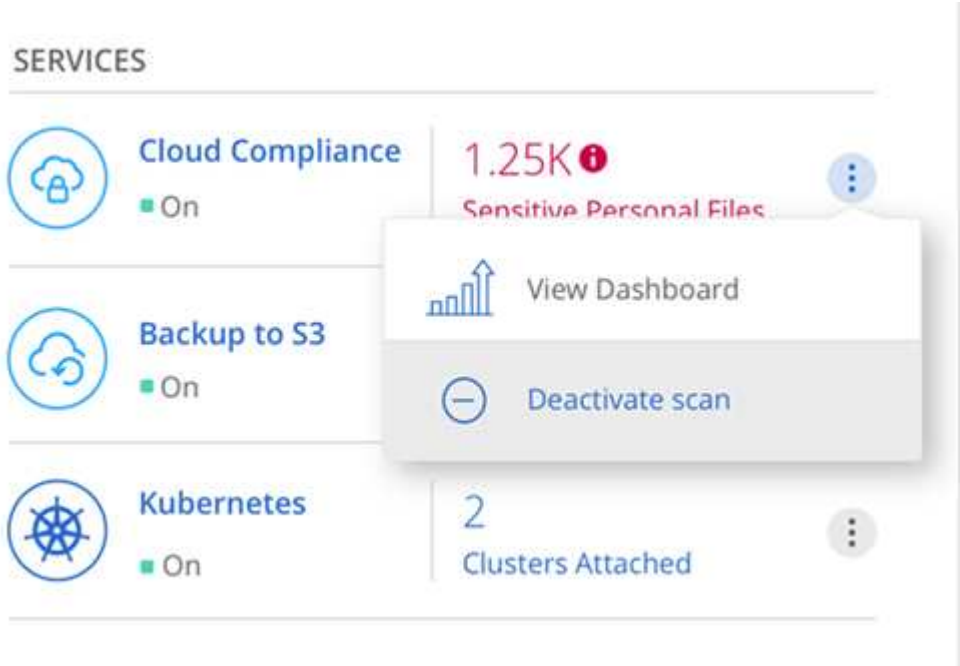
如果需要、您可以停止 Cloud Compliance 掃描一或多個工作環境。如果您不想再將Cloud Compliance搭配Cloud Volumes ONTAP 使用於您的作業系統、也可以刪除Cloud Compliance執行個體。

停用工作環境的法規遵循掃描

當您停用掃描時、Cloud Compliance不再掃描系統上的資料、也會從Cloud Compliance執行個體移除已建立索引的法規遵循洞見（不會刪除工作環境本身的資料）。

步驟

1. 在Cloud Manager頂端、按一下*工作環境*。
2. 選取工作環境。
3. 在右側面板中、按一下Cloud Compliance Service的行動圖示、然後選取* Deactivate scan *。



刪除 **Cloud Compliance** 執行個體

如果您不想再使用Cloud Compliance with Cloud Volumes ONTAP the效益、可以刪除Cloud Compliance執行個體。刪除執行個體也會刪除索引資料所在的相關磁碟。

步驟

1. 移至雲端供應商的主控台、然後刪除 Cloud Compliance 執行個體。

   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*

雲端法規遵循的常見問題集

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。

什麼是雲端法規遵循？

Cloud Compliance是全新的NetApp雲端產品。Cloud Compliance採用人工智慧（AI）導向技術、可協助組織瞭解資料內容、並在Cloud Volumes ONTAP AWS或Azure上代管的各個支援系統中識別敏感資料。

雲端法規遵循提供預先定義的參數（例如敏感資訊類型和類別）、以因應新的資料法規遵循法規、以確保資料隱私和敏感度、例如GDPR、CCPA等。

為何應該使用雲端法規遵循？

雲端法規遵循可協助您運用資料、協助您：

- 遵守資料法規遵循與隱私權法規。
- 遵守資料保留政策。
- 根據GDPR、CCPA及其他資料隱私權法規的要求、輕鬆找到並報告特定資料、以因應資料主題。

雲端法規遵循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。

"深入瞭解雲端法規遵循的使用案例"。

哪些類型的資料可透過 **Cloud Compliance** 進行掃描？

Cloud Compliance支援透過NFS和CIFS傳輸協定掃描非結構化資料。目前Cloud Compliance會掃描Cloud Volumes ONTAP 由NetApp管理的資料。

"瞭解掃描的運作方式"。

支援哪些雲端供應商？

Cloud Compliance 是 Cloud Manager 的一部分、目前支援 AWS 和 Azure 。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。Google Cloud Platform （GCP）支援即將新增。

如何存取雲端法規遵循？

雲端法規遵循是透過 Cloud Manager 進行營運與管理。您可以從 Cloud Manager 的「* Compliance *」（* 法規遵循 *）索引標籤存取 Cloud Compliance 功能。

雲端法規遵循的運作方式為何？

Cloud Compliance會在Cloud Manager系統和Cloud Volumes ONTAP 例項中部署另一層人工智慧。然後掃描Cloud Volumes ONTAP 有關資料的資料、並為找到的資料洞見建立索引。

"深入瞭解 Cloud Compliance 的運作方式"。

Cloud Compliance 的成本是多少？

Cloud Compliance是Cloud Volumes ONTAP 以不需額外成本的方式提供、不需額外付費。未來可能需要額外的成本來進行自訂功能。

> Cloud Compliance需要在雲端供應商中部署執行個體、您必須向雲端供應商收取相關費用。

Cloud Compliance 多久掃描一次我的資料？

資料經常變更、因此 Cloud Compliance 會持續掃描您的資料、而不會對您的資料造成任何影響。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"。

Cloud Compliance 是否提供報告？

是的。Cloud Compliance 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。

下列報告適用於雲端法規遵循：

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"。

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"。

雲端法規遵循需要哪種類型的執行個體或 VM ？

- 在 Azure 中、 Cloud Compliance 可在標準磁碟機 D16s_v3 VM 上執行、磁碟容量為 512 GB 。
- 在AWS中、Cloud Compliance會在具有500 GB IO1磁碟的m5.4x大型 執行個體上執行。

  在無法使用 m5.4xLarge 的區域中、 Cloud Compliance 會改在 m4.4xLarge 執行個體上執行。

"深入瞭解 Cloud Compliance 的運作方式"。

掃描效能是否有所差異？

掃描效能可能會因網路頻寬和雲端環境中的平均檔案大小而異。

如何實現雲端法規遵循？

您可以在建立新的工作環境時、啟用Cloud Compliance。您可以從* Compliance *（符合性）索引標籤（僅限初次啟動時）或選取特定工作環境、在現有的工作環境中啟用此功能。

"瞭解如何開始使用"。

啟動 Cloud Compliance 會立即進行初始掃描。法規遵循結果不久即會顯示。

如何停用雲端法規遵循？

選取個別工作環境之後、即可從「工作環境」頁面停用「雲端法規遵循」。

"深入瞭解"。

> 若要完全移除 Cloud Compliance 執行個體、您可以從雲端供應商的入口網站手動移除 Cloud Compliance 執行個體。

如果在不支援的情況下啟用資料分層、會發生什麼情況 **Cloud Volumes ONTAP** ？

您可能想要在 Cloud Volumes ONTAP 將冷資料分層儲存至物件儲存的支援系統上、啟用 Cloud Compliance 。如果啟用資料分層、 Cloud Compliance 會掃描磁碟上的所有資料、然後將冷資料分層至物件儲存設備。

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。

我可以使用**Cloud Compliance**來掃描內部部署**ONTAP** 的不實資料儲存設備嗎？

不可以Cloud Compliance目前已成為Cloud Manager的一部分、並支援Cloud Volumes ONTAP 各種功能。我們計畫支援Cloud Compliance、提供Cloud Volumes Service 更多雲端產品、例如：功能豐富的功能、例如：Azure NetApp Files

Cloud Compliance 是否能傳送通知給我的組織？

否、但您可以下載狀態報告、以便在組織內部分享。

我可以根據組織的需求自訂服務嗎？

雲端法規遵循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。

我可以將雲端法規遵循資訊限制在特定使用者身上嗎？

是的、 Cloud Compliance 已與 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。

"深入瞭解"。