Approfondimenti sulla privacy dei dati

Cloud Manager 3.7

NetApp
March 25, 2024

Sommario

Approfondimenti sulla privacy dei dati . . . 1
Scopri di più sulla conformità al cloud . . . 1
Introduzione alla conformità cloud per Cloud Volumes ONTAP . . . 4
Ottenere visibilità e controllo sui dati privati . . . 10
Visualizzazione del report sulla valutazione dei rischi per la privacy . . . 17
Risposta a una richiesta di accesso soggetto a dati . . . 19
Disattivazione della conformità al cloud . . . 20
Domande frequenti sulla conformità al cloud . . . 21

Approfondimenti sulla privacy dei dati

Scopri di più sulla conformità al cloud

La conformità al cloud è un servizio di privacy e conformità dei dati per Cloud Volumes ONTAP in AWS e Azure. Utilizzando la tecnologia basata sull'intelligenza artificiale (ai), la conformità al cloud aiuta le organizzazioni a comprendere il contesto dei dati e a identificare i dati sensibili nei sistemi Cloud Volumes ONTAP.

Cloud Compliance è attualmente disponibile come release a disponibilità controllata.

"Scopri i casi di utilizzo per la conformità al cloud".

Caratteristiche

Cloud Compliance offre diversi strumenti che possono aiutarti con le tue attività di compliance. Puoi utilizzare la conformità al cloud per:

- Identificare le informazioni personali identificabili (PII)
- Identificare un ampio ambito di informazioni sensibili come richiesto dalle normative sulla privacy GDPR, CCPA, PCI e HIPAA
- Rispondere alle richieste di accesso dei soggetti a dati (DSAR)

Costo

La conformità al cloud è un servizio add-on per Cloud Volumes ONTAP fornito da NetApp senza costi aggiuntivi. L'attivazione della conformità al cloud richiede l'implementazione di un'istanza del cloud, che verrà addebitata dal tuo cloud provider. Non sono previsti costi per l'ingresso o l'uscita dei dati perché i dati non fluiscono all'esterno della rete.

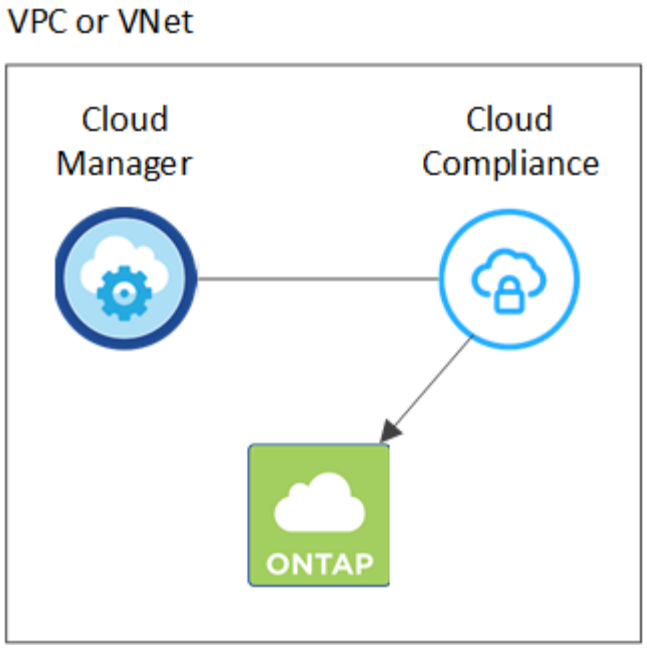
Come funziona Cloud Compliance

Ad alto livello, la conformità al cloud funziona come segue:

1. Abilita la conformità al cloud su uno o più sistemi Cloud Volumes ONTAP.
2. Cloud Compliance esegue la scansione dei dati utilizzando un processo di apprendimento ai.
3. In Cloud Manager, fai clic su **Compliance** e utilizza la dashboard e gli strumenti di reporting forniti per aiutarti nelle tue attività di compliance.

L'istanza di Cloud Compliance

Quando abiliti la conformità al cloud su uno o più sistemi Cloud Volumes ONTAP, Cloud Manager implementa un'istanza di conformità al cloud nello stesso VPC o VNET del primo sistema Cloud Volumes ONTAP nella richiesta.



Tenere presente quanto segue a proposito dell'istanza:

- In Azure, Cloud Compliance viene eseguito su una macchina virtuale Standard_D16s_v3 con un disco da 512 GB.
- In AWS, Cloud Compliance viene eseguito su un'istanza m5.4xLarge con un disco io1 da 500 GB.

  Nelle regioni in cui m5.4xlarge non è disponibile, Cloud Compliance viene eseguito su un'istanza m4.4xlarge.

- L'istanza è denominata *CloudCompliance* con un hash generato (UUID) concatenato ad essa. Ad esempio: *CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*
- Per ogni sistema Cloud Manager viene implementata una sola istanza di Cloud Compliance.
- Gli aggiornamenti del software Cloud Compliance sono automatizzati e non dovrai preoccuparti di questo.

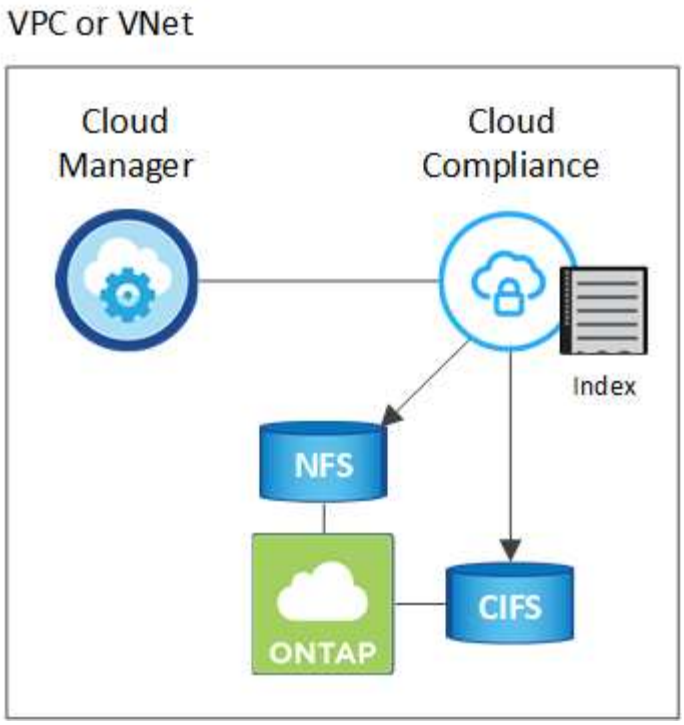
L'istanza deve rimanere sempre in esecuzione perché la conformità cloud esegue continuamente la scansione dei dati sui sistemi Cloud Volumes ONTAP.

Come funzionano le scansioni

Dopo aver attivato la conformità al cloud, inizia immediatamente la scansione dei dati per identificare i dati personali e sensibili.

La conformità al cloud si connette a Cloud Volumes ONTAP come qualsiasi altro client montando volumi NFS e CIFS. Ai volumi NFS viene automaticamente eseguito l'accesso in sola lettura, mentre è necessario fornire le credenziali Active Directory per eseguire la scansione dei volumi CIFS.

Cloud Compliance esegue la scansione dei dati non strutturati su ciascun volume per individuare una serie di informazioni personali. Mappa i dati dell'organizzazione, classifica ciascun file e identifica ed estrae entità e modelli predefiniti nei dati. Il risultato della scansione è un indice di informazioni personali, informazioni personali sensibili e categorie di dati.



Dopo la scansione iniziale, Cloud Compliance esegue una scansione continua di ciascun volume per rilevare le modifiche incrementali (per questo motivo è importante mantenere l'istanza in esecuzione).

È possibile attivare e disattivare le scansioni a livello di ambiente di lavoro, ma non a livello di volume. "Scopri come".

Informazioni indicizzati dalla Cloud Compliance

Cloud Compliance raccoglie, indicizza e assegna le categorie ai dati non strutturati (file). I dati indicizzati dalla Cloud Compliance includono:

Metadati standard

Cloud Compliance raccoglie i metadati standard relativi ai file: Il tipo, le dimensioni, le date di creazione e modifica e così via.

Dati personali

Informazioni personali come indirizzi e-mail, numeri di identificazione o numeri di carta di credito. "Scopri di più sui dati personali".

Dati personali sensibili

Tipi speciali di informazioni sensibili, come dati sanitari, origine etnica o opinioni politiche, come definito dal GDPR e da altre normative sulla privacy. "Scopri di più sui dati personali sensibili".

Categorie

Cloud Compliance prende i dati sottoposti a scansione e li divide in diversi tipi di categorie. Le categorie sono argomenti basati sull'analisi ai del contenuto e dei metadati di ciascun file. "Scopri di più sulle categorie".

Riconoscimento entità nome

Cloud Compliance utilizza l'ai per estrarre i nomi delle persone fisiche dai documenti. "Scopri come rispondere alle richieste di accesso ai soggetti dati".

Panoramica delle reti

Cloud Manager implementa l'istanza Cloud Compliance con un indirizzo IP privato e un gruppo di sicurezza che abilita le connessioni HTTP in entrata da Cloud Manager. Questa connessione consente di accedere alla dashboard Cloud Compliance dall'interfaccia di Cloud Manager.

Le regole in uscita sono completamente aperte. L'istanza si connette ai sistemi Cloud Volumes ONTAP e a Internet tramite un proxy da Cloud Manager. L'accesso a Internet è necessario per aggiornare il software Cloud Compliance e inviare metriche di utilizzo.

Se hai requisiti di rete rigorosi, "Scopri gli endpoint che la Cloud Compliance contatta".

I dati indicizzati non lasciano mai l'istanza di Cloud Compliance: I dati non vengono inoltrati al di fuori della rete virtuale e non vengono inviati a Cloud Manager.

Accesso dell'utente alle informazioni di conformità

Gli amministratori di Cloud Manager possono visualizzare le informazioni di conformità per tutti gli ambienti di lavoro.

Gli amministratori dello spazio di lavoro possono visualizzare le informazioni di conformità solo per i sistemi ai quali sono autorizzati ad accedere. Se un amministratore dell'area di lavoro non riesce ad accedere a un ambiente di lavoro in Cloud Manager, non può visualizzare alcuna informazione di conformità per l'ambiente di lavoro nella scheda Compliance.

"Scopri di più sui ruoli di Cloud Manager".

Introduzione alla conformità cloud per Cloud Volumes ONTAP

Completa alcuni passaggi per iniziare a utilizzare la conformità cloud per Cloud Volumes ONTAP in AWS o Azure.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

Verificare che la configurazione soddisfi i requisiti

- Assicurarsi che l'istanza Cloud Compliance disponga dell'accesso a Internet in uscita.

  Cloud Manager implementa l'istanza nello stesso VPC o VNET del primo sistema Cloud Volumes ONTAP nella richiesta.

- Assicurarsi che gli utenti possano accedere all'interfaccia di Cloud Manager da un host che dispone di una connessione diretta ad AWS o Azure o da un host che si trova all'interno della stessa rete dell'istanza di Cloud Compliance (l'istanza avrà un indirizzo IP privato).
- Assicurarsi di poter mantenere in esecuzione l'istanza Cloud Compliance.

Abilita la conformità del cloud su Cloud Volumes ONTAP

- Nuovi ambienti di lavoro: Assicurati di mantenere la conformità cloud abilitata quando crei l'ambiente di lavoro (è attivata per impostazione predefinita).
- Ambienti di lavoro esistenti: Fare clic su **Compliance**, modificare l'elenco degli ambienti di lavoro e fare clic su **Show Compliance Dashboard** (Mostra dashboard conformità).

Garantire l'accesso ai volumi

Ora che la conformità al cloud è abilitata, assicurati che l'IT possa accedere ai volumi.

- L'istanza di conformità cloud richiede una connessione di rete a ciascuna subnet Cloud Volumes ONTAP.
- I gruppi di sicurezza per Cloud Volumes ONTAP devono consentire connessioni in entrata dall'istanza di conformità cloud.
- Le policy di esportazione dei volumi NFS devono consentire l'accesso dall'istanza Cloud Compliance.
- Cloud Compliance necessita delle credenziali di Active Directory per eseguire la scansione dei volumi CIFS.

  Fare clic su **Compliance** > **CIFS Scan Status** > **Edit CIFS Credentials** (Modifica credenziali CIFS) e fornire le credenziali. Le credenziali possono essere di sola lettura, ma fornire credenziali di amministratore garantisce che Cloud Compliance possa leggere i dati che richiedono autorizzazioni elevate.

Garantire la connettività tra Cloud Manager e Cloud Compliance

- Il gruppo di sicurezza per Cloud Manager deve consentire il traffico in entrata e in uscita sulla porta 80 da e verso l'istanza Cloud Compliance.
- Se la rete AWS non utilizza un NAT o un proxy per l'accesso a Internet, il gruppo di sicurezza per Cloud Manager deve consentire il traffico in entrata sulla porta TCP 3128 dall'istanza Cloud Compliance.

Verifica dei prerequisiti

Prima di attivare la conformità al cloud, verificare di disporre di una configurazione supportata. Dopo aver attivato la conformità al cloud, dovrai garantire la connettività tra i componenti. Di seguito viene descritto.

Abilitare l'accesso a Internet in uscita

La conformità al cloud richiede l'accesso a Internet in uscita. Se la rete virtuale utilizza un server proxy per l'accesso a Internet, assicurarsi che l'istanza Cloud Compliance disponga dell'accesso a Internet in uscita per contattare i seguenti endpoint:

Endpoint	Scopo
https://cloudmanager.cloud.netapp.com	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.

Endpoint	Scopo
https://cloud-compliance-support-netapp.s3.us-west-1.amazonaws.com https://hub.docker.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Consente alla conformità del cloud di accedere e scaricare manifesti e modelli e di inviare registri e metriche.

Verificare la connettività del browser Web alla conformità del cloud

L'istanza Cloud Compliance utilizza un indirizzo IP privato per garantire che i dati indicizzati non siano accessibili a Internet. Di conseguenza, il browser Web utilizzato per accedere a Cloud Manager deve disporre di una connessione a tale indirizzo IP privato. Tale connessione può provenire da una connessione diretta ad AWS o Azure (ad esempio, una VPN) o da un host che si trova all'interno della stessa rete dell'istanza Cloud Compliance.

Se si accede a Cloud Manager da un indirizzo IP pubblico, probabilmente il browser Web non è in esecuzione su un host all'interno della rete.

Mantieni la conformità al cloud in esecuzione

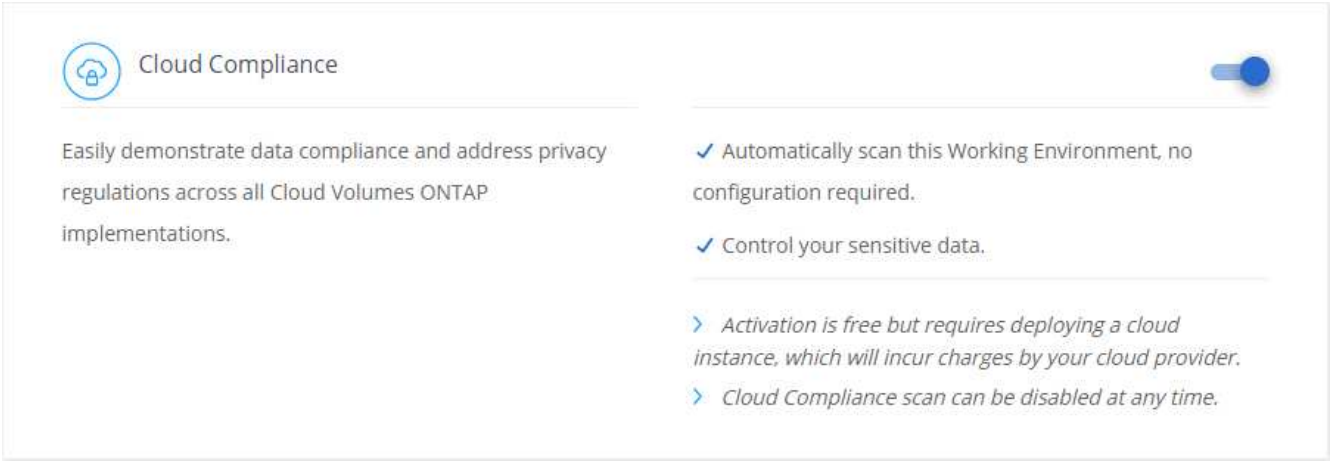
L'istanza di Cloud Compliance deve continuare a eseguire la scansione dei dati.

Abilitare la conformità al cloud in un nuovo ambiente di lavoro

La conformità cloud è attivata per impostazione predefinita nella procedura guidata dell'ambiente di lavoro. Assicurarsi di mantenere l'opzione attivata.

Fasi

1. Fare clic su **Crea Cloud Volumes ONTAP**.
2. Selezionare Amazon Web Services o Microsoft Azure come provider cloud, quindi scegliere un singolo nodo o sistema ha.
3. Compila la pagina Dettagli e credenziali.
4. Nella pagina servizi, lasciare abilitata la conformità cloud e fare clic su **continua**.



5. Completare le pagine della procedura guidata per implementare il sistema.

   Per ulteriori informazioni, vedere "Avvio di Cloud Volumes ONTAP in AWS" e. "Lancio di Cloud Volumes ONTAP in Azure".

Risultato

La conformità al cloud è abilitata sul sistema Cloud Volumes ONTAP. Se questa è la prima volta che hai attivato la conformità al cloud, Cloud Manager implementa l'istanza di conformità al cloud nel tuo cloud provider. Non appena l'istanza è disponibile, inizia la scansione dei dati man mano che vengono scritti in ciascun volume creato.

Abilitare la conformità al cloud negli ambienti di lavoro esistenti

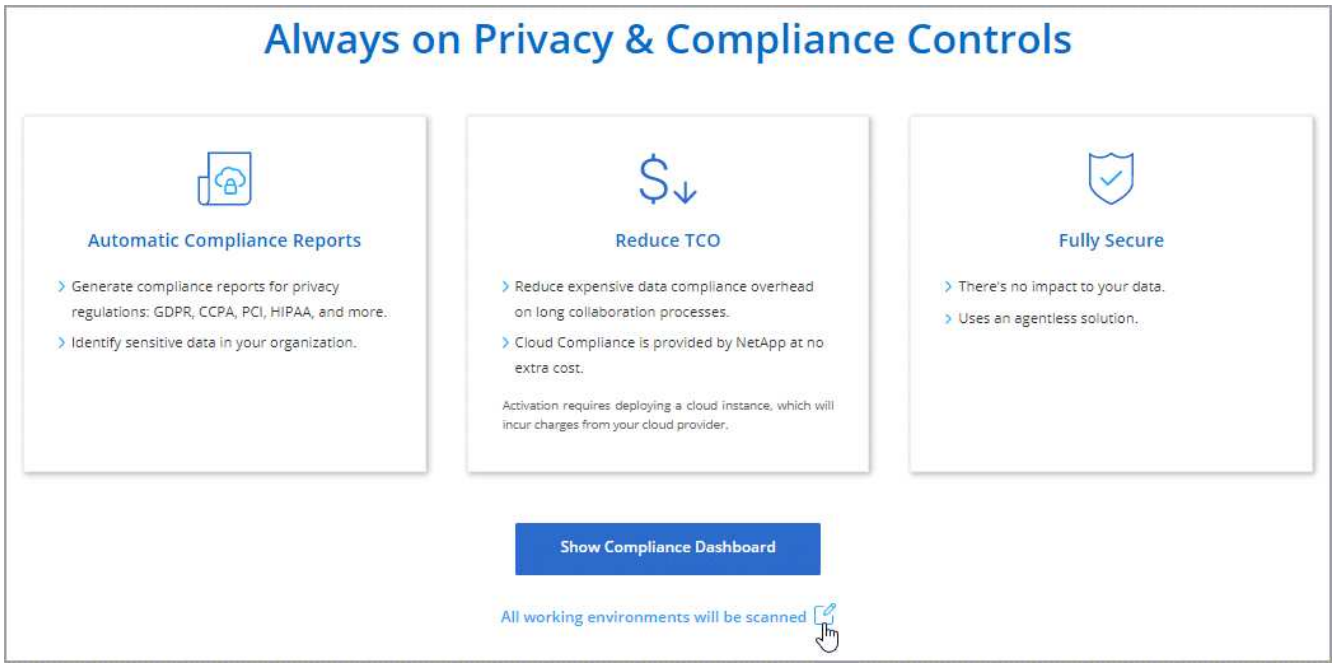
Abilita la conformità al cloud sui tuoi sistemi Cloud Volumes ONTAP esistenti dalla scheda **Compliance** di Cloud Manager.

Un'altra opzione consiste nell'attivare la conformità cloud dalla scheda **ambienti di lavoro** selezionando ciascun ambiente di lavoro singolarmente. Il completamento di questo processo richiede più tempo, a meno che non si disponga di un solo sistema.

Passaggi per ambienti di lavoro multipli

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.
2. Se si desidera attivare la conformità cloud su ambienti di lavoro specifici, fare clic sull'icona di modifica.

   In caso contrario, Cloud Manager è impostato per abilitare la conformità al cloud in tutti gli ambienti di lavoro ai quali si ha accesso.

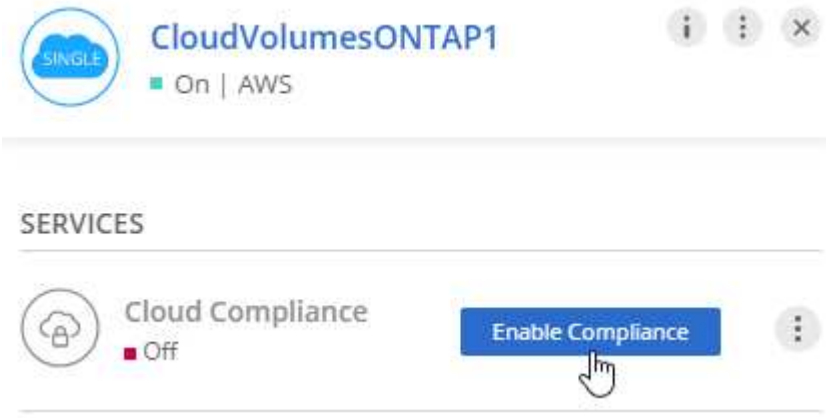


3. Fare clic su **Mostra dashboard conformità**.

Passaggi per un singolo ambiente di lavoro

1. Nella parte superiore di Cloud Manager, fare clic su **Working Environments** (ambienti di lavoro).
2. Selezionare un ambiente di lavoro.

3. Nel riquadro a destra, fare clic su **Enable Compliance** (attiva conformità).



Risultato

Se questa è la prima volta che hai attivato la conformità al cloud, Cloud Manager implementa l'istanza di conformità al cloud nel tuo cloud provider.

Cloud Compliance inizia la scansione dei dati in ogni ambiente di lavoro. I dati saranno disponibili nella dashboard Compliance non appena la Cloud Compliance terminerà le scansioni iniziali. Il tempo necessario dipende dalla quantità di dati, che potrebbe essere di pochi minuti o ore.

Verificare che la conformità del cloud abbia accesso ai volumi

Assicurati che la conformità al cloud possa accedere ai volumi su Cloud Volumes ONTAP controllando il networking, i gruppi di sicurezza e le policy di esportazione. È necessario fornire le credenziali CIFS per la conformità al cloud in modo che possa accedere ai volumi CIFS.

Fasi

1. Assicurarsi che sia presente una connessione di rete tra l'istanza di conformità cloud e ciascuna subnet Cloud Volumes ONTAP.

   Cloud Manager implementa l'istanza di conformità cloud nello stesso VPC o VNET del primo sistema Cloud Volumes ONTAP nella richiesta. Pertanto, questo passaggio è importante se alcuni sistemi Cloud Volumes ONTAP si trovano in sottoreti o reti virtuali diverse.

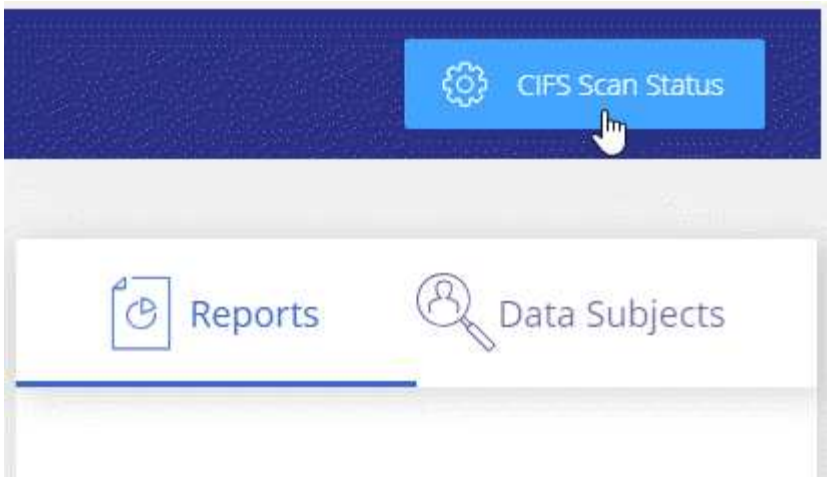
2. Assicurarsi che il gruppo di sicurezza per Cloud Volumes ONTAP consenta il traffico in entrata dall'istanza di conformità cloud.

   È possibile aprire il gruppo di sicurezza per il traffico dall'indirizzo IP dell'istanza Cloud Compliance oppure aprire il gruppo di sicurezza per tutto il traffico dall'interno della rete virtuale.

3. Assicurarsi che le policy di esportazione dei volumi NFS includano l'indirizzo IP dell'istanza Cloud Compliance in modo che possa accedere ai dati di ciascun volume.
4. Se si utilizza CIFS, fornire la conformità cloud con le credenziali Active Directory in modo che possa eseguire la scansione dei volumi CIFS.

   a. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.

   b. In alto a destra, fare clic su **CIFS Scan Status** (Stato scansione CIFS).



c. Per ciascun sistema Cloud Volumes ONTAP, fare clic su **Modifica credenziali CIFS** e immettere il nome utente e la password necessari per accedere ai volumi CIFS nel sistema.

   Le credenziali possono essere di sola lettura, ma fornire credenziali di amministratore garantisce che Cloud Compliance possa leggere tutti i dati che richiedono autorizzazioni elevate. Le credenziali vengono memorizzate nell'istanza Cloud Compliance.

   Dopo aver immesso le credenziali, viene visualizzato un messaggio che indica che tutti i volumi CIFS sono stati autenticati correttamente.

Verificare che Cloud Manager possa accedere alla conformità cloud

Assicurati la connettività tra Cloud Manager e Cloud Compliance per visualizzare le informazioni sulla conformità rilevate dalla Cloud Compliance.

Fasi

1. Assicurarsi che il gruppo di sicurezza per Cloud Manager consenta il traffico in entrata e in uscita sulla porta 80 da e verso l'istanza Cloud Compliance.

   Questa connessione consente di visualizzare le informazioni nella scheda Compliance.

2. Se la rete AWS non utilizza un NAT o un proxy per l'accesso a Internet, modificare il gruppo di sicurezza per Cloud Manager in modo da consentire il traffico in entrata sulla porta TCP 3128 dall'istanza Cloud Compliance.

   Ciò è necessario perché l'istanza Cloud Compliance utilizza Cloud Manager come proxy per accedere a Internet.

Questa porta è aperta per impostazione predefinita in tutte le nuove istanze di Cloud Manager, a partire dalla versione 3.7.5. Non è aperto sulle istanze di Cloud Manager create prima di quella versione.

Ottenere visibilità e controllo sui dati privati

Ottieni il controllo dei tuoi dati privati visualizzando i dettagli relativi ai dati personali e ai dati personali sensibili della tua organizzazione. Puoi anche ottenere visibilità esaminando le categorie e i tipi di file che Cloud Compliance ha trovato nei tuoi dati.

Dati personali

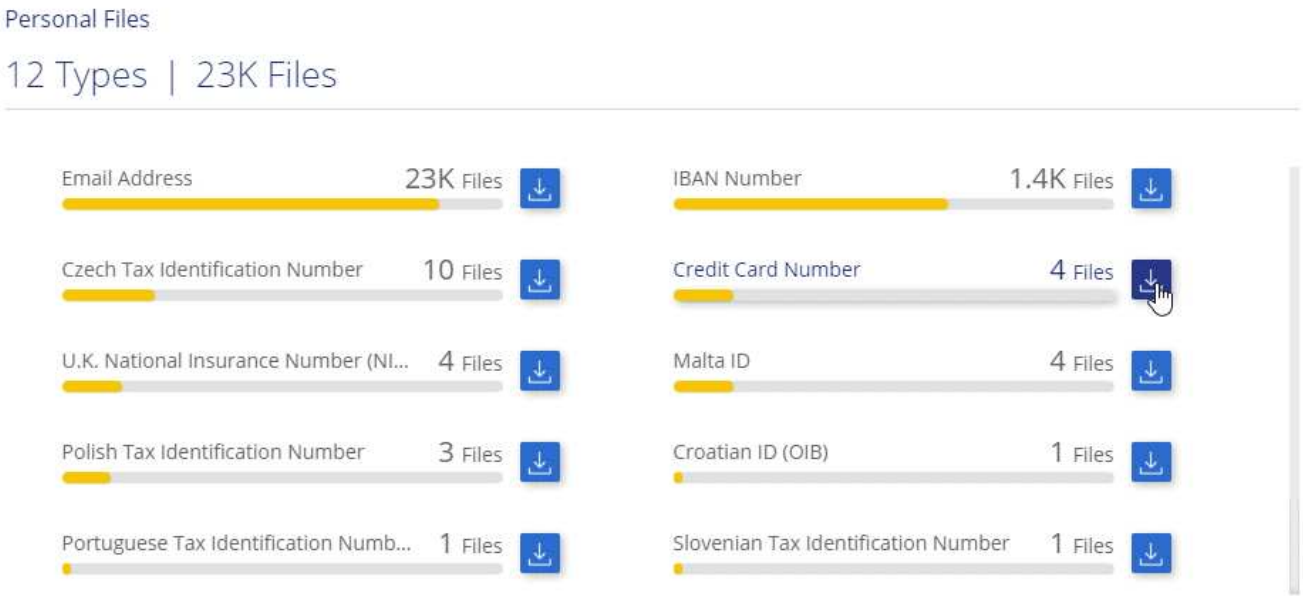
Cloud Compliance identifica automaticamente parole, stringhe e modelli specifici (Regex) all'interno dei dati. Ad esempio, informazioni di identificazione personale (PII), numeri di carta di credito, numeri di previdenza sociale, numeri di conto bancario e altro ancora. Consulta l'elenco completo.

Per alcuni tipi di dati personali, Cloud Compliance utilizza *Proximity Validation* per validarne i risultati. La convalida avviene cercando una o più parole chiave predefinite in prossimità dei dati personali trovati. Ad esempio, Cloud Compliance identifica un Numero di previdenza sociale (SSN) come SSN se viene visualizzato un termine di prossimità, ad esempio *SSN* o *social Security*. L'elenco seguente Mostra quando Cloud Compliance utilizza la convalida di prossimità.

Visualizzazione di file contenenti dati personali

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.
2. Scaricare i dettagli di uno dei 2 tipi di file principali direttamente dalla schermata principale oppure fare clic su **Visualizza tutto** e quindi scaricare l'elenco dei tipi di dati personali trovati.



Tipi di dati personali

I dati personali contenuti nei file possono essere dati personali di carattere generale o identificativi nazionali. La terza colonna indica se la conformità al cloud utilizza convalida della prossimità per convalidare i risultati per l'identificatore.

Tipo	Identificatore	Convalida della prossimità?
Generale	Indirizzo e-mail	No
	Numero della carta di credito	No
	Numero IBAN (International Bank account Number)	No
	Indirizzo IP	Sì

Tipo	Identificatore	Convalida della prossimità?
Identificatori nazionali	ID belga (numero nazionale)	Sì
	ID bulgaro (numero civile unificato)	Sì
	Codice fiscale di Cipro (TIC)	Sì
	Codice fiscale danese (CPR)	Sì
	ID estone (Isikukood)	Sì
	ID finlandese (henkilötunnus)	Sì
	Francese Tax Identification Number (SPI)	Sì
	Codice fiscale tedesco (Steuerliche Identifikationsnummer)	Sì
	Codice fiscale ungherese (Adóazonosító jel)	Sì
	Irish ID (PPS) (ID irlandese)	Sì
	ID Israeliano	Sì
	ID italiano (Codice fiscale)	Sì
	Codice fiscale lettone	Sì
	Lituano ID (Asmens kodas)	Sì
	Lussemburgo ID	Sì
	ID Malta	Sì
	ID Paesi Bassi (BSN)	Sì
	Codice fiscale polacco	Sì
	Portoghese Tax Identification Number (NIF)	Sì
	Codice fiscale rumeno	Sì
	Numero di identificazione fiscale slovacco	Sì
	Codice fiscale sloveno	Sì
	ID sudafricano	Sì
	Codice fiscale spagnolo	Sì
	Codice fiscale svedese	Sì
	REGNO UNITO NINO (National Insurance Number)	Sì
	Numero di previdenza sociale (SSN) USA	Sì

Dati personali sensibili

Cloud Compliance identifica automaticamente tipi speciali di informazioni personali sensibili, come definito dalle normative sulla privacy, ad esempio "articoli 9 e 10 del GDPR". Ad esempio, informazioni relative alla salute, all'origine etnica o all'orientamento sessuale di una persona. Consulta l'elenco completo.

Cloud Compliance utilizza l'intelligenza artificiale (ai), l'elaborazione del linguaggio naturale (NLP), l'apprendimento automatico (ML) e il calcolo cognitivo (CC) per comprendere il significato dei contenuti che

scansiona al fine di estrarre le entità e classificarle di conseguenza.

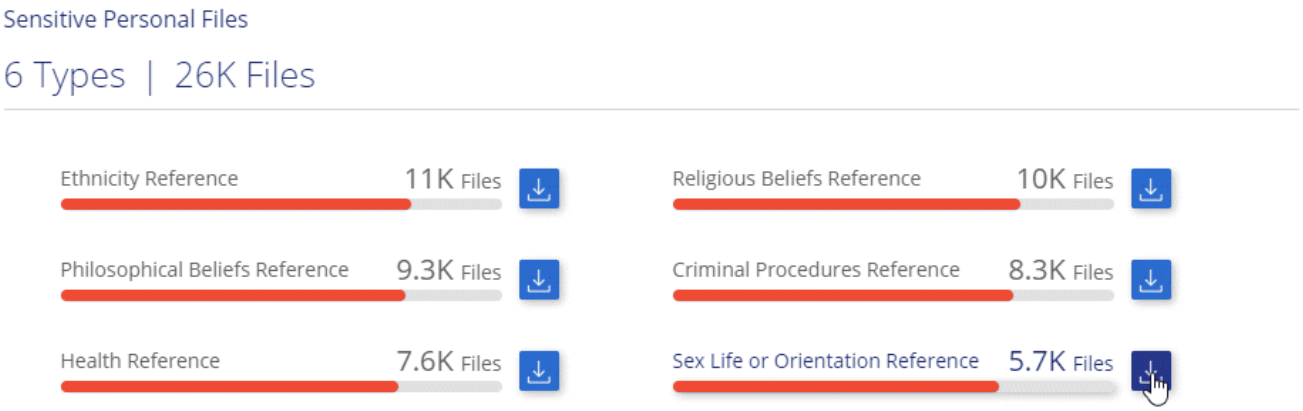
Ad esempio, una categoria di dati GDPR sensibili è l'origine etnica. Grazie alle sue capacità di NLP, Cloud Compliance è in grado di distinguere la differenza tra una frase con la dicitura "George is Mexican" (che indica i dati sensibili come specificato nell'articolo 9 del GDPR) e "George is Eating Mexican Food" (George is Eating Mexican Food).

Quando si esegue la scansione di dati personali sensibili, è supportata solo l'inglese. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Visualizzazione di file contenenti dati personali sensibili

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.
2. Scaricare i dettagli di uno dei 2 tipi di file principali direttamente dalla schermata principale oppure fare clic su **View All** (Visualizza tutto) e quindi scaricare l'elenco dei tipi di dati personali sensibili trovati.



Tipi di dati personali sensibili

I dati personali sensibili che Cloud Compliance può trovare nei file includono:

Riferimento alle procedure penali
Dati relativi alle condanne e ai reati penali di una persona fisica.

Riferimento di etnia
Dati relativi alla razza o all'origine etnica di una persona fisica.

Riferimento di salute
Dati relativi alla salute di una persona fisica.

Riferimento alle credenze filosofiche
Dati relativi alle convinzioni filosofiche di una persona naturale.

Riferimenti alle credenze religiose
Dati relativi alle convinzioni religiose di una persona fisica.

Sex Life o orientamento di riferimento

Dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica.

Categorie

Cloud Compliance prende i dati sottoposti a scansione e li divide in diversi tipi di categorie. Le categorie sono argomenti basati sull'analisi ai del contenuto e dei metadati di ciascun file. Vedere l'elenco delle categorie.

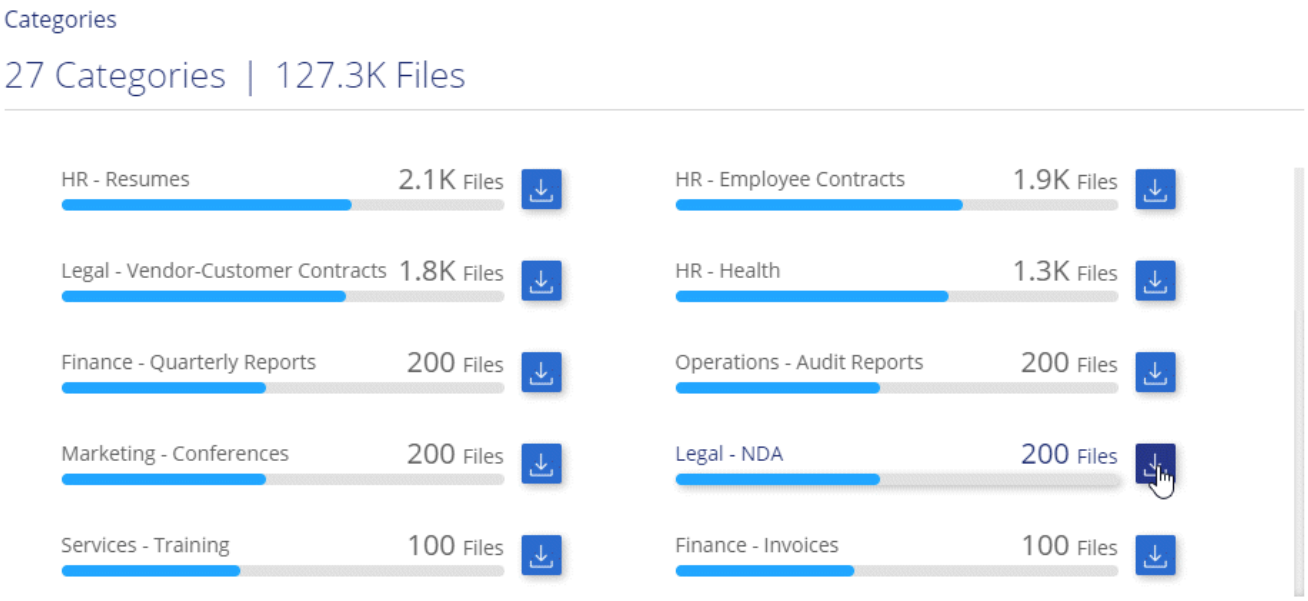
Le categorie possono aiutarti a capire cosa accade con i tuoi dati mostrando il tipo di informazioni di cui disponi. Ad esempio, una categoria come i curriculum o i contratti dei dipendenti può includere dati sensibili. Quando si scarica il report CSV, i contratti dei dipendenti potrebbero essere memorizzati in una posizione non sicura. A questo punto, è possibile correggere il problema.

Per le categorie è supportato solo l'inglese. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Visualizzazione dei file in base alle categorie

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.
2. Scarica i dettagli di uno dei primi 4 tipi di file direttamente dalla schermata principale oppure fai clic su **Visualizza tutto** e scarica l'elenco per qualsiasi categoria.



Tipi di categorie

La conformità al cloud classifica i tuoi dati nel modo seguente:

Finanza

- Bilanci
- Ordini di acquisto
- Fatture

- Report trimestrali

FC

- Controllo in background
- Piani di compensazione
- Contratti con i dipendenti
- Analisi dei dipendenti
- Salute
- Riprende

Legale

- NDA
- Contratti fornitore-cliente

Marketing

- Campagne
- Conferenze

Operazioni

- Report di audit

Vendite

- Ordini di vendita

Servizi

- RFI
- RFP
- Formazione

Supporto

- Reclami e biglietti

Altro

- Archiviare i file
- Audio
- File CAD
- Codice
- Eseguibili
- Immagini

Tipi di file

Cloud Compliance prende i dati sottoposti a scansione e li suddivide in base al tipo di file. Cloud Compliance consente di visualizzare tutti i tipi di file trovati nelle scansioni.

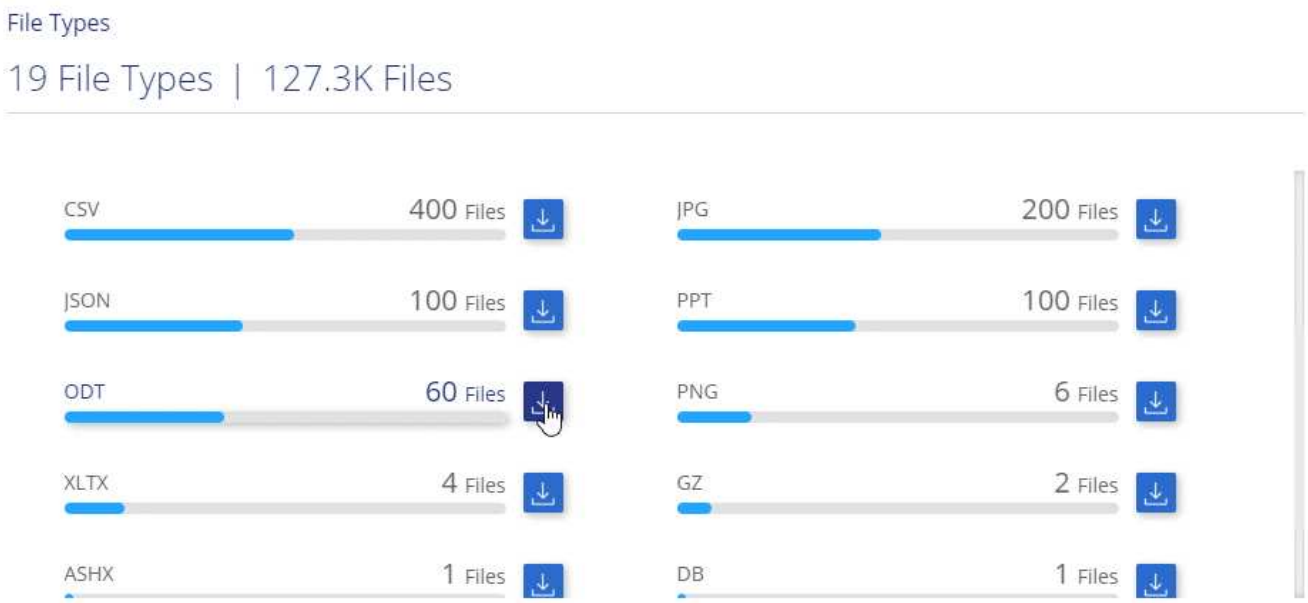
La revisione dei tipi di file consente di controllare i dati sensibili, poiché alcuni tipi di file potrebbero non essere

memorizzati correttamente. Ad esempio, è possibile memorizzare file CAD che includono informazioni molto sensibili sull'organizzazione. Se non sono protetti, è possibile assumere il controllo dei dati sensibili limitando le autorizzazioni o spostando i file in un'altra posizione.

Visualizzazione dei tipi di file

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.
2. Scaricare i dettagli di uno dei 4 tipi di file principali direttamente dalla schermata principale oppure fare clic su **View All** (Visualizza tutto) e quindi scaricare l'elenco per qualsiasi tipo di file.



Accuratezza delle informazioni rilevate

NetApp non può garantire una precisione del 100% dei dati personali e dei dati personali sensibili identificati dalla Cloud Compliance. È sempre necessario convalidare le informazioni esaminando i dati.

In base ai nostri test, la tabella seguente mostra l'accuratezza delle informazioni rilevate dalla Cloud Compliance. Lo suddivideremo per *precisione* e *richiamo*:

Precisione

La probabilità che ciò che trova Cloud Compliance sia stata identificata correttamente. Ad esempio, un tasso di precisione del 90% per i dati personali significa che 9 file su 10 identificati come contenenti informazioni personali contengono effettivamente informazioni personali. 1 file su 10 sarebbe un falso positivo.

Ricorda

La probabilità che la conformità cloud trovi ciò che dovrebbe. Ad esempio, un tasso di richiamo del 70% per i dati personali significa che Cloud Compliance è in grado di identificare 7 file su 10 che contengono effettivamente informazioni personali nella tua organizzazione. La conformità al cloud perderebbe il 30% dei dati e non verrà visualizzata nella dashboard.

Cloud Compliance è in una release di disponibilità controllata e stiamo costantemente migliorando la precisione dei nostri risultati. Tali miglioramenti saranno automaticamente disponibili nelle future release di Cloud Compliance.

Tipo	Precisione	Ricorda
Dati personali - Generale	90%-95%	60%-80%
Dati personali - identificatori del Paese	30%-60%	40%-60%
Dati personali sensibili	80%-95%	20%-30%
Categorie	90%-97%	60%-80%

Contenuto di ciascun report elenco file (file CSV)

La dashboard consente di scaricare elenchi di file (in formato CSV) che includono dettagli sui file identificati. Se sono presenti più di 10,000 risultati, nell'elenco vengono visualizzati solo i primi 10,000 risultati (il supporto per altri verrà aggiunto in seguito).

Ciascun elenco di file include le seguenti informazioni:

- Nome del file
- Tipo di ubicazione
- Posizione
- Percorso del file
- Tipo di file
- Categoria
- Informazioni personali
- Informazioni personali sensibili
- Data di rilevamento dell'eliminazione

  Una data di rilevamento dell'eliminazione identifica la data in cui il file è stato cancellato o spostato. In questo modo è possibile identificare quando sono stati spostati file sensibili. I file cancellati non fanno parte del numero di file visualizzato nella dashboard. I file vengono visualizzati solo nei report CSV.

Visualizzazione del report sulla valutazione dei rischi per la privacy

Il report sulla valutazione dei rischi per la privacy fornisce una panoramica dello stato di rischio per la privacy della tua organizzazione, come richiesto dalle normative sulla privacy come GDPR e CCPA.

NetApp non può garantire una precisione del 100% dei dati personali e dei dati personali sensibili identificati dalla Cloud Compliance. È sempre necessario convalidare le informazioni esaminando i dati.

Il report contiene le seguenti informazioni:

Stato di compliance

Un punteggio di severità (vedi sotto per ulteriori dettagli) e la distribuzione dei dati, sia che si tratti di dati non sensibili, personali o sensibili.

Panoramica della valutazione

Analisi dei tipi di dati personali rilevati, nonché delle categorie di dati.

Argomenti trattati in questa valutazione

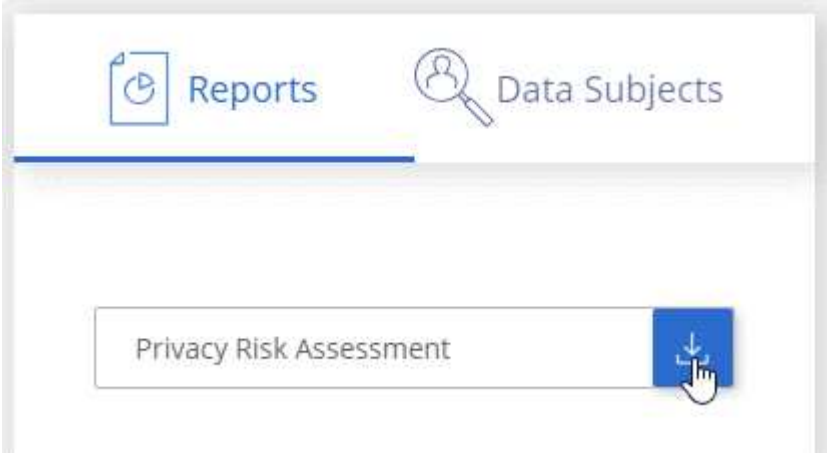
Il numero di persone per località per le quali sono stati trovati identificatori nazionali.

Generazione del report sulla valutazione dei rischi per la privacy

Accedere alla scheda Compliance per generare il report.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.
2. In **Report**, fare clic sull'icona di download accanto a **Privacy Risk Assessment**.



Risultato

Cloud Compliance genera un report PDF che puoi rivedere e inviare ad altri gruppi in base alle esigenze.

Punteggio di severità

Cloud Compliance calcola il punteggio di severità per il report di valutazione dei rischi per la privacy sulla base di tre variabili:

- La percentuale di dati personali su tutti i dati.
- La percentuale di dati personali sensibili rispetto a tutti i dati.
- La percentuale di file che includono soggetti dati, determinata da identificatori nazionali come ID nazionali, numeri di previdenza sociale e numeri di identificazione fiscale.

La logica utilizzata per determinare il punteggio è la seguente:

Punteggio di severità	Logica
0	Tutte e tre le variabili sono esattamente 0%
1	Una delle variabili è maggiore dello 0%
2	Una delle variabili è maggiore del 3%
3	Due delle variabili sono maggiori del 3%

Punteggio di severità	Logica
4	Tre delle variabili sono maggiori del 3%
5	Una delle variabili è maggiore del 6%
6	Due delle variabili sono più grandi del 6%
7	Tre delle variabili sono più grandi del 6%
8	Una delle variabili è maggiore del 15%
9	Due delle variabili sono più grandi del 15%
10	Tre delle variabili sono più grandi del 15%

Risposta a una richiesta di accesso soggetto a dati

Rispondere a una richiesta di accesso soggetto a dati (DSAR) cercando il nome completo o l'identificatore noto di un soggetto (ad esempio un indirizzo e-mail) e scaricando un report. Il report è stato progettato per aiutare l'organizzazione a rispettare il GDPR o leggi simili sulla privacy dei dati.

NetApp non può garantire una precisione del 100% dei dati personali e dei dati personali sensibili identificati dalla Cloud Compliance. È sempre necessario convalidare le informazioni esaminando i dati.

Che cos'è una richiesta di accesso ai dati?

Le normative sulla privacy, come il GDPR europeo, concedono ai soggetti interessati (come clienti o dipendenti) il diritto di accedere ai propri dati personali. Quando un soggetto interessato richiede queste informazioni, queste vengono denominate DSAR (data subject access request). Le organizzazioni devono rispondere a queste richieste "senza ritardi indebito" e al più tardi entro un mese dalla ricezione.

In che modo la Cloud Compliance può aiutarti a rispondere a una DSAR?

Quando esegui una ricerca dell'oggetto dati, Cloud Compliance trova tutti i file che contengono il nome o l'identificatore della persona. Cloud Compliance verifica i dati pre-indicizzati più recenti per il nome o l'identificatore. Non avvia una nuova scansione.

Una volta completata la ricerca, è possibile scaricare l'elenco dei file o un report Data Subject Access Request. Il report aggrega le informazioni dei dati e le inserisce in termini legali che è possibile inviare alla persona.

Ricerca di dati e download di report

Cercare il nome completo o l'identificatore noto del soggetto interessato, quindi scaricare un report elenco file o un report DSAR. È possibile eseguire la ricerca in base a. "qualsiasi tipo di informazione personale".

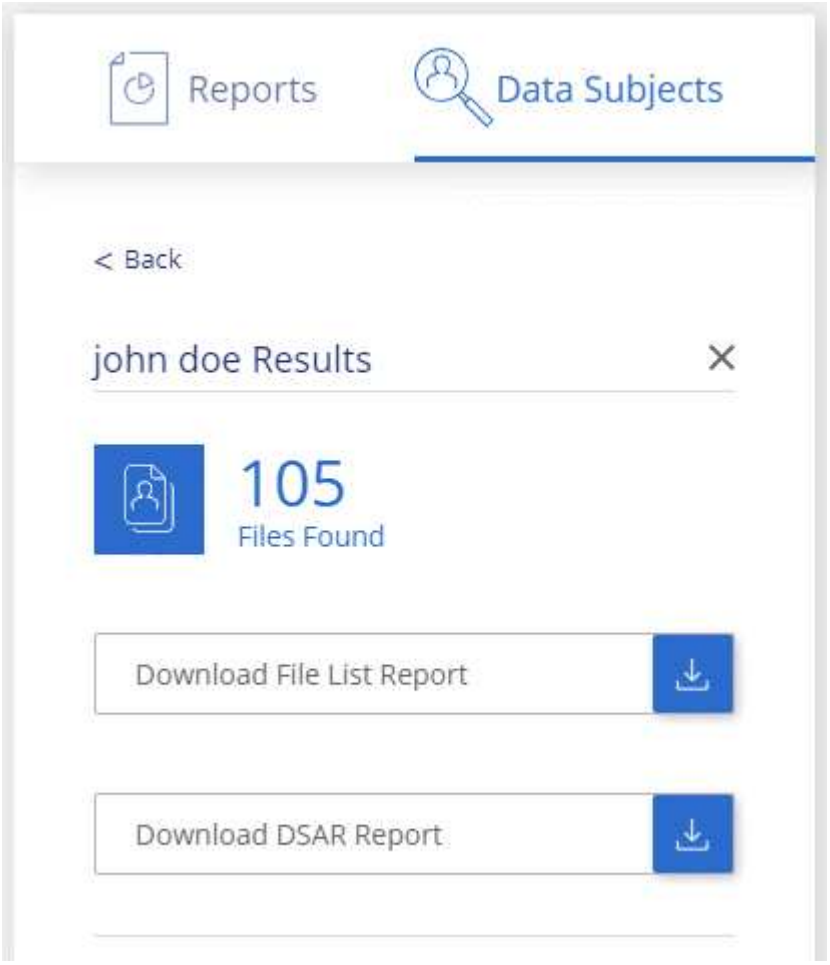
Quando si ricercano i nomi dei soggetti dati, è supportato solo l'inglese. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.

2. Fare clic su **Data subjects**.
3. Cercare il nome completo o l'identificativo noto dell'interessato.

   Ecco un esempio che mostra una ricerca per il nome *john Doe*:



4. Scegliere una delle opzioni disponibili:
   - **Download file List Report**: Un elenco dei file che contengono informazioni sull'oggetto dei dati.

     Se sono presenti più di 10,000 risultati, nel report vengono visualizzati solo i primi 10,000 risultati (il supporto per altri verrà aggiunto in seguito).

   - **Download del report DSAR**: Una risposta formale alla richiesta di accesso che è possibile inviare al soggetto interessato. Questo report contiene informazioni generate automaticamente in base ai dati rilevati dalla Cloud Compliance nell'oggetto dei dati ed è progettato per essere utilizzato come modello. Completare il modulo e esaminarlo internamente prima di inviarlo al soggetto interessato.

Disattivazione della conformità al cloud

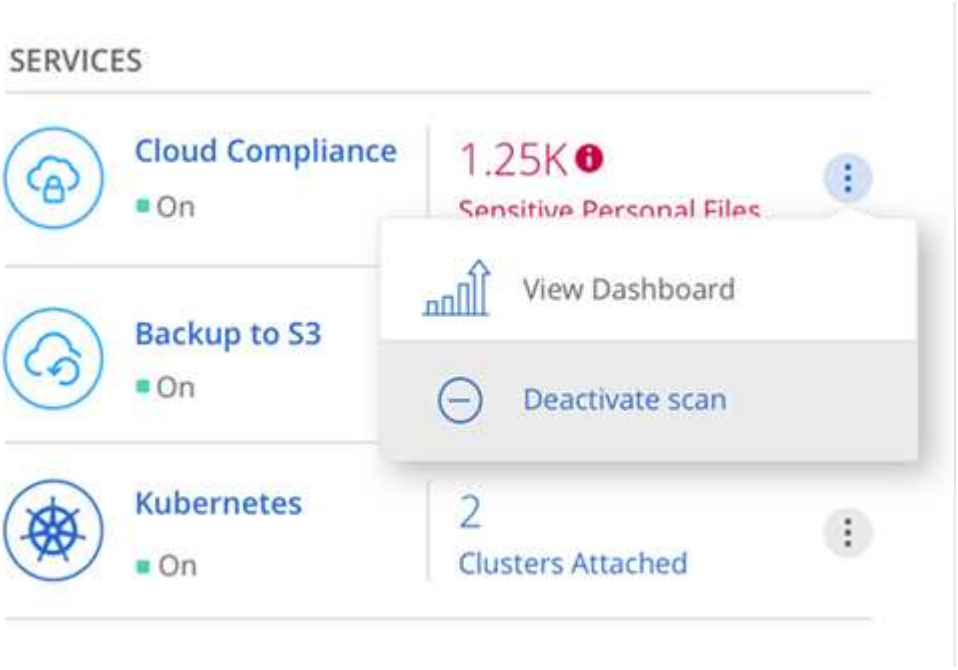
Se necessario, puoi impedire alla conformità cloud di eseguire la scansione di uno o più ambienti di lavoro. Puoi anche eliminare l'istanza di conformità cloud se non desideri più utilizzare la conformità cloud con i tuoi sistemi Cloud Volumes ONTAP.

Disattivazione delle scansioni di compliance per un ambiente di lavoro

Quando si disattivano le scansioni, Cloud Compliance non esegue più la scansione dei dati sul sistema e rimuove le informazioni indicizzate sulla compliance dall'istanza Cloud Compliance (i dati dell'ambiente di lavoro stesso non vengono cancellati).

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Working Environments** (ambienti di lavoro).
2. Selezionare l'ambiente di lavoro.
3. Nel pannello di destra, fare clic sull'icona dell'azione relativa al servizio Cloud Compliance e selezionare **Disattiva scansione**.



Eliminazione dell'istanza di Cloud Compliance

Se non si desidera più utilizzare la conformità cloud con Cloud Volumes ONTAP, è possibile eliminare l'istanza di conformità cloud. L'eliminazione dell'istanza comporta anche l'eliminazione dei dischi associati in cui risiedono i dati indicizzati.

Fase

1. Accedere alla console del provider di servizi cloud ed eliminare l'istanza Cloud Compliance.

   L'istanza è denominata *CloudCompliance* con un hash generato (UUID) concatenato ad essa. Ad esempio: *CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*

Domande frequenti sulla conformità al cloud

Queste FAQ possono essere utili se stai cercando una risposta rapida a una domanda.

Che cos'è la conformità al cloud?

Cloud Compliance è una nuova offerta cloud di NetApp. Utilizzando la tecnologia basata sull'intelligenza artificiale (ai), la conformità al cloud aiuta le organizzazioni a comprendere il contesto dei dati e a identificare i dati sensibili nei sistemi Cloud Volumes ONTAP ospitati in AWS o Azure.

Cloud Compliance offre parametri predefiniti (ad esempio tipi e categorie di informazioni sensibili) per soddisfare le nuove normative sulla conformità dei dati per la privacy e la sensibilità dei dati, come GDPR, CCPA e altro ancora.

Perché dovrei utilizzare Cloud Compliance?

La conformità al cloud può aiutarti con i dati per aiutarti a:

- Rispettare le normative sulla privacy e sulla conformità dei dati.
- Rispettare le policy di conservazione dei dati.
- Individuare e creare report su dati specifici in risposta a soggetti interessati, come richiesto dal GDPR, dal CCPA e da altre normative sulla privacy dei dati.

Quali sono i casi di utilizzo più comuni per la conformità al cloud?

- Identificare le informazioni personali identificabili (PII).
- Identificare un ampio ambito di informazioni sensibili come richiesto dalle normative sulla privacy GDPR e CCPA.
- Rispettare le nuove e future normative sulla privacy dei dati.

"Scopri di più sui casi di utilizzo per la conformità al cloud".

Quali tipi di dati è possibile sottoporre a scansione con la conformità al cloud?

Cloud Compliance supporta la scansione di dati non strutturati su protocolli NFS e CIFS. Attualmente, la conformità al cloud esegue la scansione dei dati gestiti da Cloud Volumes ONTAP.

"Scopri come funzionano le scansioni".

Quali cloud provider sono supportati?

Cloud Compliance opera come parte di Cloud Manager e attualmente supporta AWS e Azure. In questo modo, la tua organizzazione potrà ottenere una visibilità unificata della privacy tra diversi cloud provider. Il supporto per Google Cloud Platform (GCP) verrà aggiunto a breve.

Come posso accedere alla conformità cloud?

La conformità al cloud viene gestita e gestita tramite Cloud Manager. Puoi accedere alle funzionalità Cloud Compliance dalla scheda **Compliance** di Cloud Manager.

Come funziona Cloud Compliance?

La conformità al cloud implementa un altro livello di intelligenza artificiale insieme al sistema Cloud Manager e alle istanze di Cloud Volumes ONTAP. Quindi, esegue la scansione dei dati su Cloud Volumes ONTAP e indicizza le informazioni rilevate.

"Scopri di più sul funzionamento della conformità al cloud".

Quanto costa la Cloud Compliance?

La conformità al cloud viene offerta come parte di Cloud Volumes ONTAP e non richiede costi aggiuntivi. In futuro potrebbero essere necessari costi aggiuntivi per le funzionalità personalizzate.

La conformità al cloud richiede l'implementazione di un'istanza nel tuo cloud provider, per la quale ti verrà addebitato il costo del tuo cloud provider.

Con quale frequenza la Cloud Compliance esegue la scansione dei miei dati?

I dati cambiano di frequente, pertanto la conformità del cloud esegue una scansione continua dei dati senza alcun impatto sui dati. Anche se la scansione iniziale dei dati potrebbe richiedere più tempo, le scansioni successive eseguono solo la scansione delle modifiche incrementali, riducendo i tempi di scansione del sistema.

"Scopri come funzionano le scansioni".

Cloud Compliance offre report?

Sì. Le informazioni offerte dalla Cloud Compliance possono essere rilevanti per gli altri stakeholder delle tue organizzazioni, pertanto ti consentiamo di generare report per condividere le informazioni.

Per la conformità al cloud sono disponibili i seguenti report:

Report sulla valutazione dei rischi per la privacy
: Fornisce informazioni sulla privacy dai dati e un punteggio di rischio per la privacy. "Scopri di più".

Report Data Subject Access Request
: Consente di estrarre un report di tutti i file che contengono informazioni relative al nome specifico o all'identificativo personale di un soggetto. "Scopri di più".

Report su un tipo di informazioni specifico
: Sono disponibili report che includono dettagli sui file identificati che contengono dati personali e dati personali sensibili. È inoltre possibile visualizzare i file suddivisi per categoria e tipo di file. "Scopri di più".

Quale tipo di istanza o macchina virtuale è richiesto per la conformità al cloud?

- In Azure, Cloud Compliance viene eseguito su una macchina virtuale Standard_D16s_v3 con un disco da 512 GB.
- In AWS, Cloud Compliance viene eseguito su un'istanza m5.4xLarge con un disco io1 da 500 GB.

  Nelle regioni in cui m5.4xlarge non è disponibile, Cloud Compliance viene eseguito su un'istanza m4.4xlarge.

"Scopri di più sul funzionamento della conformità al cloud".

Le prestazioni di scansione variano?

Le performance di scansione possono variare in base alla larghezza di banda della rete e alle dimensioni medie dei file nel tuo ambiente cloud.

Come posso abilitare la conformità al cloud?

Puoi abilitare la conformità al cloud quando crei un nuovo ambiente di lavoro. È possibile abilitarla negli ambienti di lavoro esistenti dalla scheda **Compliance** (solo alla prima attivazione) o selezionando un ambiente di lavoro specifico.

"Scopri come iniziare".

L'attivazione della conformità cloud comporta una scansione iniziale immediata. I risultati della compliance vengono visualizzati poco dopo.

Come si disattiva la conformità al cloud?

Dopo aver selezionato un singolo ambiente di lavoro, è possibile disattivare Cloud Compliance dalla pagina Working Environments (ambienti di lavoro).

"Scopri di più".

Per rimuovere completamente l'istanza di Cloud Compliance, puoi rimuovere manualmente l'istanza di Cloud Compliance dal portale del tuo cloud provider.

Cosa succede se il tiering dei dati è attivato su Cloud Volumes ONTAP?

Potresti voler abilitare la conformità al cloud su un sistema Cloud Volumes ONTAP che esegue il Tier dei dati cold sullo storage a oggetti. Se il tiering dei dati è attivato, Cloud Compliance esegue la scansione di tutti i dati presenti sui dischi e cold data tiered in storage a oggetti.

La scansione di compliance non riscalda i dati cold, ma rimane fredda e viene tierata per lo storage a oggetti.

Posso utilizzare la conformità al cloud per eseguire la scansione dello storage ONTAP on-premise?

No La conformità al cloud è attualmente disponibile come parte di Cloud Manager e supporta Cloud Volumes ONTAP. Stiamo pianificando di supportare la conformità al cloud con offerte cloud aggiuntive come Cloud Volumes Service e Azure NetApp Files.

Cloud Compliance può inviare notifiche alla mia organizzazione?

No, ma è possibile scaricare i report di stato che è possibile condividere internamente all'organizzazione.

Posso personalizzare il servizio in base alle esigenze della mia organizzazione?

La conformità al cloud offre informazioni pronte all'uso ai tuoi dati. Queste informazioni possono essere estratte e utilizzate per le esigenze della tua organizzazione.

Posso limitare le informazioni sulla conformità al cloud a utenti specifici?

Sì, la conformità del cloud è completamente integrata con Cloud Manager. Gli utenti di Cloud Manager possono visualizzare le informazioni solo per gli ambienti di lavoro che possono visualizzare in base ai privilegi dell'area di lavoro.

"Scopri di più".

Informazioni sul copyright

Informazioni sul marchio commerciale