Approfondimenti sulla privacy dei dati

Cloud Manager 3.8

NetApp
March 25, 2024

Sommario

Approfondimenti sulla privacy dei dati

Scopri di più sulla conformità al cloud

Cloud Compliance è un servizio di privacy e conformità dei dati per Cloud Manager che esegue la scansione di volumi, bucket Amazon S3 e database per identificare i dati personali e sensibili presenti in tali file. Utilizzando la tecnologia basata sull'intelligenza artificiale (ai), Cloud Compliance aiuta le organizzazioni a comprendere il contesto dei dati e a identificare i dati sensibili.

"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)

Ambienti di lavoro e origini dati supportati

Cloud Compliance può eseguire la scansione dei dati dai seguenti tipi di origini dati:

- Cloud Volumes ONTAP in AWS
- Cloud Volumes ONTAP in Azure
- Azure NetApp Files
- Amazon S3
- Database che risiedono ovunque (non è necessario che il database risieda in un ambiente di lavoro)

Nota: per Azure NetApp Files, la conformità del cloud può eseguire la scansione di tutti i volumi che si trovano nella stessa regione di Cloud Manager.

Costo

- Il costo per l'utilizzo della conformità cloud dipende dalla quantità di dati che si sta scansionando. A partire dal 7 ottobre 2020, i primi 1 TB di dati che Cloud Compliance analizza in uno spazio di lavoro di Cloud Manager sono gratuiti. Sono inclusi i dati provenienti da volumi Cloud Volumes ONTAP, volumi Azure NetApp Files, bucket Amazon S3 e schemi di database. Per continuare a eseguire la scansione dei dati dopo tale data, è necessario un abbonamento ad AWS o Azure Marketplace. Vedere "prezzi" per ulteriori informazioni.

  "Scopri come iscriverti".

- L'installazione di Cloud Compliance richiede l'implementazione di un'istanza di cloud, con conseguente addebito da parte del cloud provider in cui viene implementata. Vedere il tipo di istanza implementata per ciascun cloud provider

- La conformità al cloud richiede l'implementazione di un connettore. In molti casi hai già un connettore a causa di altri servizi e storage utilizzati in Cloud Manager. L'istanza del connettore comporta addebiti da parte del cloud provider in cui viene implementata. Vedere "tipo di istanza implementata per ciascun cloud provider".

Costi di trasferimento dei dati

I costi di trasferimento dei dati dipendono dalla configurazione. Se l'istanza di Cloud Compliance e l'origine dati si trovano nella stessa zona di disponibilità e nella stessa regione, non ci sono costi di trasferimento dei dati. Tuttavia, se l'origine dati, come un cluster Cloud Volumes ONTAP o un bucket S3, si trova in una _area o regione di disponibilità diversa, il tuo cloud provider addebiterà i costi di trasferimento dei dati. Per ulteriori informazioni, consulta i seguenti xref:./* "AWS: Prezzi Amazon EC2"
* "Microsoft Azure: Dettagli sui prezzi della larghezza di banda"

Come funziona Cloud Compliance

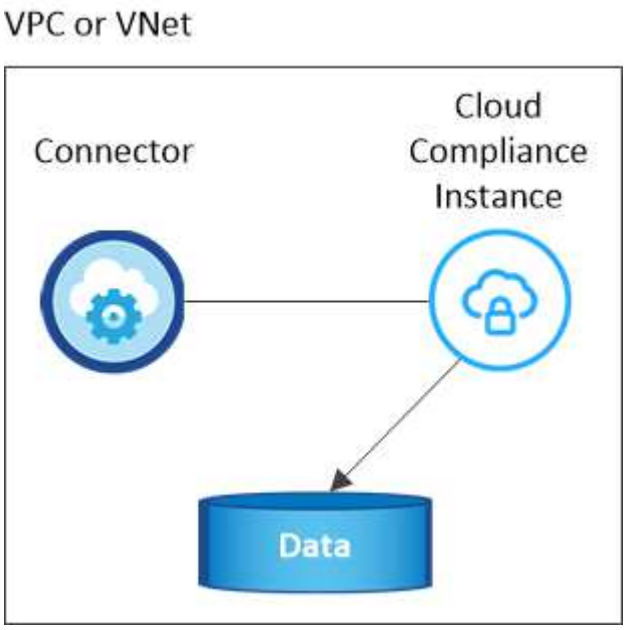
Ad alto livello, la conformità al cloud funziona come segue:

1. Implementa un'istanza di Cloud Compliance in Cloud Manager.
2. È possibile attivarlo su uno o più ambienti di lavoro o sui database.
3. Cloud Compliance esegue la scansione dei dati utilizzando un processo di apprendimento ai.
4. 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 si attiva Cloud Compliance, Cloud Manager implementa un'istanza di Cloud Compliance nella stessa sottorete del connettore. "Scopri di più sui connettori."

Se il connettore è installato on-premise, implementa l'istanza di conformità 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 GP2 da 500 GB.

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

> La modifica o il ridimensionamento del tipo di istanza/VM non è supportato. È necessario utilizzare le dimensioni fornite.

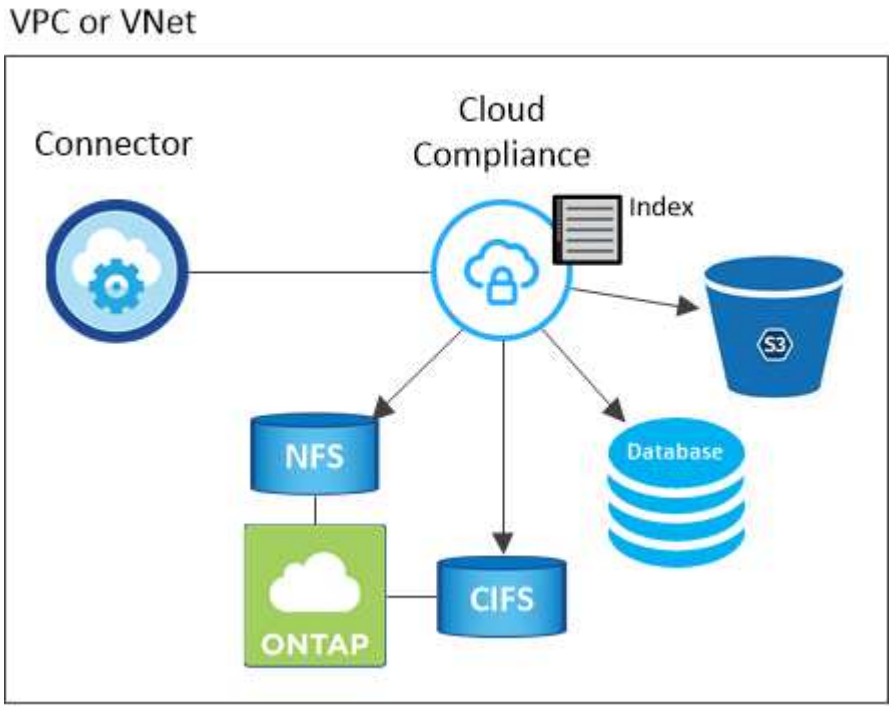
- L'istanza è denominata *CloudCompliance* con un hash generato (UUID) concatenato ad essa. Ad esempio: *CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*
- Viene implementata una sola istanza di Cloud Compliance per connettore.
- Gli aggiornamenti del software Cloud Compliance sono automatizzati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

> L'istanza deve rimanere sempre in esecuzione perché Cloud Compliance esegue continuamente la scansione dei dati.

Come funzionano le scansioni

Dopo aver attivato Cloud Compliance e selezionato i volumi, i bucket o gli schemi di database da sottoporre a scansione, inizia immediatamente la scansione dei dati per identificare i dati personali e sensibili. 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.

Cloud Compliance si connette ai dati 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.



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 in "livello del volume"in corrispondenza di "livello della benna"e in "livello di schema del database".

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 gruppo di sicurezza che abilita le connessioni HTTP in entrata dall'istanza del connettore.

Quando si utilizza Cloud Manager in modalità SaaS, la connessione a Cloud Manager viene servita su HTTPS e i dati privati inviati tra il browser e l'istanza di conformità cloud sono protetti con crittografia end-to-end, il che significa che NetApp e terze parti non possono leggerli.

Se per qualsiasi motivo è necessario utilizzare l'interfaccia utente locale invece dell'interfaccia utente SaaS, è comunque possibile "Accedere all'interfaccia utente locale".

Le regole in uscita sono completamente aperte. L'accesso a Internet è necessario per installare e aggiornare il software Cloud Compliance e per inviare metriche di utilizzo.

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

Accesso dell'utente alle informazioni di conformità

Il ruolo assegnato a ciascun utente offre diverse funzionalità all'interno di Cloud Manager e nell'ambito della Cloud Compliance:

- **Gli account Admins** possono gestire le impostazioni di conformità e visualizzare le informazioni di conformità per tutti gli ambienti di lavoro.
- **Workspace Admins** è in grado di gestire le impostazioni di conformità e 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.
- Gli utenti con il ruolo **Cloud Compliance Viewer** possono solo visualizzare le informazioni di conformità e generare report per i sistemi ai quali sono autorizzati ad accedere. Questi utenti non possono attivare/disattivare la scansione di volumi, bucket o schemi di database.

"Scopri di più sui ruoli di Cloud Manager" e come fare "aggiungere utenti con ruoli specifici".

Inizia subito

Implementazione della conformità al cloud

Completa alcuni passaggi per implementare l'istanza Cloud Compliance nel tuo spazio di lavoro Cloud Manager.

Avvio rapido

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

Creare un connettore

Se non si dispone già di un connettore, creare un connettore in Azure o AWS. Vedere "Creazione di un connettore in AWS" oppure "Creazione di un connettore in Azure".

Esaminare i prerequisiti

Assicurati che il tuo ambiente cloud sia in grado di soddisfare i prerequisiti, che includono 16 vCPU per l'istanza Cloud Compliance, accesso a Internet in uscita per l'istanza, connettività tra il connettore e Cloud Compliance tramite la porta 80 e altro ancora. Consulta l'elenco completo.

Implementazione della conformità al cloud

Avviare l'installazione guidata per implementare l'istanza Cloud Compliance in Cloud Manager.

Iscriviti al servizio Cloud Compliance

I primi 1 TB di dati che Cloud Compliance analizza in Cloud Manager sono gratuiti. Per continuare a eseguire la scansione dei dati dopo tale data, è necessario un abbonamento ad AWS o Azure Marketplace.

Creazione di un connettore

Se non si dispone già di un connettore, creare un connettore in Azure o AWS. Vedere "Creazione di un connettore in AWS" oppure "Creazione di un connettore in Azure". Nella maggior parte dei casi, è probabile che sia stato configurato un connettore prima di tentare di attivare la conformità cloud, perché la maggior parte di essi "Le funzionalità di Cloud Manager richiedono un connettore", ma in alcuni casi è necessario impostarne uno ora.

Esistono alcuni scenari in cui è necessario utilizzare un connettore in AWS o Azure per la conformità al cloud.

- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP nei bucket AWS o AWS S3, si utilizza un connettore in AWS.
- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in Azure o in Azure NetApp Files, si utilizza un connettore in Azure.
- È possibile eseguire la scansione dei database utilizzando uno dei due connettori.

Come puoi vedere, potrebbero esserci alcune situazioni in cui devi utilizzare "Connettori multipli".

> Se si intende eseguire la scansione di Azure NetApp Files, è necessario assicurarsi che l'implementazione venga eseguita nella stessa regione dei volumi che si desidera sottoporre a scansione.

Verifica dei prerequisiti

Prima di implementare Cloud Compliance, esaminare i seguenti prerequisiti per assicurarsi di disporre di una configurazione supportata.

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. Si noti che Cloud Manager implementa l'istanza Cloud Compliance nella stessa subnet del connettore.

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 https://auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
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://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.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.

Assicurarsi che Cloud Manager disponga delle autorizzazioni necessarie

Assicurarsi che Cloud Manager disponga delle autorizzazioni per implementare le risorse e creare gruppi di sicurezza per l'istanza di conformità cloud. Le autorizzazioni più recenti di Cloud Manager sono disponibili in "Le policy fornite da NetApp".

Controllare i limiti della vCPU

Assicurati che il limite vCPU del tuo provider cloud consenta l'implementazione di un'istanza con 16 core. È necessario verificare il limite vCPU per la famiglia di istanze pertinente nella regione in cui è in esecuzione Cloud Manager.

In AWS, la famiglia di istanze è *istanze standard on-Demand*. In Azure, la famiglia di istanze è *Standard DSv3 Family*.

Per ulteriori informazioni sui limiti delle vCPU, consulta la seguente pagina:

- "Documentazione AWS: Limiti di servizio Amazon EC2"
- "Documentazione di Azure: Quote vCPU delle macchine virtuali"

Assicurati che Cloud Manager possa accedere alla conformità al cloud

Garantire la connettività tra il connettore e l'istanza Cloud Compliance. Il gruppo di sicurezza per il connettore deve consentire il traffico in entrata e in uscita sulla porta 80 da e verso l'istanza Cloud Compliance.

Questa connessione consente l'implementazione dell'istanza Cloud Compliance e consente di visualizzare le informazioni nella scheda Compliance.

Impostare il rilevamento di Azure NetApp Files

Prima di eseguire la scansione dei volumi per Azure NetApp Files, "Cloud Manager deve essere configurato per rilevare la configurazione".

Assicurati di mantenere la conformità al cloud in esecuzione

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

Garantire la connettività del browser Web alla conformità al cloud

Dopo aver attivato Cloud Compliance, assicurarsi che gli utenti accedano all'interfaccia di Cloud Manager da un host che dispone di una connessione all'istanza di Cloud Compliance.

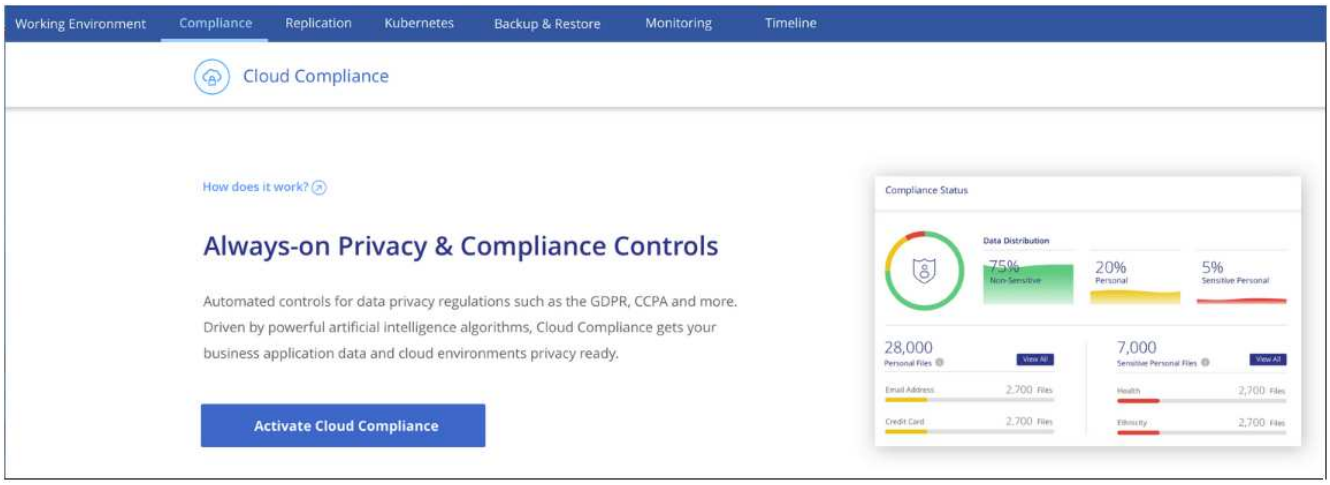
L'istanza Cloud Compliance utilizza un indirizzo IP privato per garantire che i dati indicizzati non siano accessibili a Internet. Di conseguenza, il browser Web utilizzato per accedere a Cloud Manager deve disporre di una connessione a tale indirizzo IP privato. Tale connessione può provenire da una 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.

Implementazione dell'istanza Cloud Compliance

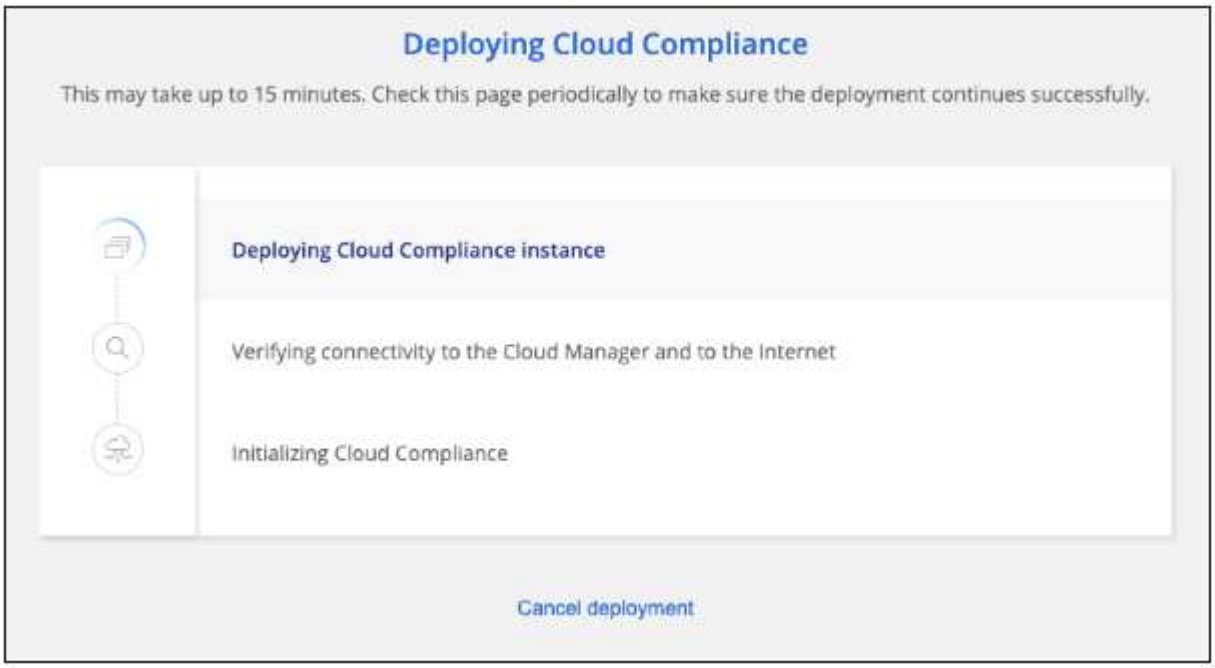
Implementa un'istanza di Cloud Compliance per ogni istanza di Cloud Manager.

Fasi

1. In Cloud Manager, fare clic su **Cloud Compliance**.
2. Fare clic su **Activate Cloud Compliance** (attiva conformità cloud) per avviare la procedura guidata di implementazione.



3. La procedura guidata visualizza lo stato di avanzamento durante le fasi di implementazione. In caso di problemi, il sistema si interrompe e richiede un input.



4. Una volta implementata l'istanza, fare clic su **Continue to Configuration** (continua alla configurazione) per accedere alla pagina *Scan Configuration* (Configurazione scansione).

Risultato

Cloud Manager implementa l'istanza Cloud Compliance nel tuo cloud provider.

Cosa c'è di nuovo

Dalla pagina Scan Configuration (Configurazione scansione) è possibile selezionare gli ambienti di lavoro, i volumi e i bucket che si desidera sottoporre a scansione per verificare la conformità. È inoltre possibile connettersi a un server di database per eseguire la scansione di schemi di database specifici. Attivare la conformità del cloud su una qualsiasi di queste origini dati.

Iscrizione al servizio Cloud Compliance

I primi 1 TB di dati che Cloud Compliance analizza in uno spazio di lavoro di Cloud Manager sono gratuiti. Per continuare a eseguire la scansione dei dati dopo tale data, è necessario un abbonamento ad AWS o Azure

Marketplace.

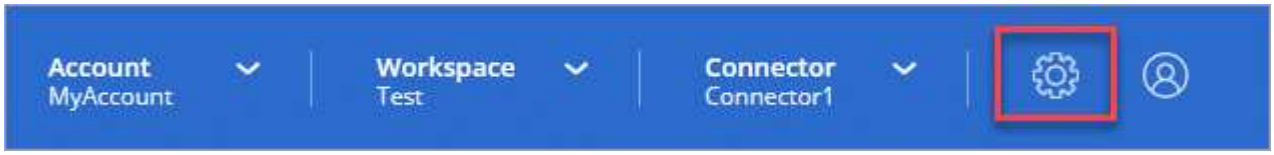
Puoi iscriverti in qualsiasi momento e non ti verrà addebitato alcun costo fino a quando la quantità di dati non supera 1 TB. Puoi sempre visualizzare la quantità totale di dati sottoposti a scansione dal Cloud Compliance Dashboard. Inoltre, il pulsante *Iscriviti ora* semplifica l'iscrizione quando sei pronto.

Nota: se la Cloud Compliance ti chiede di iscriverti, ma hai già un abbonamento Azure, probabilmente stai utilizzando il vecchio abbonamento **Cloud Manager** e devi passare al nuovo abbonamento **NetApp Cloud Manager**. VederePassaggio al nuovo piano NetApp Cloud Manager in Azure per ulteriori informazioni.

Fasi

Questi passaggi devono essere completati da un utente che ha il ruolo di *account Admin*.

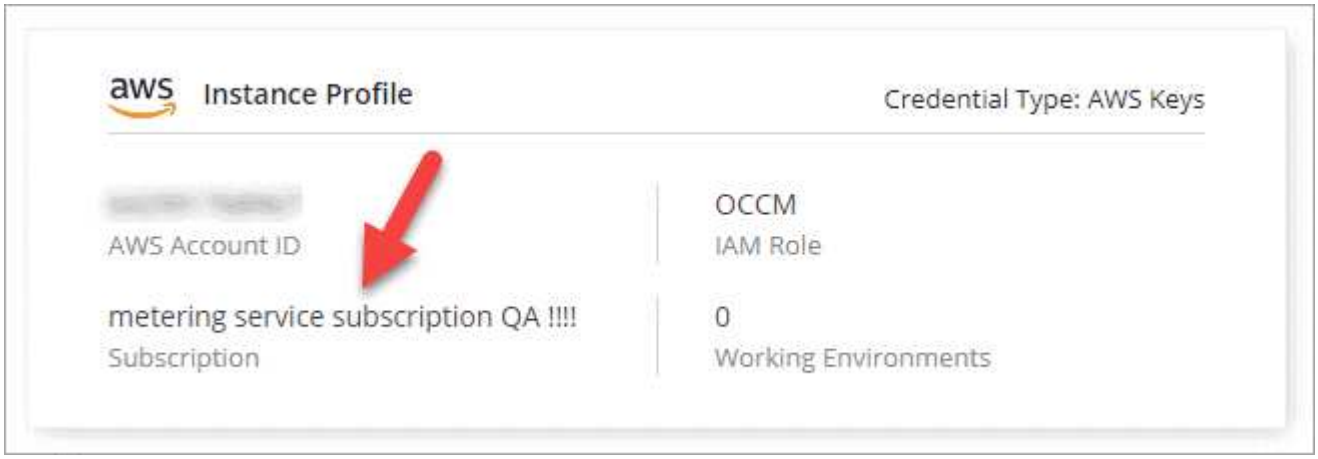
1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **credenziali**.



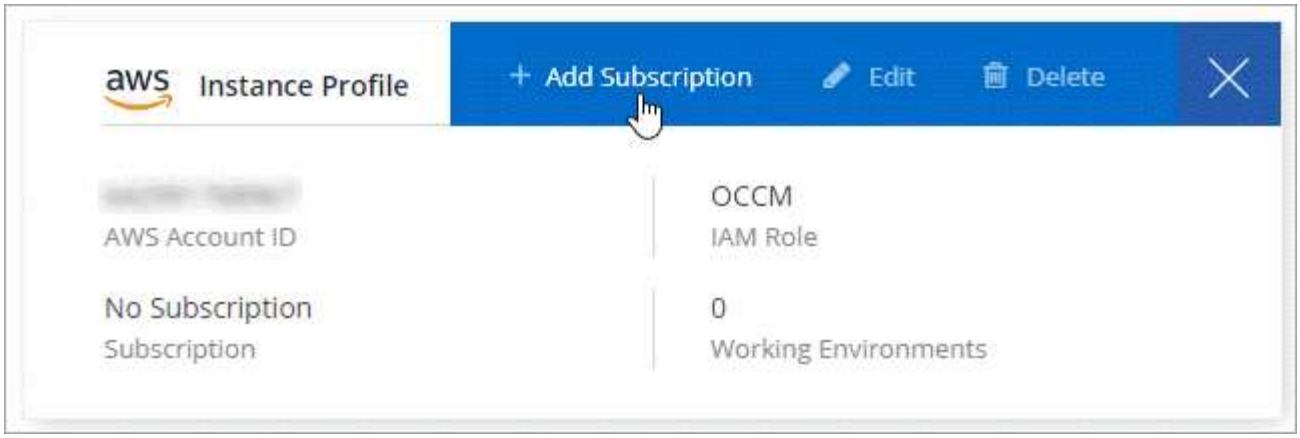
2. Trova le credenziali per AWS Instance Profile o Azure Managed Service Identity.

   L'abbonamento deve essere aggiunto al profilo istanza o all'identità del servizio gestito. La ricarica non funziona altrimenti.

   Se hai già un abbonamento, sei tutto impostato, non c'è altro da fare.



3. Se non disponi ancora di un abbonamento, passa il mouse sulle credenziali e fai clic sul menu delle azioni.
4. Fare clic su **Aggiungi abbonamento**.



5. Fare clic su **Add Subscription** (Aggiungi abbonamento), fare clic su **Continue** (continua) e seguire la procedura.

   Il video seguente mostra come associare un abbonamento Marketplace a un abbonamento AWS:

   ► https://docs.netapp.com/it-it/occm38//media/video_subscribing_aws.mp4 *(video)*

   Il video seguente mostra come associare un abbonamento Marketplace a un abbonamento Azure:

   ► https://docs.netapp.com/it-it/occm38//media/video_subscribing_azure.mp4 *(video)*

Passaggio al nuovo piano Cloud Manager in Azure

Cloud Compliance è stata aggiunta all'abbonamento ad Azure Marketplace denominato **NetApp Cloud Manager** al 7 ottobre 2020. Se disponi già dell'abbonamento originale a Azure **Cloud Manager**, non potrai utilizzare Cloud Compliance.

Seguire questi passaggi e selezionare il nuovo abbonamento **NetApp Cloud Manager**, quindi rimuovere il vecchio abbonamento **Cloud Manager**.

Se il tuo abbonamento esistente è stato emesso con un'offerta privata speciale, devi contattare NetApp in modo da poter emettere una nuova offerta privata speciale con conformità inclusa.

Fasi

Questi passaggi sono simili all'aggiunta di un nuovo abbonamento come descritto in precedenza, ma variano in alcuni punti.

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **credenziali**.
2. Individuare le credenziali per Azure Managed Service Identity per cui si desidera modificare l'abbonamento e passare il mouse sulle credenziali e fare clic su **Associa abbonamento**.

   Vengono visualizzati i dettagli dell'attuale abbonamento Marketplace.

3. Fare clic su **Add Subscription** (Aggiungi abbonamento), fare clic su **Continue** (continua) e seguire la procedura. Verrai reindirizzato al portale Azure per creare il nuovo abbonamento.
4. Assicurati di selezionare il piano **NetApp Cloud Manager** che fornisce l'accesso alla conformità del cloud e non **Cloud Manager**.
5. Seguire i passaggi del video per associare un abbonamento Marketplace a un abbonamento Azure:

► https://docs.netapp.com/it-it/occm38//media/video_subscribing_azure.mp4 *(video)*

6. Torna a Cloud Manager, seleziona il nuovo abbonamento e fai clic su **associate**.
7. Per verificare che l'abbonamento sia stato modificato, passare il mouse sopra la "i" nella scheda credenziali.

   Ora puoi annullare la tua vecchia iscrizione dal portale Azure.

8. Nel portale Azure, accedere a Software as a Service (SaaS), selezionare l'abbonamento e fare clic su **Annulla iscrizione**.

Attivare la scansione sulle origini dati

Introduzione alla conformità del cloud per Cloud Volumes ONTAP e Azure NetApp Files

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

Avvio rapido

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

Implementare l'istanza Cloud Compliance

"Implementazione della conformità al cloud in Cloud Manager" se non è già stata implementata un'istanza.

Abilita la conformità al cloud nei tuoi ambienti di lavoro

Fare clic su **Cloud Compliance**, selezionare la scheda **Configuration** e attivare le scansioni di compliance per ambienti di lavoro specifici.

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 o subnet Azure NetApp Files.
- 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 **Cloud Compliance** > **Scan Configuration** > **Edit CIFS Credentials** 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.

Configurare i volumi da sottoporre a scansione

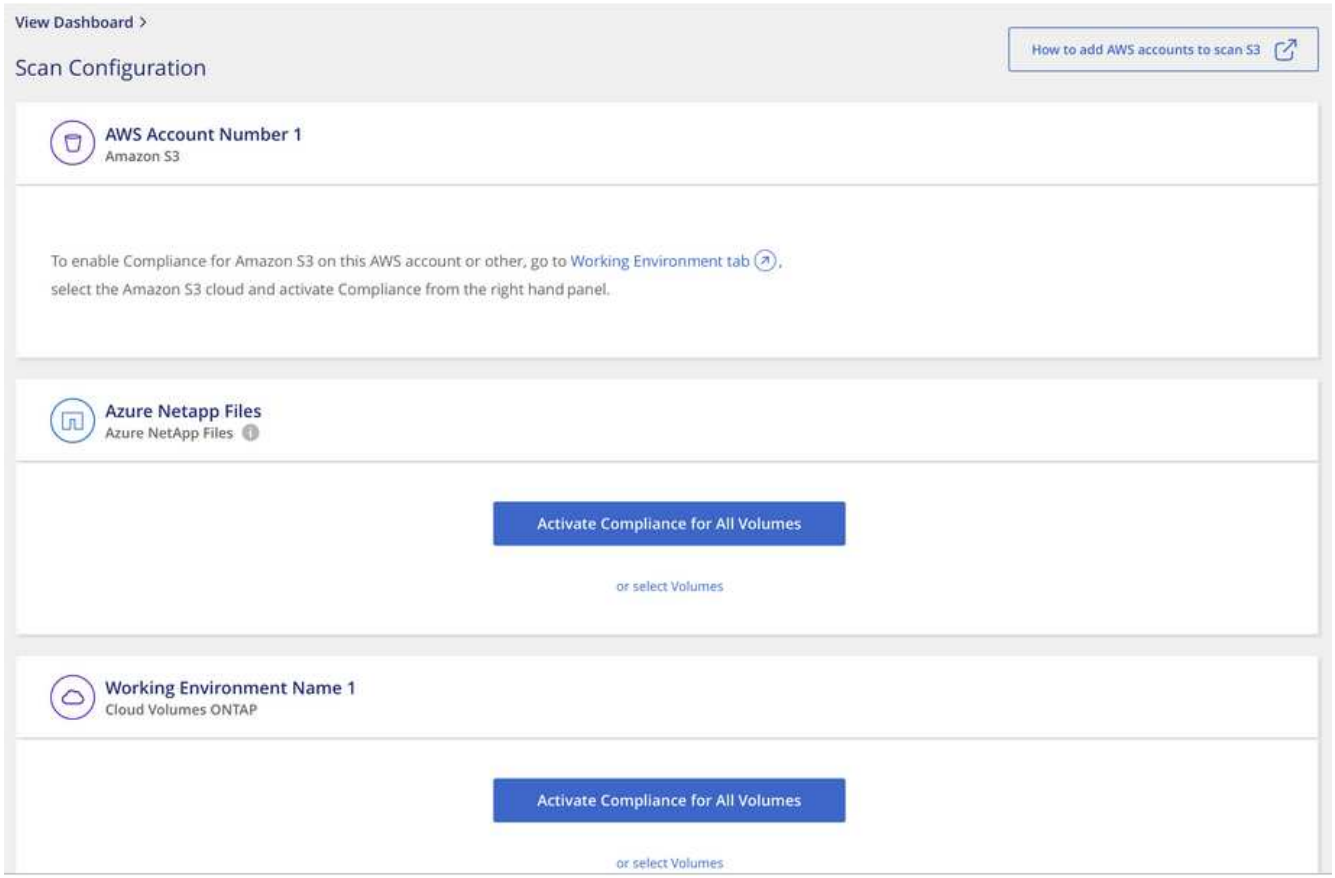
Seleziona i volumi che desideri sottoporre a scansione e la Cloud Compliance inizierà a eseguirne la scansione.

Implementazione dell'istanza Cloud Compliance

"Implementazione della conformità al cloud in Cloud Manager" se non è già stata implementata un'istanza.

Abilitare la conformità al cloud nei tuoi ambienti di lavoro

1. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**, quindi selezionare la scheda **Configuration**.



2. Per eseguire la scansione di tutti i volumi in un ambiente di lavoro, fare clic su **Activate Compliance for All Volumes** (attiva conformità per tutti i volumi).

   Per eseguire la scansione solo di determinati volumi in un ambiente di lavoro, fare clic su **o selezionare Volumes** (volumi), quindi scegliere i volumi da sottoporre a scansione.

Vedere Attivazione e disattivazione delle scansioni di compliance sui volumi per ulteriori informazioni.

Risultato

Cloud Compliance inizia la scansione dei dati in ogni ambiente di lavoro. I risultati 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 Cloud Compliance possa accedere ai volumi 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 ogni rete che include volumi per Cloud Volumes ONTAP o Azure NetApp Files.

   Per Azure NetApp Files, la conformità del cloud può eseguire la scansione solo dei volumi che si trovano nella stessa regione di Cloud Manager.

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.

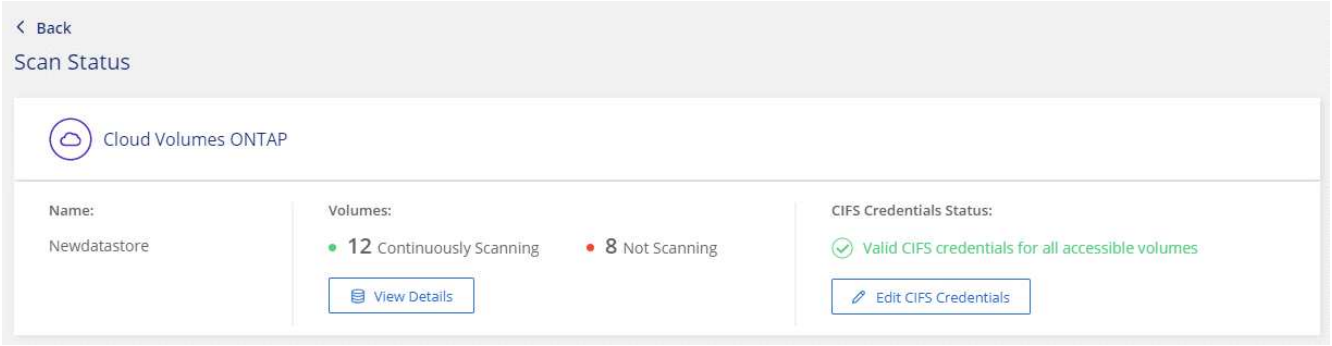
   a. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**.

   b. Fare clic sulla scheda **Configurazione**.

   c. Per ciascun ambiente di lavoro, fare clic su **Edit CIFS Credentials** (Modifica credenziali CIFS) e immettere il nome utente e la password necessari per l'accesso ai volumi CIFS nel sistema.

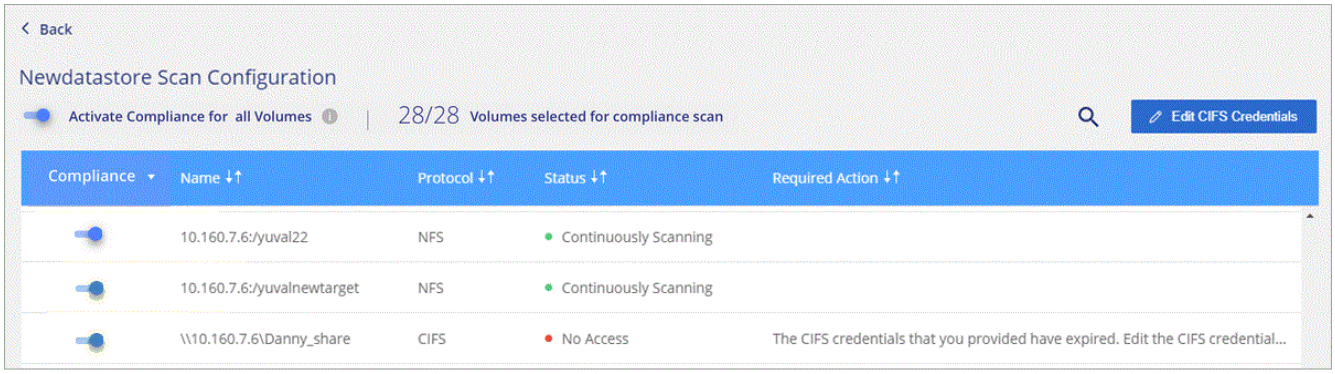
      Le credenziali possono essere di sola lettura, ma fornire credenziali di amministratore garantisce che Cloud Compliance possa leggere tutti i dati che richiedono autorizzazioni elevate. Le credenziali vengono memorizzate nell'istanza Cloud Compliance.

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



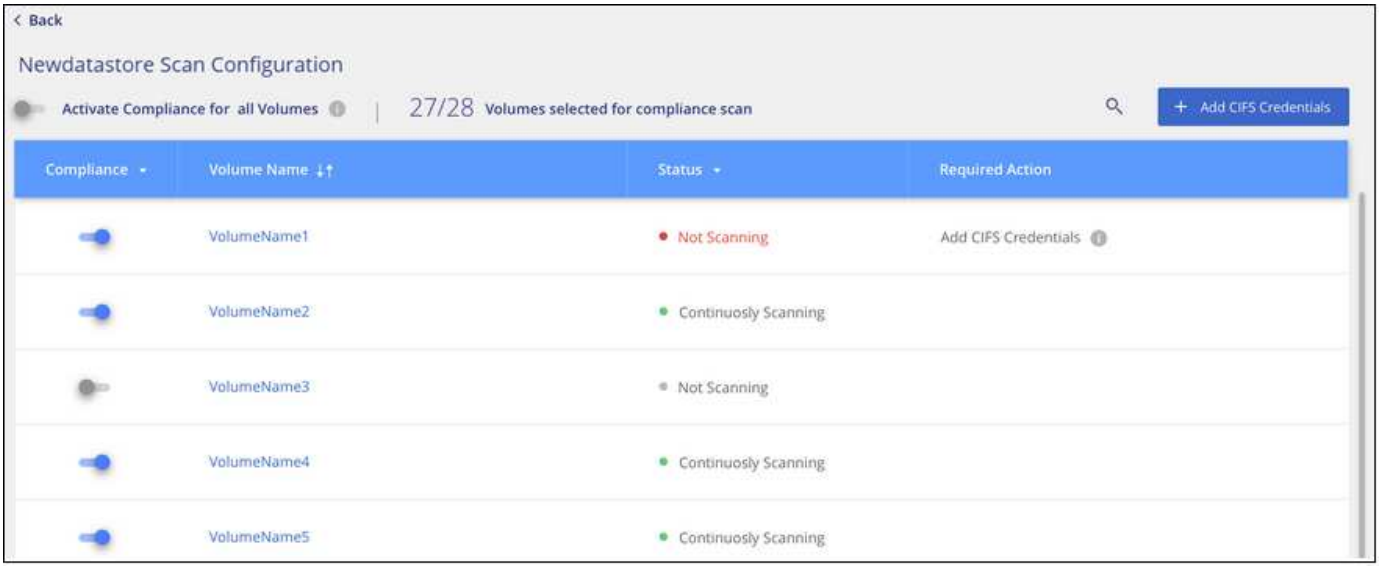
5. Nella pagina *Scan Configuration*, fare clic su **View Details** (Visualizza dettagli) per esaminare lo stato di ciascun volume CIFS e NFS e correggere eventuali errori.

   Ad esempio, l'immagine seguente mostra tre volumi, uno dei quali non è in grado di eseguire la scansione di Cloud Compliance a causa di problemi di connettività di rete tra l'istanza di Cloud Compliance e il volume.



Attivazione e disattivazione delle scansioni di compliance sui volumi

È possibile interrompere o avviare la scansione dei volumi in un ambiente di lavoro in qualsiasi momento dalla pagina Scan Configuration (Configurazione scansione). Si consiglia di eseguire la scansione di tutti i volumi.



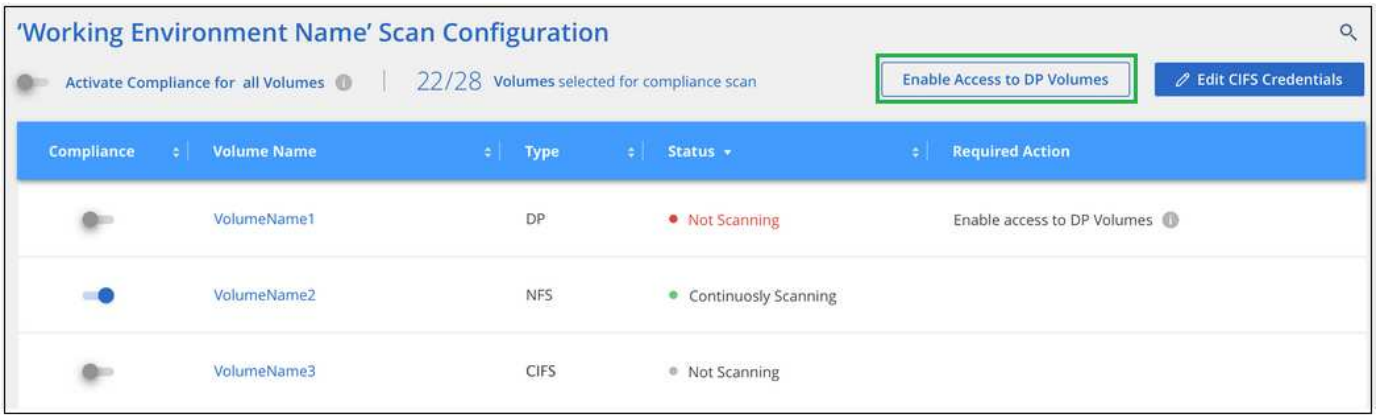
A:	Eseguire questa operazione:
Disattivare la scansione di un volume	Spostare il dispositivo di scorrimento del volume verso sinistra
Disattivare la scansione per tutti i volumi	Spostare il dispositivo di scorrimento **Activate Compliance for all Volumes** (attiva compliance per tutti i volumi) verso sinistra
Abilitare la scansione per un volume	Spostare il dispositivo di scorrimento del volume verso destra
Abilitare la scansione per tutti i volumi	Spostare il dispositivo di scorrimento **Activate Compliance for All Volumes** (attiva conformità per tutti i volumi) verso destra

I nuovi volumi aggiunti all'ambiente di lavoro vengono sottoposti automaticamente a scansione solo quando è attivata l'impostazione **attiva conformità per tutti i volumi**. Quando questa impostazione è disattivata, è necessario attivare la scansione su ogni nuovo volume creato nell'ambiente di lavoro.

Scansione dei volumi di protezione dei dati

Per impostazione predefinita, i volumi di protezione dei dati (DP) non vengono sottoposti a scansione perché non sono esposti esternamente e la Cloud Compliance non può accedervi. Questi volumi sono in genere i volumi di destinazione per le operazioni SnapMirror da un cluster ONTAP on-premise.

Inizialmente, l'elenco dei volumi Cloud Compliance identifica questi volumi come *Type* **DP** con *Status* **Not Scanning** e *Required Action* **Enable Access to DP Volumes**.



Fasi

Se si desidera eseguire la scansione di questi volumi di protezione dei dati:

1. Fare clic sul pulsante **Enable Access to DP Volumes** (Abilita accesso ai volumi DP) nella parte superiore della pagina.
2. Attivare ciascun volume DP che si desidera sottoporre a scansione oppure utilizzare il controllo **Activate Compliance for All Volumes** (attiva conformità per tutti i volumi) per abilitare tutti i volumi, inclusi tutti i volumi DP.

Una volta attivata, Cloud Compliance crea una condivisione NFS da ogni volume DP attivato per la conformità, in modo che possa essere scansionato. Le policy di esportazione delle condivisioni consentono l'accesso solo

dall'istanza Cloud Compliance.

> Solo i volumi creati inizialmente come volumi NFS nel sistema ONTAP di origine vengono visualizzati nell'elenco dei volumi. I volumi di origine creati inizialmente come CIFS non vengono attualmente visualizzati in Cloud Compliance.

Introduzione alla conformità cloud per Amazon S3

Cloud Compliance può eseguire la scansione dei bucket Amazon S3 per identificare i dati personali e sensibili che risiedono nello storage a oggetti S3. Cloud Compliance può eseguire la scansione di qualsiasi bucket dell'account, indipendentemente dal fatto che sia stato creato per una soluzione NetApp.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle sezioni rimanenti per ottenere dettagli completi.

Imposta i requisiti S3 nel tuo ambiente cloud

Assicurati che il tuo ambiente cloud sia in grado di soddisfare i requisiti per la conformità al cloud, tra cui la preparazione di un ruolo IAM e la configurazione della connettività da Cloud Compliance a S3. Consulta l'elenco completo.

Implementare l'istanza Cloud Compliance

"Implementazione della conformità al cloud in Cloud Manager" se non è già stata implementata un'istanza.

Attivare la conformità sull'ambiente di lavoro S3

Selezionare l'ambiente di lavoro Amazon S3, fare clic su **Enable Compliance** (attiva conformità) e selezionare un ruolo IAM che includa le autorizzazioni richieste.

Selezionare i bucket da sottoporre a scansione

Seleziona i bucket che desideri sottoporre a scansione e Cloud Compliance inizierà a eseguirne la scansione.

Verifica dei prerequisiti di S3

I seguenti requisiti sono specifici per la scansione dei bucket S3.

Impostare un ruolo IAM per l'istanza Cloud Compliance

Cloud Compliance ha bisogno di autorizzazioni per connettersi ai bucket S3 del tuo account e per eseguirne la scansione. Impostare un ruolo IAM che includa le autorizzazioni elencate di seguito. Cloud Manager ti chiede di selezionare un ruolo IAM quando abiliti Cloud Compliance sull'ambiente di lavoro Amazon S3.

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

Connettività da Cloud Compliance ad Amazon S3

Cloud Compliance richiede una connessione ad Amazon S3. Il modo migliore per fornire tale connessione è tramite un endpoint VPC al servizio S3. Per istruzioni, vedere "Documentazione AWS: Creazione di un endpoint gateway".

Quando si crea l'endpoint VPC, assicurarsi di selezionare la regione, il VPC e la tabella di routing che corrispondono all'istanza di Cloud Compliance. È inoltre necessario modificare il gruppo di protezione per aggiungere una regola HTTPS in uscita che abilita il traffico all'endpoint S3. In caso contrario, Cloud Compliance non può connettersi al servizio S3.

In caso di problemi, vedere "AWS Support Knowledge Center: Perché non è possibile connettersi a un bucket S3 utilizzando un endpoint VPC gateway?"

In alternativa, è possibile stabilire la connessione utilizzando un gateway NAT.

Non puoi utilizzare un proxy per accedere a S3 tramite Internet.

Implementazione dell'istanza Cloud Compliance

"Implementazione della conformità al cloud in Cloud Manager" se non è già stata implementata un'istanza.

È necessario implementare l'istanza in un connettore AWS in modo che Cloud Manager scopra automaticamente i bucket S3 in questo account AWS e li visualizzi in un ambiente di lavoro Amazon S3.

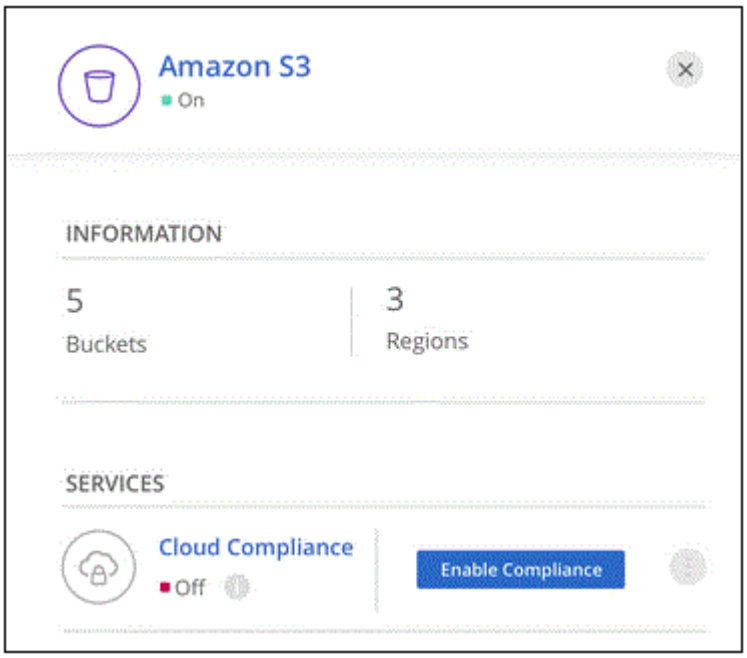
Attivazione della conformità nell'ambiente di lavoro S3

Attiva Cloud Compliance su Amazon S3 dopo aver verificato i prerequisiti.

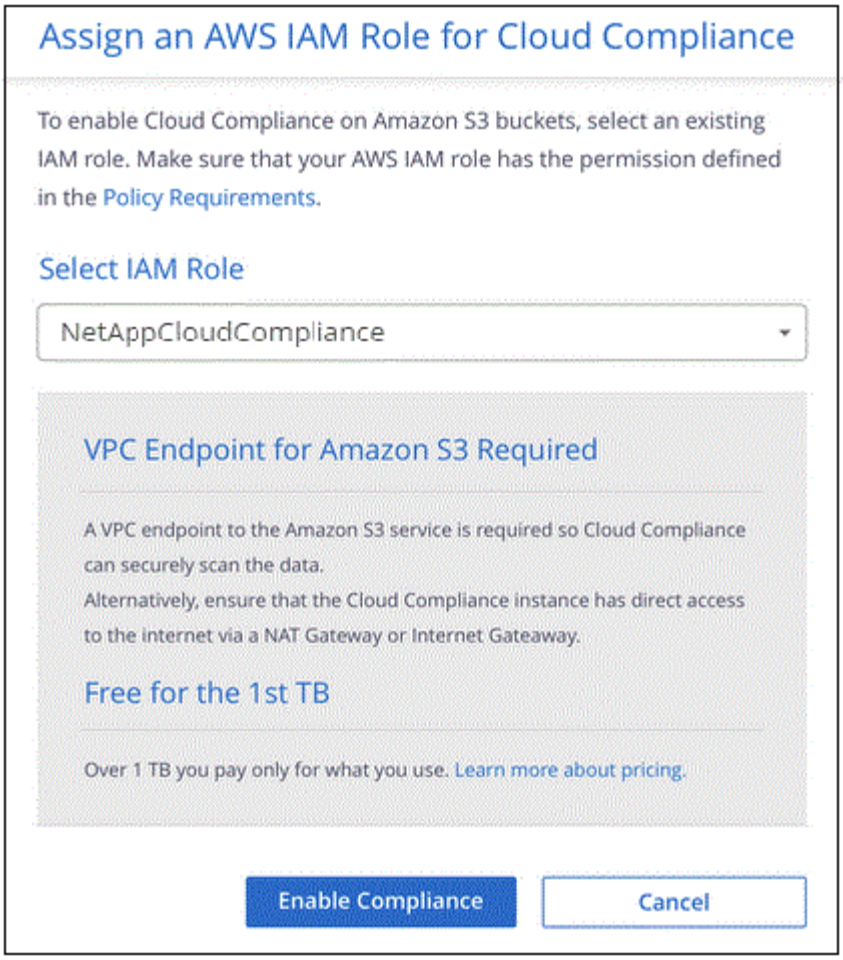
Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Working Environments** (ambienti di lavoro).
2. Selezionare l'ambiente di lavoro Amazon S3.

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



4. Quando richiesto, assegnare un ruolo IAM all'istanza di Cloud Compliance che ha le autorizzazioni richieste.



5. Fare clic su **Enable Compliance** (attiva conformità)

È inoltre possibile attivare le scansioni di conformità per un ambiente di lavoro dalla pagina Scan Configuration (Configurazione scansione) facendo clic su E selezionando **Activate Compliance**.

Risultato

Cloud Manager assegna il ruolo IAM all'istanza.

Attivazione e disattivazione delle scansioni di compliance sui bucket S3

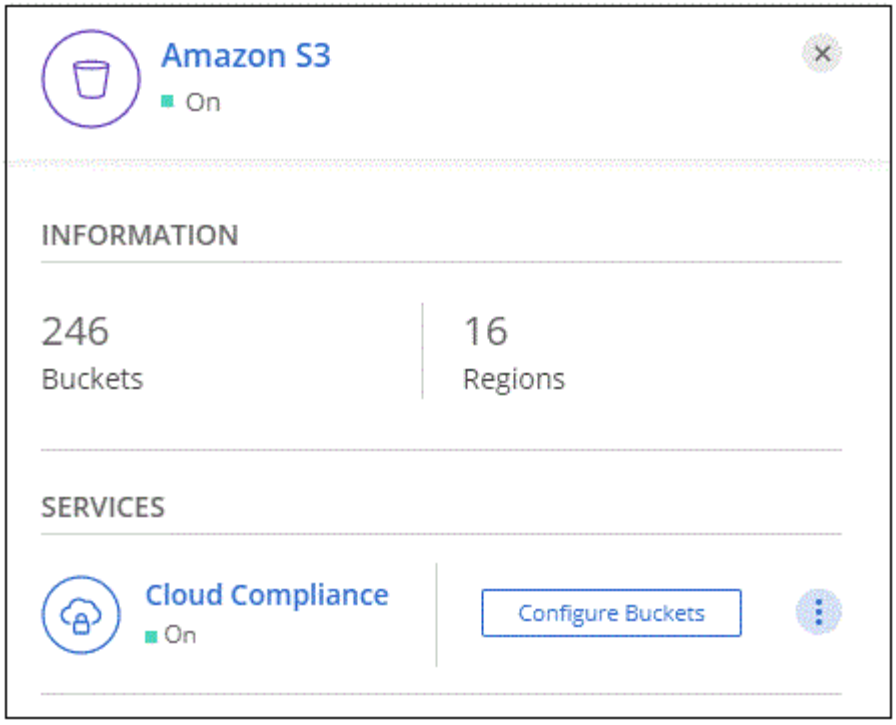
Dopo che Cloud Manager ha attivato Cloud Compliance su Amazon S3, il passaggio successivo consiste nel configurare i bucket che si desidera sottoporre a scansione.

Quando Cloud Manager viene eseguito nell'account AWS che dispone dei bucket S3 che si desidera sottoporre a scansione, rileva tali bucket e li visualizza in un ambiente di lavoro Amazon S3.

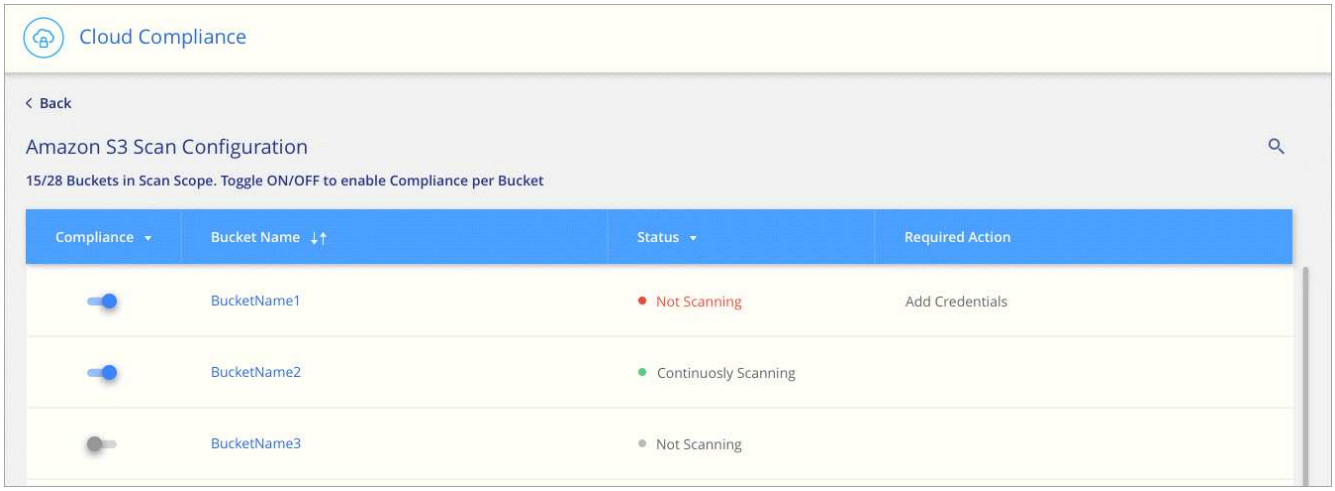
Anche la conformità al cloud può farlo Eseguire la scansione dei bucket S3 che si trovano in diversi account AWS.

Fasi

1. Selezionare l'ambiente di lavoro Amazon S3.
2. Nel riquadro a destra, fare clic su **Configure Bucket** (Configura bucket).



3. Consentire la conformità sui bucket che si desidera sottoporre a scansione.



Risultato

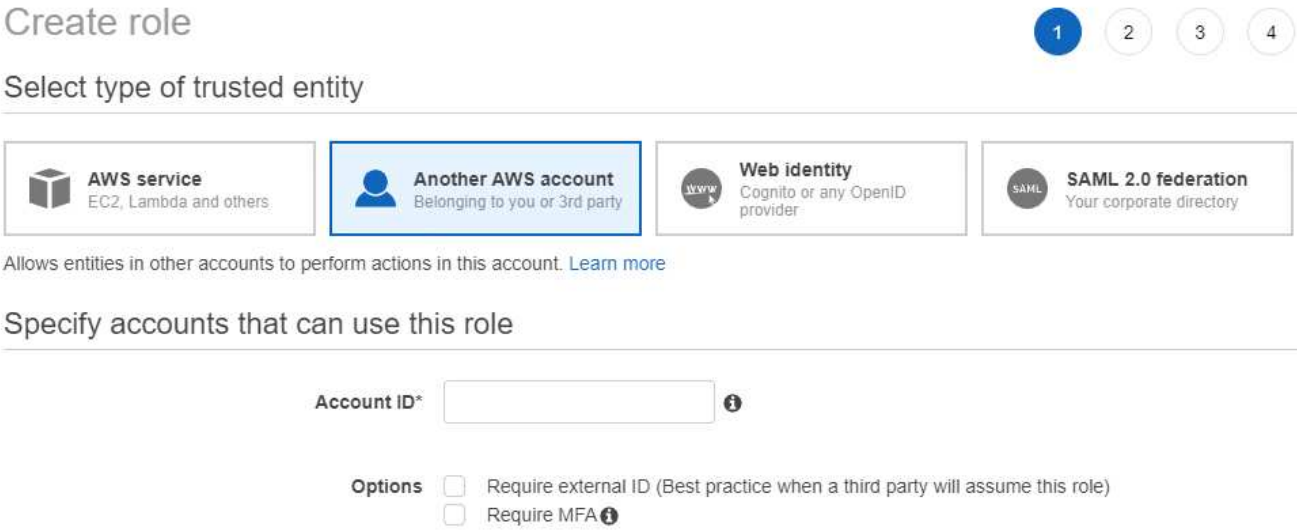
Cloud Compliance inizia la scansione dei bucket S3 abilitati. In caso di errori, questi vengono visualizzati nella colonna Status (Stato), insieme all'azione richiesta per risolvere l'errore.

Scansione dei bucket da account AWS aggiuntivi

È possibile eseguire la scansione dei bucket S3 che si trovano sotto un account AWS diverso assegnando un ruolo da tale account per accedere all'istanza esistente di Cloud Compliance.

Fasi

1. Accedere all'account AWS di destinazione in cui si desidera eseguire la scansione dei bucket S3 e creare un ruolo IAM selezionando **un altro account AWS**.



Assicurarsi di effettuare le seguenti operazioni:

- Inserire l'ID dell'account in cui risiede l'istanza di Cloud Compliance.
- Modificare la **durata massima della sessione CLI/API** da 1 ora a 12 ore e salvare la modifica.
- Allega la policy IAM sulla conformità al cloud. Assicurarsi che disponga delle autorizzazioni necessarie.

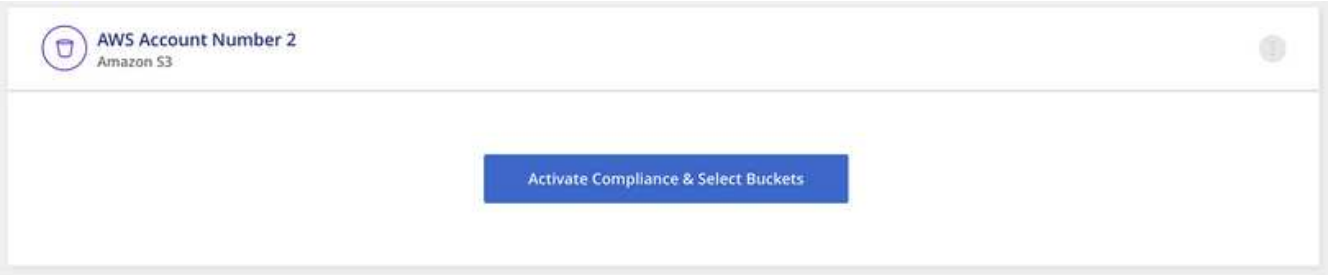
```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:HeadBucket"
          ],
          "Resource": "*"
      },
  ]
}
```

2. Accedere all'account AWS di origine in cui risiede l'istanza Cloud Compliance e selezionare il ruolo IAM associato all'istanza.
   a. Modificare la **durata massima della sessione CLI/API** da 1 ora a 12 ore e salvare la modifica.
   b. Fare clic su **Allega policy**, quindi su **Crea policy**.
   c. Creare una policy che includa l'azione "sts:AssumeRole" e l'ARN del ruolo creato nell'account di destinazione.

```
{
    "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/*"
            ]
        }
    ]
}
```

L'account del profilo dell'istanza Cloud Compliance ora ha accesso all'account AWS aggiuntivo.

3. Accedere alla pagina **Amazon S3 Scan Configuration** (Configurazione scansione Amazon S3) per visualizzare il nuovo account AWS. Nota: La sincronizzazione dell'ambiente di lavoro del nuovo account e la visualizzazione di queste informazioni possono richiedere alcuni minuti per la conformità cloud.



4. Fare clic su **Activate Compliance & Select Bucket** (attiva Compliance e seleziona bucket) e selezionare i bucket da sottoporre a scansione.

Risultato

Cloud Compliance inizia la scansione dei nuovi bucket S3 che hai attivato.

Scansione degli schemi del database

Completa alcuni passaggi per iniziare la scansione degli schemi di database con Cloud

Compliance.

Avvio rapido

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

Esaminare i prerequisiti del database

Assicurarsi che il database sia supportato e di disporre delle informazioni necessarie per la connessione al database.

Implementare l'istanza Cloud Compliance

"Implementazione della conformità al cloud in Cloud Manager" se non è già stata implementata un'istanza.

Aggiungere il server database

Aggiungere il server database a cui si desidera accedere.

Selezionare gli schemi

Selezionare gli schemi da sottoporre a scansione.

Verifica dei prerequisiti

Prima di attivare la conformità al cloud, verificare di disporre di una configurazione supportata.

Database supportati

Cloud Compliance può eseguire la scansione degli schemi dai seguenti database:

- MongoDB
- Oracle
- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)

La funzione di raccolta delle statistiche **deve essere abilitata** nel database.

Requisiti del database

È possibile eseguire la scansione di qualsiasi database con connettività all'istanza Cloud Compliance, indipendentemente da dove è ospitato. Per connettersi al database sono necessarie solo le seguenti informazioni:

- Indirizzo IP o nome host
- Porta
- Nome del servizio (solo per l'accesso ai database Oracle)
- Credenziali che consentono l'accesso in lettura agli schemi

  Quando si sceglie un nome utente e una password, è importante sceglierne uno che disponga delle autorizzazioni di lettura complete per tutti gli schemi e le tabelle che si desidera sottoporre a scansione. Si consiglia di creare un utente dedicato per il sistema Cloud Compliance con tutte le autorizzazioni necessarie.

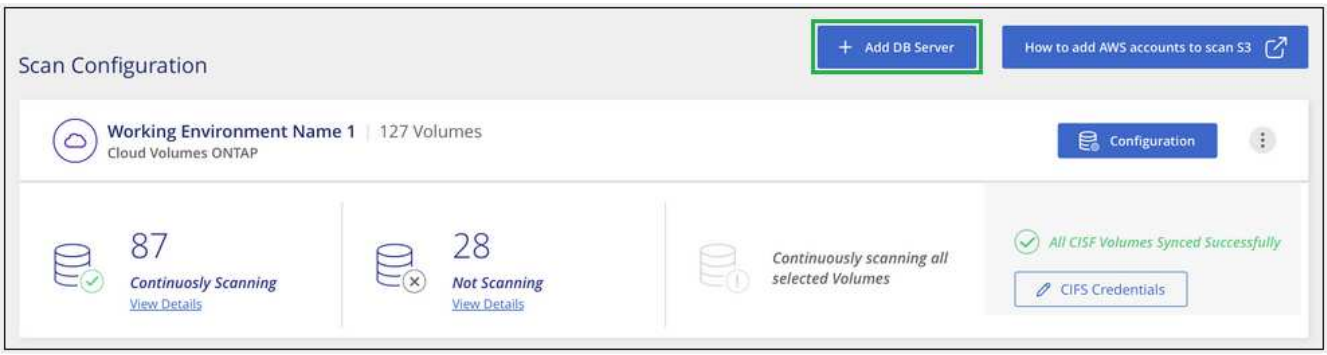
Nota: per MongoDB, è necessario un ruolo Admin di sola lettura.

Aggiunta del server database

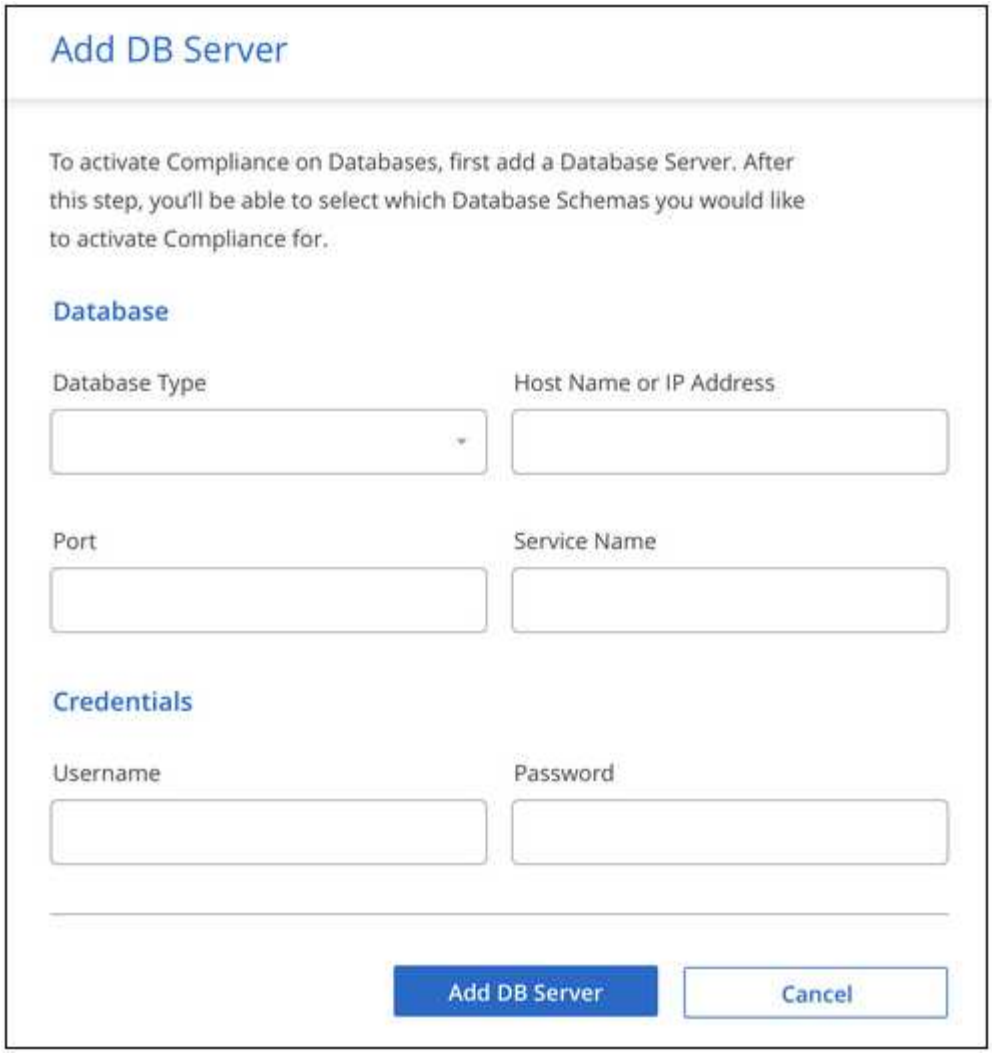
Devi avere "Ha già implementato un'istanza di Cloud Compliance in Cloud Manager".

Aggiungere il server di database in cui risiedono gli schemi.

1. Dalla pagina *Scan Configuration*, fare clic sul pulsante **Add DB Server** (Aggiungi server DB).



2. Inserire le informazioni richieste per identificare il server di database.
   a. Selezionare il tipo di database.
   b. Immettere la porta e il nome host o l'indirizzo IP per la connessione al database.
   c. Per i database Oracle, immettere il nome del servizio.
   d. Inserire le credenziali in modo che Cloud Compliance possa accedere al server.
   e. Fare clic su **Add DB Server** (Aggiungi server DB).



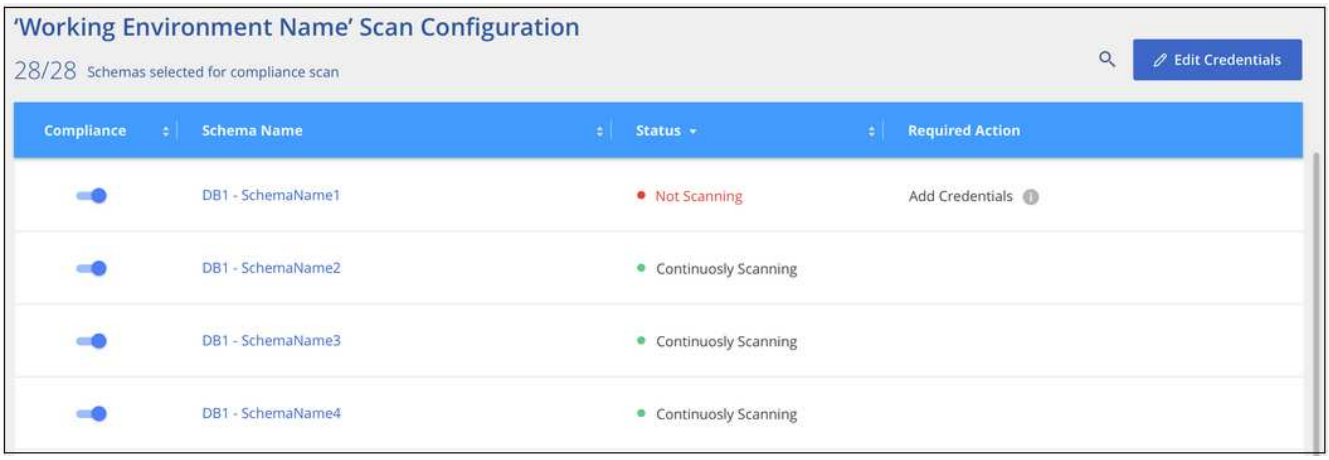
Il database viene aggiunto all'elenco delle directory di lavoro.

Attivazione e disattivazione delle scansioni di compliance sugli schemi di database

È possibile interrompere o avviare la scansione degli schemi in qualsiasi momento.

1. Dalla pagina *Scan Configuration*, fare clic sul pulsante **Configuration** relativo al database che si desidera configurare.

2. Selezionare gli schemi da sottoporre a scansione spostando il dispositivo di scorrimento verso destra.



Risultato

Cloud Compliance inizia la scansione degli schemi di database abilitati. In caso di errori, questi vengono visualizzati nella colonna Status (Stato), insieme all'azione richiesta per risolvere l'errore.

Rimozione di un database da Cloud Manager

Se non si desidera più eseguire la scansione di un determinato database, è possibile eliminarlo dall'interfaccia di Cloud Manager e interrompere tutte le scansioni.

Dalla pagina *Scan Configuration*, fare clic su Nella riga del database, quindi fare clic su **Remove DB Server** (Rimuovi server DB).

Scansione on-premise dei dati ONTAP con conformità al cloud utilizzando SnapMirror

È possibile eseguire la scansione dei dati ONTAP on-premise con la conformità al cloud replicando i dati NFS o CIFS on-premise in un ambiente di lavoro Cloud Volumes ONTAP e abilitando quindi la conformità. La scansione dei dati direttamente da un ambiente di lavoro ONTAP on-premise non è supportata.

Devi avere "Ha già implementato un'istanza di Cloud Compliance in Cloud Manager".

Fasi

1. Da Cloud Manager, creare una relazione SnapMirror tra il cluster ONTAP on-premise e Cloud Volumes ONTAP.
   a. "Scopri il cluster on-premise in Cloud Manager".
   b. "Creare una replica SnapMirror tra il cluster ONTAP on-premise e Cloud Volumes ONTAP da Cloud

Manager".

2. Per i volumi DP creati dai volumi di origine SMB, dalla CLI ONTAP, configurare i volumi di destinazione SMB per l'accesso ai dati. (Non è necessario per i volumi NFS perché l'accesso ai dati viene attivato automaticamente tramite Cloud Compliance).
   a. "Creare una condivisione SMB sul volume di destinazione".
   b. "Applicare gli ACL appropriati alla condivisione SMB nel volume di destinazione".
3. Da Cloud Manager, attivare la conformità cloud nell'ambiente di lavoro Cloud Volumes ONTAP che contiene i dati SnapMirror:
   a. Fare clic su **ambienti di lavoro**.
   b. Selezionare l'ambiente di lavoro che contiene i dati SnapMirror e fare clic su **Enable Compliance** (attiva conformità).

      "Fai clic qui per ricevere assistenza per abilitare la conformità al cloud su un sistema Cloud Volumes ONTAP".

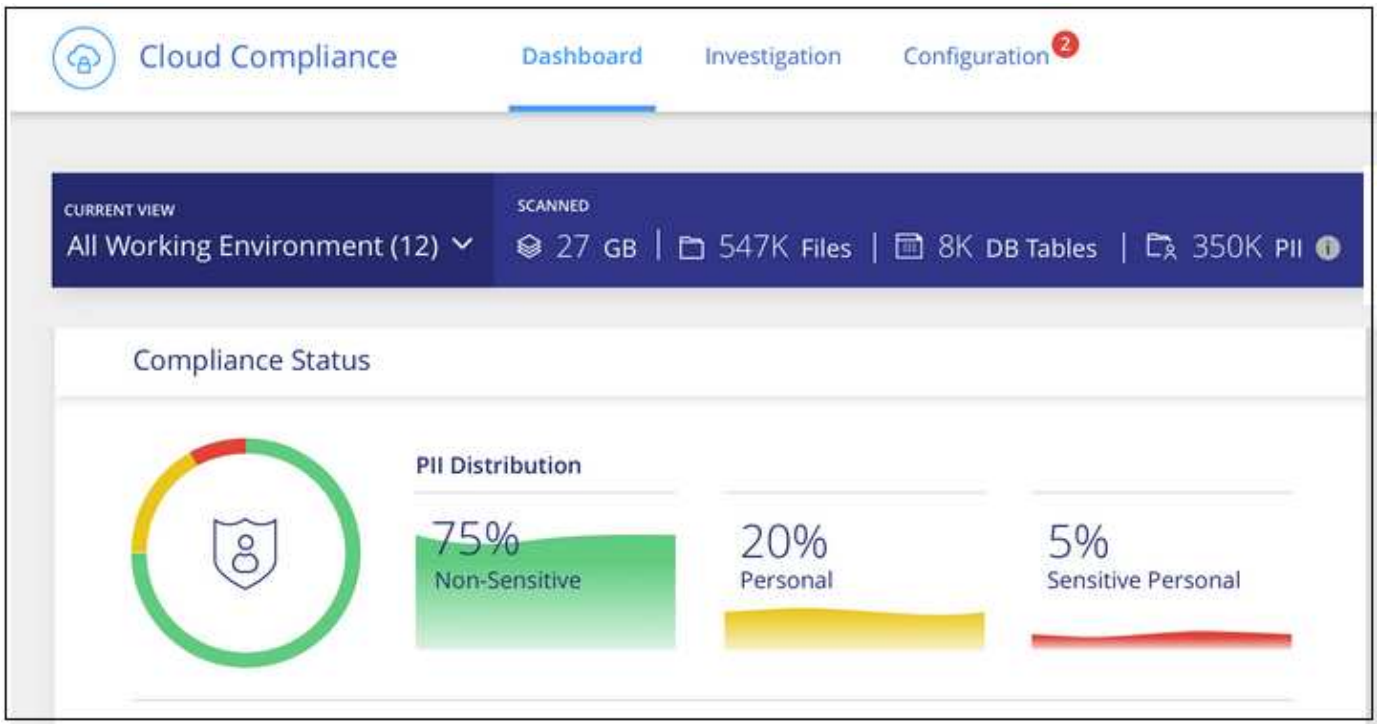
   c. Fare clic sul pulsante **Enable Access to DP Volumes** (Abilita accesso ai volumi DP) nella parte superiore della pagina *Scan Configuration* (Configurazione scansione).
   d. Attivare ciascun volume DP che si desidera sottoporre a scansione oppure utilizzare il controllo **Activate Compliance for All Volumes** (attiva conformità per tutti i volumi) per abilitare tutti i volumi, inclusi tutti i volumi DP.

Vedere "Scansione dei volumi di protezione dei dati" Per ulteriori informazioni sulla scansione di volumi DP.

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.

Per impostazione predefinita, il dashboard Cloud Compliance visualizza i dati di conformità per tutti gli ambienti di lavoro e i database.



Se si desidera visualizzare i dati solo per alcuni ambienti di lavoro, selezionare gli ambienti di lavoro.

Dati personali

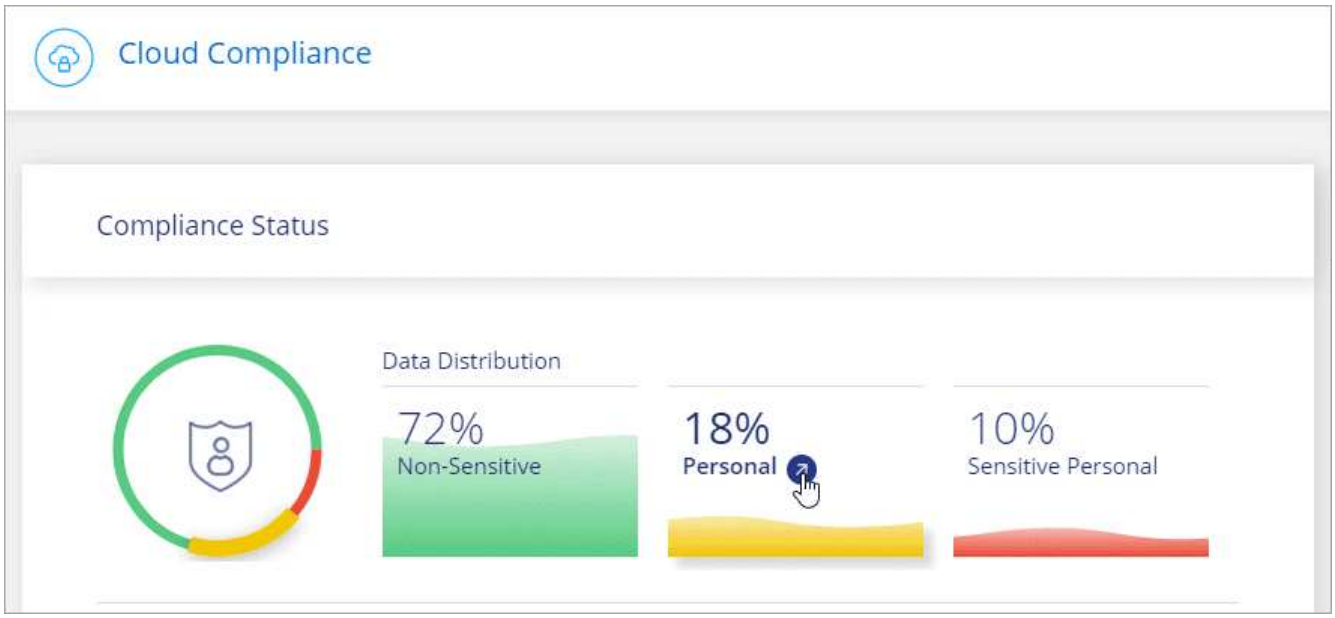
Cloud Compliance identifica automaticamente parole, stringhe e modelli specifici (Regex) all'interno dei dati. Ad esempio, informazioni di identificazione personale (PII), numeri di carta di credito, numeri di previdenza sociale, numeri di conto bancario e altro ancora. Consulta l'elenco completo.

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.

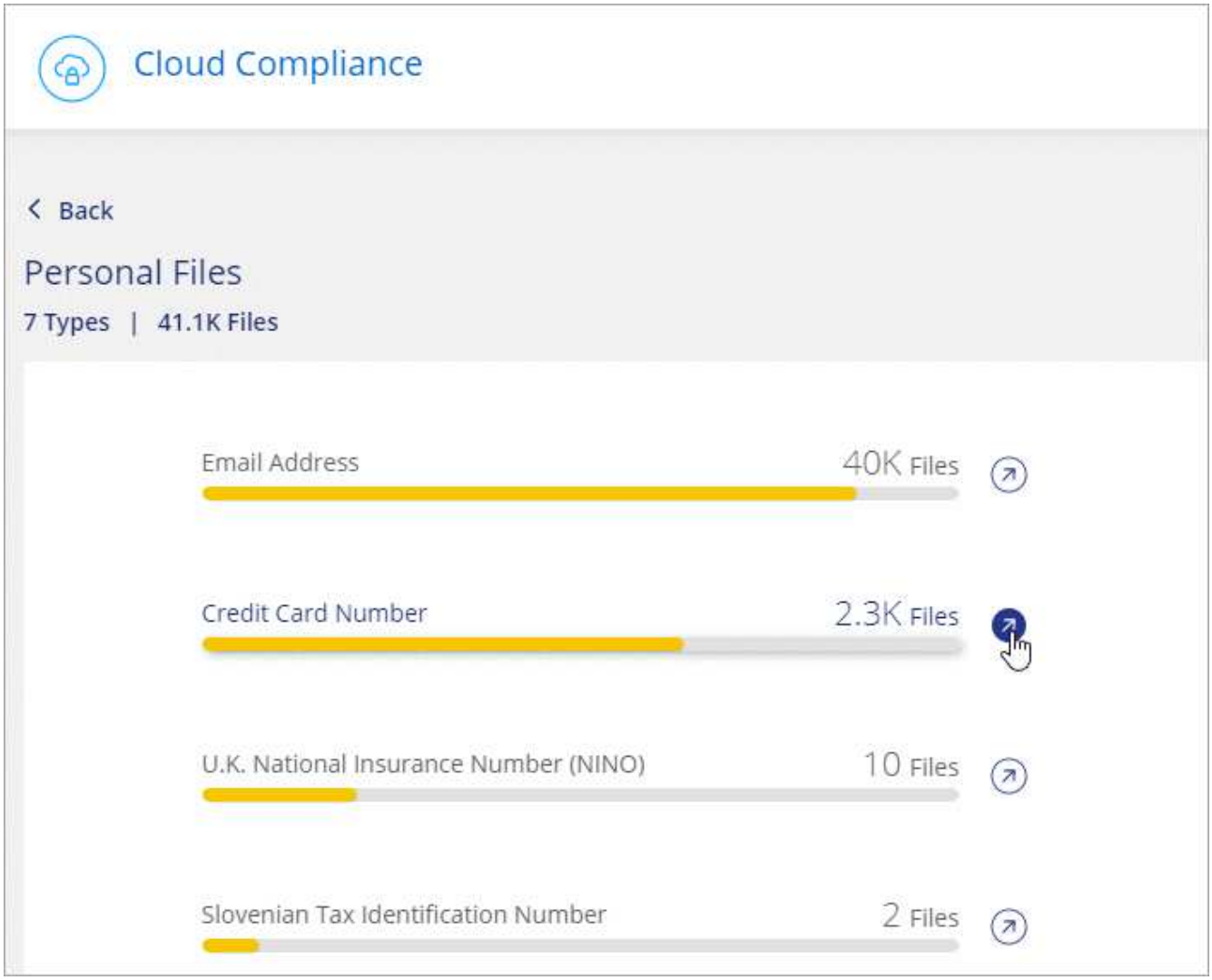
Visualizzazione di file contenenti dati personali

Fasi

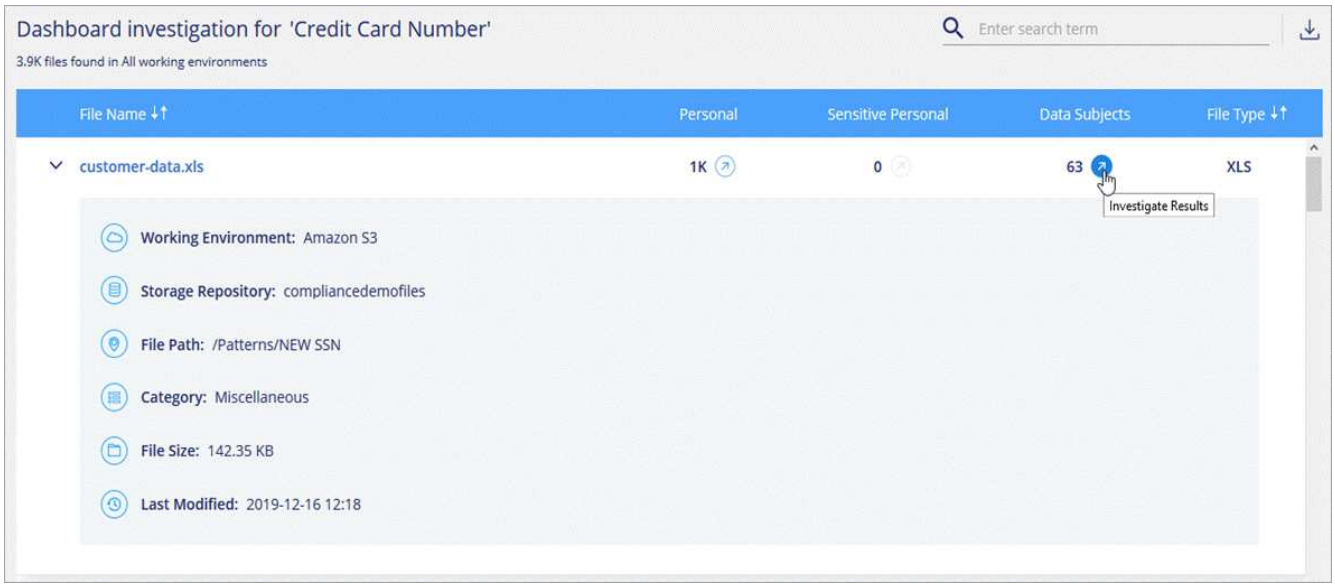
1. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance** e fare clic sulla scheda **Dashboard**.
2. Per esaminare i dettagli di tutti i dati personali, fare clic sull'icona accanto alla percentuale dei dati personali.



3. Per esaminare i dettagli di un tipo specifico di dati personali, fare clic su **Visualizza tutto**, quindi fare clic sull'icona **esamina risultati** per un tipo specifico di dati personali.

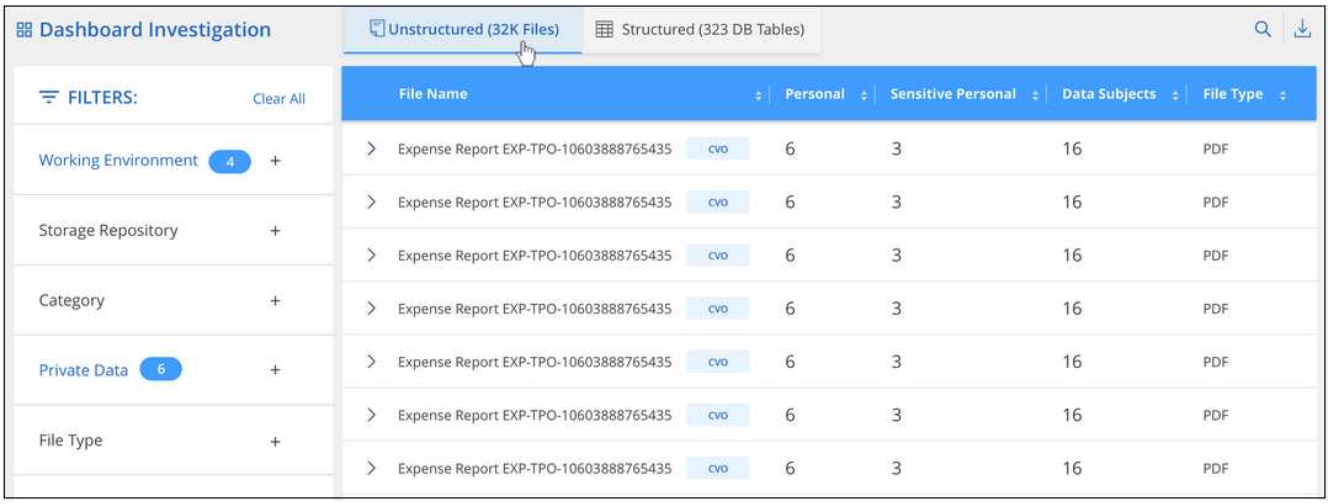


4. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.



5. È inoltre possibile filtrare il contenuto della pagina di analisi per visualizzare solo i risultati desiderati. Le schede di primo livello consentono di visualizzare i dati dai file (dati non strutturati) o dai database (dati strutturati).

   Sono disponibili filtri per ambiente di lavoro, repository di storage, categoria, dati privati, tipo di file, Data dell'ultima modifica e se le autorizzazioni dell'oggetto S3 sono aperte all'accesso pubblico.



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

Tipo	Identificatore	Convalida della prossimità?
Identificatori nazionali	ID belga (numero nazionale)	Sì
	ID brasiliano (CPF)	Sì
	ID bulgaro (UCN)	Sì
	California driver's License	Sì
	ID croato (OIB)	Sì
	Codice fiscale di Cipro (TIC)	Sì
	Documento d'identità ceco/slovacco	Sì
	ID danese (CPR)	Sì
	Olandese ID (BSN)	Sì
	ID estone	Sì
	ID finlandese (HETU)	Sì
	Francese Tax Identification Number (SPI)	Sì
	Codice fiscale tedesco (Steuerliche Identifikationsnummer)	Sì
	ID greco	Sì
	Codice fiscale ungherese	Sì
	Irish ID (PPS) (ID irlandese)	Sì
	ID Israeliano	Sì
	Codice fiscale italiano	Sì
	Documento d'identità lettone	Sì
	ID lituano	Sì
	Lussemburgo ID	Sì
	ID maltese	Sì
	ID polacco (PESEL)	Sì
	Portoghese Tax Identification Number (NIF)	Sì
	ID rumeno (CNP)	Sì
	ID sloveno (EMSO)	Sì
	ID sudafricano	Sì
	Codice fiscale spagnolo	Sì
	ID svedese	Sì
	REGNO UNITO ID (NINO)	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.

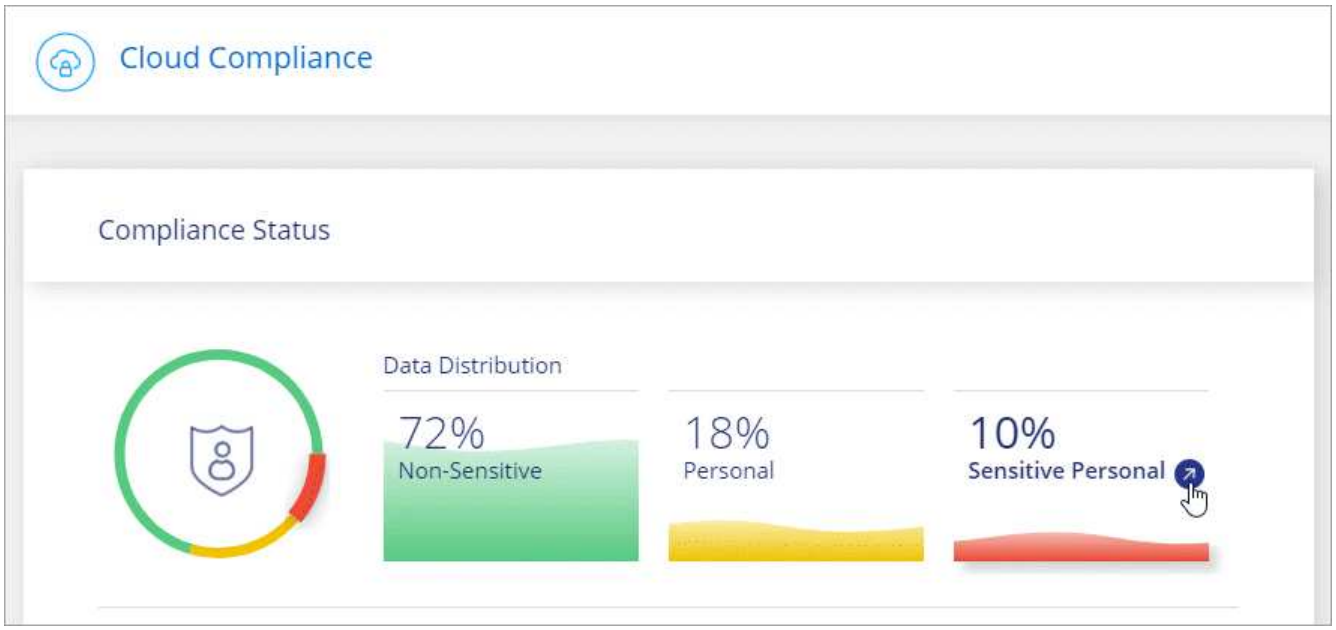
Ad esempio, una categoria di dati GDPR sensibili è l'origine etnica. Grazie alle sue capacità di NLP, Cloud Compliance è in grado di distinguere la differenza tra una frase con la dicitura "George is Mexican" (che indica i dati sensibili come specificato nell'articolo 9 del GDPR) e "George is Eating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

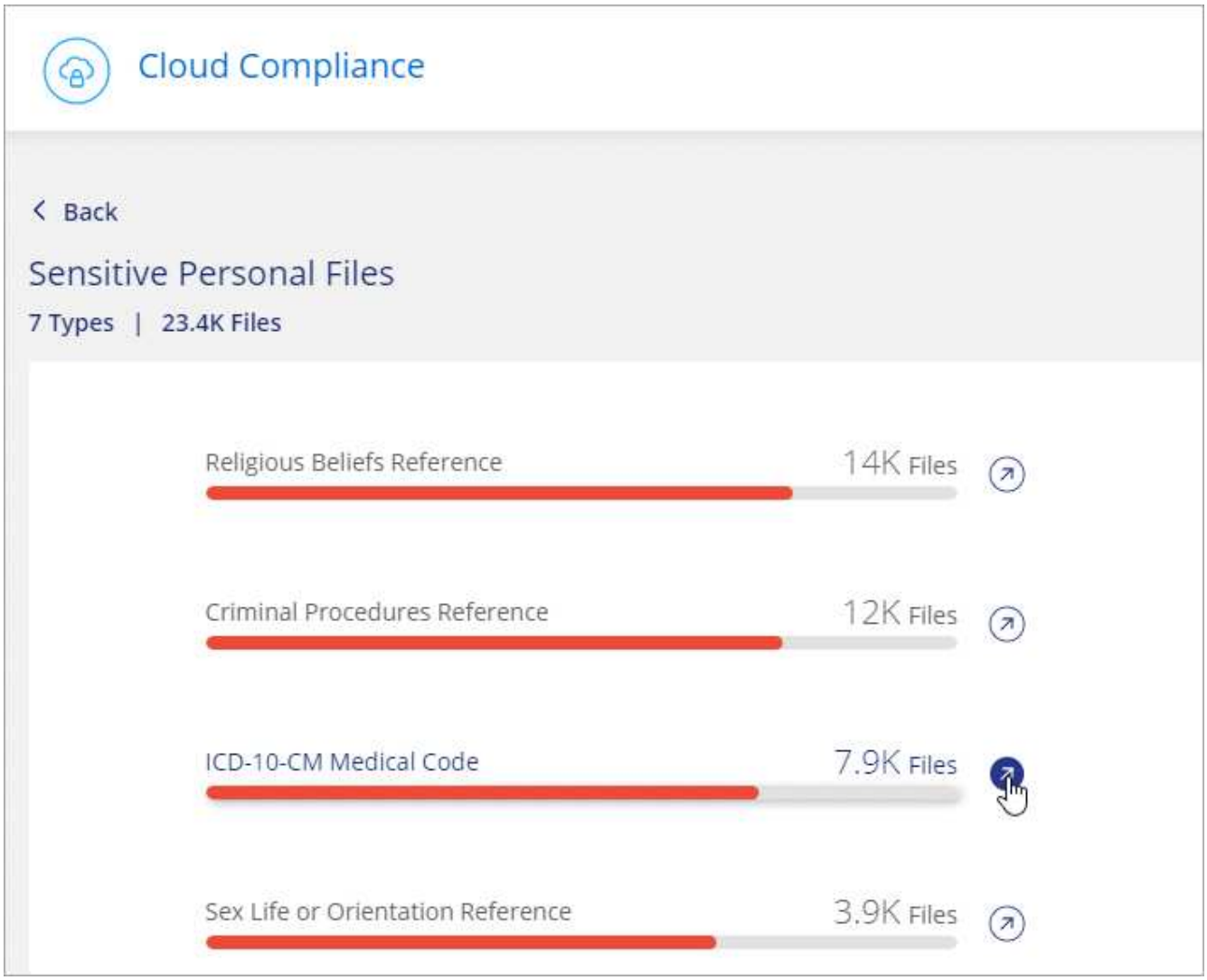
Visualizzazione di file contenenti dati personali sensibili

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**.
2. Per esaminare i dettagli di tutti i dati personali sensibili, fare clic sull'icona accanto alla percentuale dei dati personali sensibili.



3. Per esaminare i dettagli di un tipo specifico di dati personali sensibili, fare clic su **Visualizza tutto**, quindi fare clic sull'icona **esamina risultati** per un tipo specifico di dati personali sensibili.



4. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

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.

Codici medici ICD-9-CM
Codici utilizzati nel settore medico e sanitario.

Codici medici ICD-10-CM
Codici utilizzati nel settore medico e sanitario.

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.

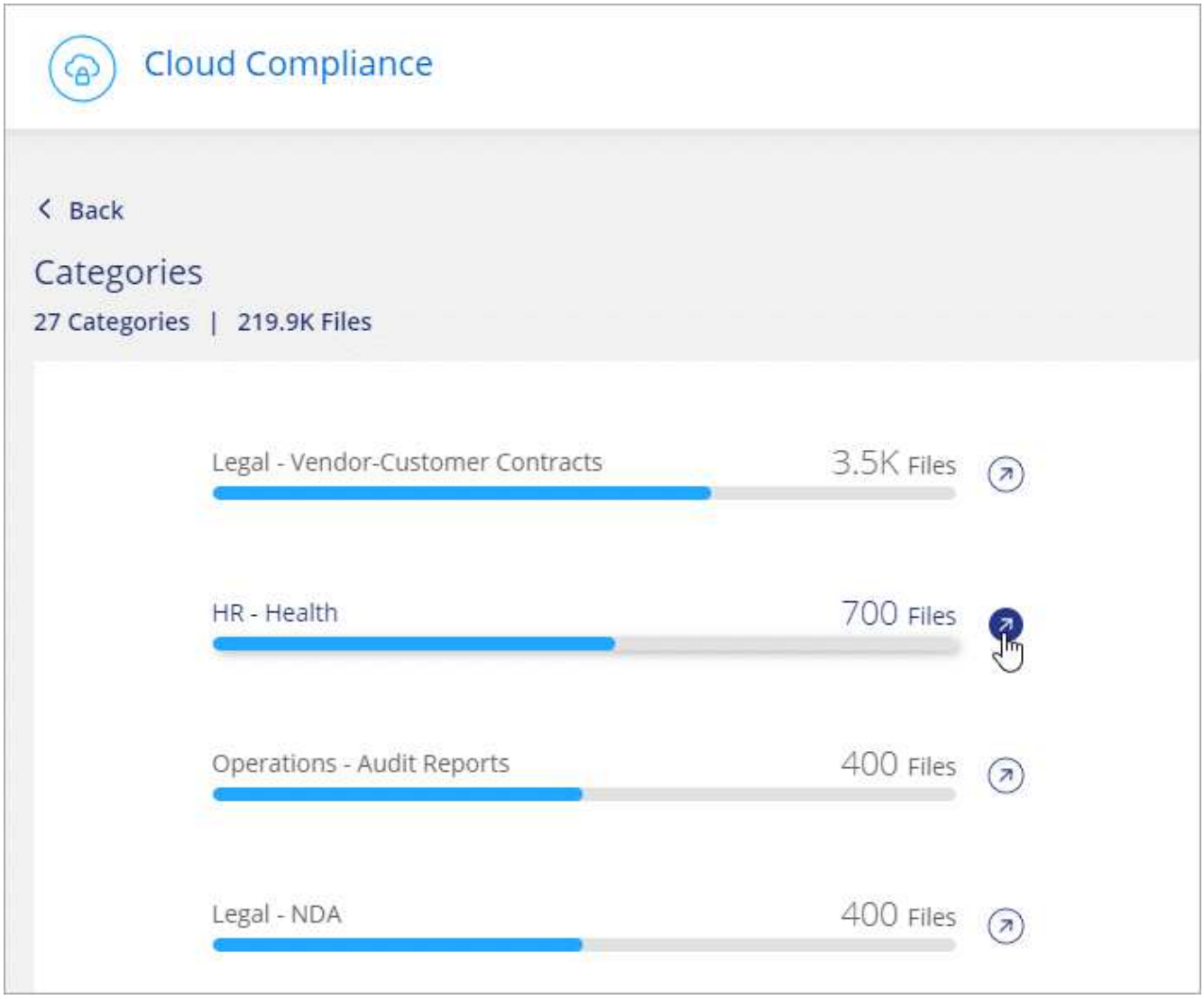
Le categorie possono aiutarti a capire cosa accade con i tuoi dati mostrando i tipi di informazioni di cui disponi. Ad esempio, una categoria come i curriculum o i contratti dei dipendenti può includere dati sensibili. Quando si analizzano i risultati, è possibile che i contratti dei dipendenti siano 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 **Cloud Compliance**.
2. Fare clic sull'icona **esamina risultati** di una delle 4 categorie principali direttamente dalla schermata principale oppure fare clic su **Visualizza tutto** e quindi sull'icona corrispondente a una delle categorie.



3. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

Tipi di categorie

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

Finanza

- Bilanci
- Ordini di acquisto
- Fatture
- Report trimestrali

FC

- Controlli in background
- Piani di compensazione
- Contratti con i dipendenti
- Recensioni dei dipendenti

- Salute
- Riprende

Legale
- NDA
- Contratti fornitore-cliente

Marketing
- Campagne
- Conferenze

Operazioni
- Report di audit

Vendite
- Ordini di vendita

Servizi
- RFI
- RFP
- SOW
- Formazione

Supporto
- Reclami e biglietti

Categorie di metadati
- Dati dell'applicazione
- Archiviare i file
- Audio
- Dati delle applicazioni di business
- File CAD
- Codice
- Database e file di indice
- File di progettazione
- Email Application Data (dati applicazione email)
- Eseguibili
- Dati delle applicazioni finanziarie
- Health Application Data
- Immagini
- Registri
- Documenti vari
- Presentazioni varie

- Fogli di calcolo vari
- Video

Tipi di file

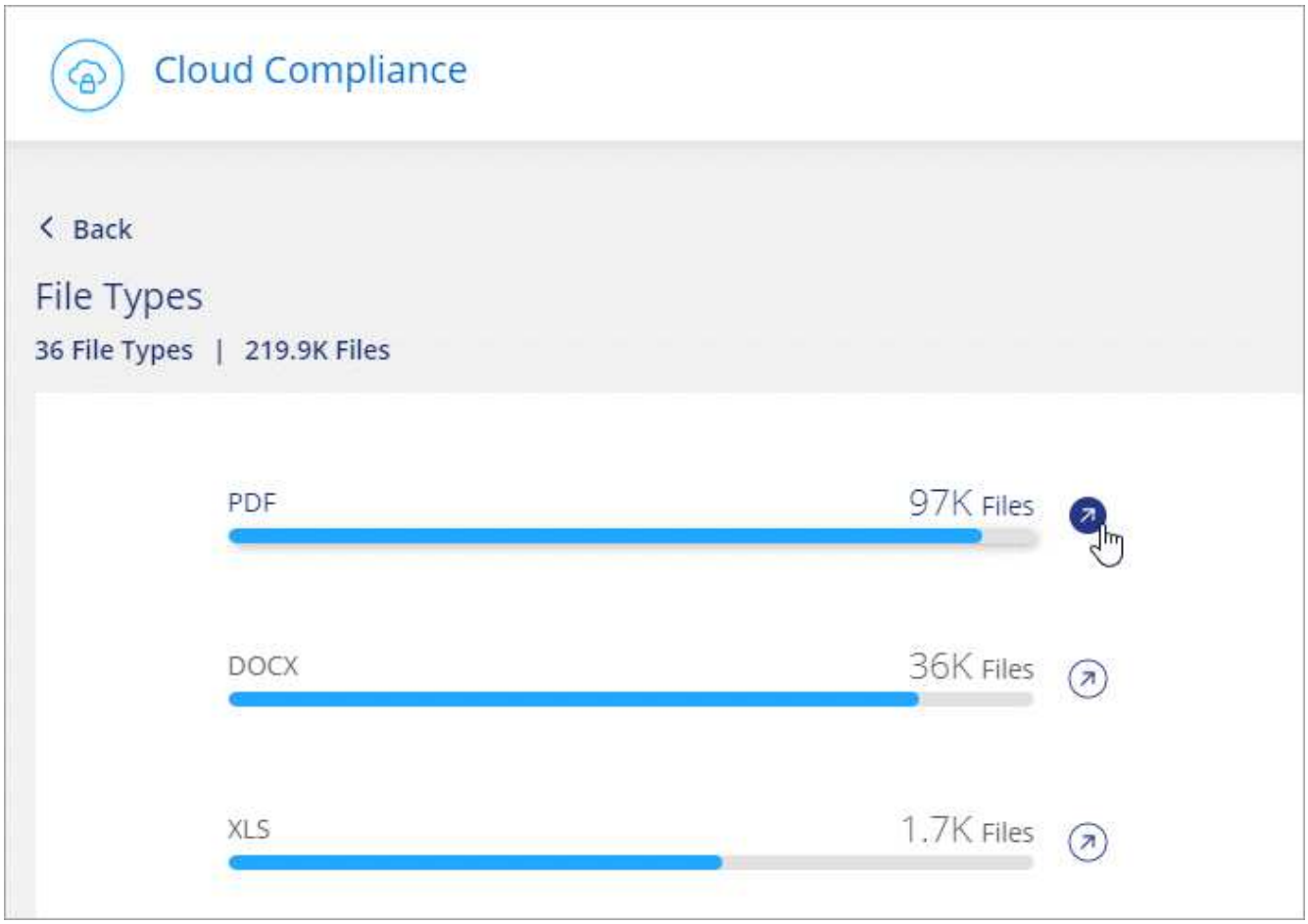
Cloud Compliance prende i dati sottoposti a scansione e li suddivide in base al tipo di file. La revisione dei tipi di file consente di controllare i dati sensibili, poiché alcuni tipi di file potrebbero non essere memorizzati correttamente. Vedere l'elenco dei tipi di file.

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 **Cloud Compliance**.
2. Fare clic sull'icona **esamina risultati** per uno dei 4 tipi di file principali direttamente dalla schermata principale oppure fare clic su **Visualizza tutto**, quindi fare clic sull'icona corrispondente a uno qualsiasi dei tipi di file.



3. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

Tipi di file

Cloud Compliance esegue la scansione di tutti i file per individuare informazioni su categorie e metadati e visualizza tutti i tipi di file nella sezione tipi di file della dashboard.

Tuttavia, quando Cloud Compliance rileva le informazioni personali identificabili (PII) o esegue una ricerca DSAR, sono supportati solo i seguenti formati di file: .PDF, .DOCX, .DOC, .PPTX, .XLS, XLSX, .CSV, .TXT, .RTF E .JSON.

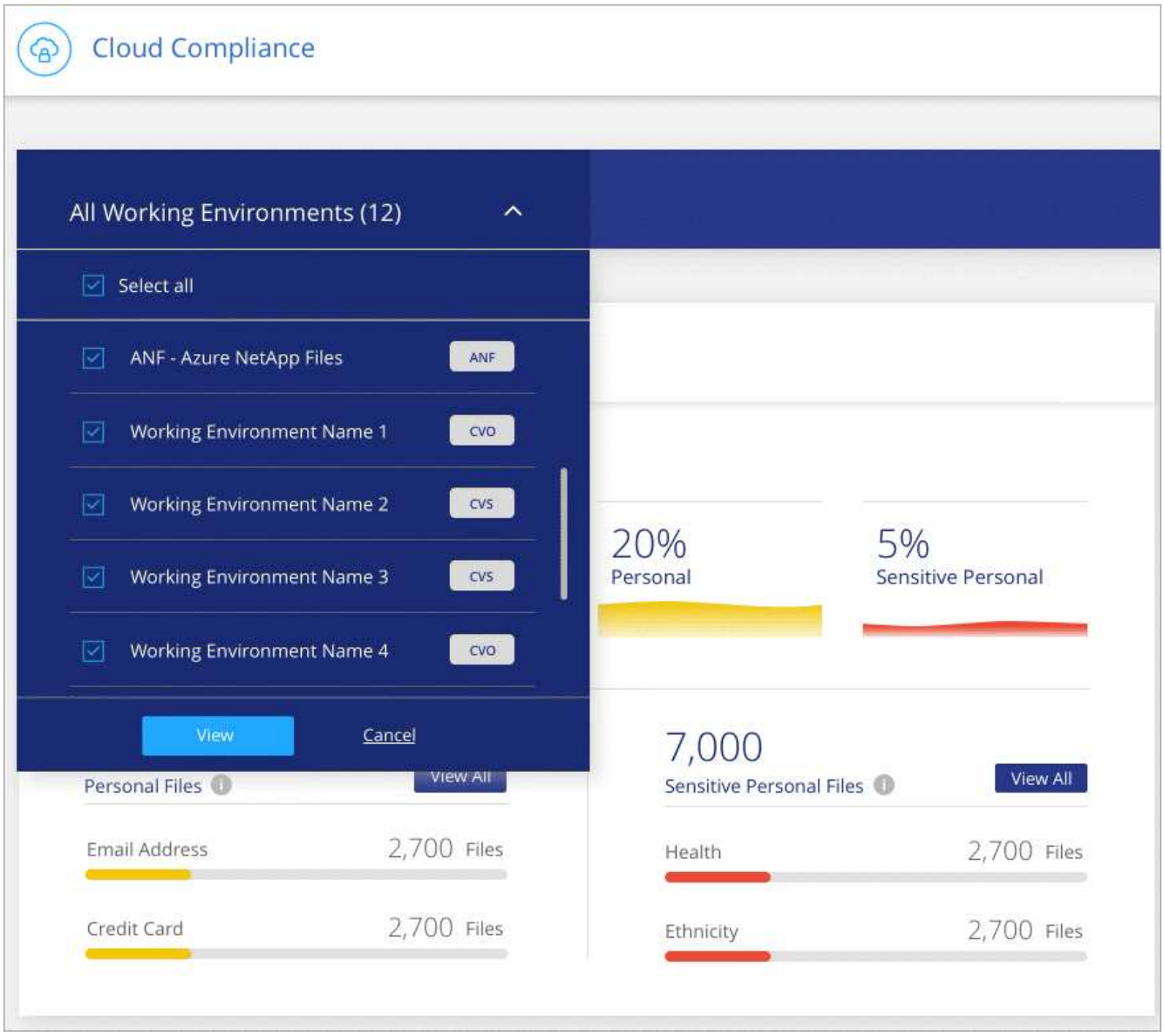
Visualizzazione dei dati da ambienti di lavoro specifici

Puoi filtrare i contenuti della dashboard Cloud Compliance per visualizzare i dati di conformità per tutti gli ambienti di lavoro e i database o solo per ambienti di lavoro specifici.

Quando filtri la dashboard, Cloud Compliance regola i dati di conformità e invia report solo agli ambienti di lavoro selezionati.

Fasi

1. Fare clic sul menu a discesa del filtro, selezionare gli ambienti di lavoro per i quali si desidera visualizzare i dati e fare clic su **View** (Visualizza).



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)

Da ogni pagina di analisi è possibile 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.

Ciascun elenco di file include le seguenti informazioni:

- Nome del file
- Tipo di ubicazione
- Ambiente di lavoro
- Repository di storage
- Protocollo
- 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 o nella pagina di analisi. I file vengono visualizzati solo nei report CSV.

Visualizzazione dei report di conformità

Cloud Compliance fornisce report che puoi utilizzare per comprendere meglio lo stato del programma per la privacy dei dati della tua organizzazione.

Per impostazione predefinita, il dashboard Cloud Compliance visualizza i dati di conformità per tutti gli ambienti di lavoro e i database. Se si desidera visualizzare report contenenti dati solo per alcuni ambienti di lavoro, selezionare gli ambienti di lavoro.

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.

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. Il report contiene le seguenti informazioni:

Stato di compliance

R punteggio di severità e la distribuzione dei dati, sia che si tratti di dati personali, non sensibili o sensibili.

Panoramica della valutazione

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

Argomenti trattati in questa valutazione

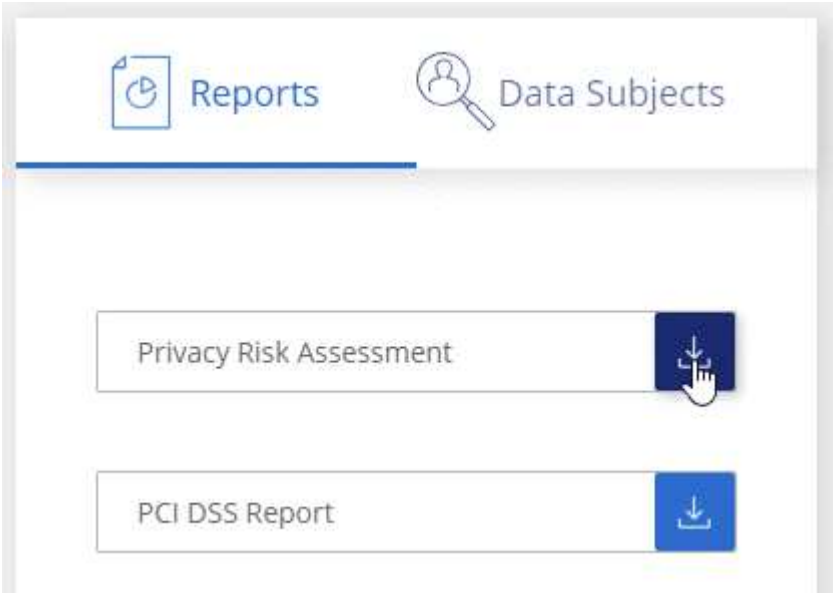
Il numero di persone, per località, per le quali sono stati trovati identificatori nazionali.

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 **Cloud 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%
4	Tre delle variabili sono maggiori del 3%
5	Una delle variabili è maggiore del 6%
6	Due delle variabili sono maggiori del 6%
7	Tre delle variabili sono maggiori del 6%
8	Una delle variabili è maggiore del 15%
9	Due delle variabili sono maggiori del 15%
10	Tre delle variabili sono maggiori del 15%

Report PCI DSS

Il report PCI DSS (Payment Card Industry Data Security Standard) consente di identificare la distribuzione delle informazioni sulle carte di credito nei file. Il report contiene le seguenti informazioni:

Panoramica
: Quanti file contengono informazioni sulla carta di credito e in quali ambienti di lavoro.

Crittografia
: La percentuale di file contenenti informazioni sulla carta di credito presenti in ambienti di lavoro crittografati o non crittografati. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Protezione ransomware
: La percentuale di file contenenti informazioni sulla carta di credito che si trovano in ambienti di lavoro in cui la protezione ransomware è attivata o meno. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Conservazione
: Il periodo di tempo in cui i file sono stati modificati per l'ultima volta. Ciò è utile perché non è necessario conservare le informazioni della carta di credito per un periodo di tempo superiore a quello necessario per elaborarle.

Distribuzione delle informazioni sulla carta di credito

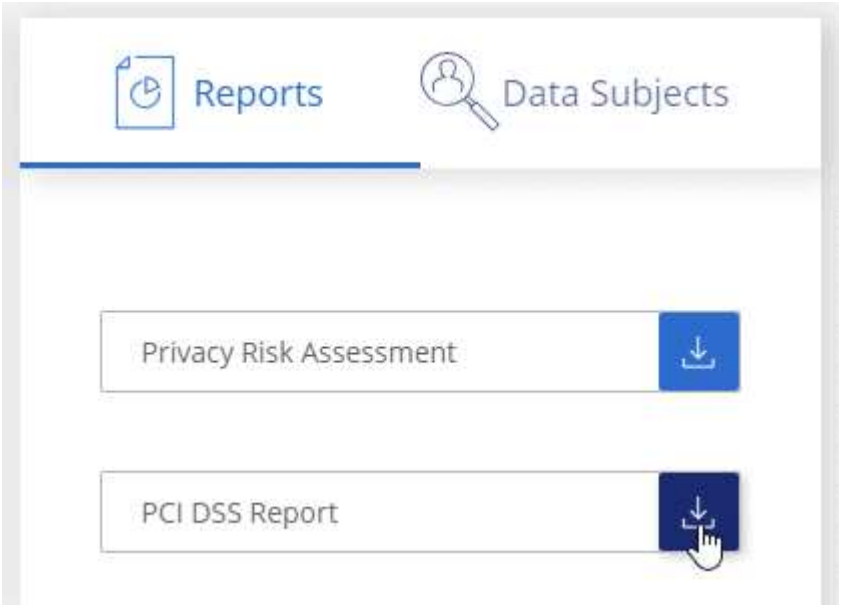
Gli ambienti di lavoro in cui sono state rilevate le informazioni sulla carta di credito e se sono attivate la crittografia e la protezione ransomware.

Generazione del rapporto PCI DSS

Accedere alla scheda Compliance per generare il report.

Fasi

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



Risultato

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

Report HIPAA

Il report HIPAA (Health Insurance Portability and Accountability Act) consente di identificare i file contenenti informazioni sulla salute. È progettato per soddisfare i requisiti della tua organizzazione in materia di privacy dei dati HIPAA. Le informazioni che la Cloud Compliance cerca includono:

- Schema di riferimento per lo stato di salute
- ICD-10-CM Codice medico
- Codice medico ICD-9-CM
- HR – Categoria di salute
- Categoria Health Application Data

Il report contiene le seguenti informazioni:

Panoramica

Quanti file contengono informazioni sullo stato di salute e in quali ambienti di lavoro.

Crittografia

La percentuale di file contenenti informazioni sullo stato di salute che si trovano in ambienti di lavoro crittografati o non crittografati. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Protezione ransomware

La percentuale di file contenenti informazioni sullo stato di salute che si trovano in ambienti di lavoro in cui la protezione ransomware è attivata o meno. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Conservazione

Il periodo di tempo in cui i file sono stati modificati per l'ultima volta. Ciò è utile perché non è necessario conservare le informazioni sulla salute per un periodo di tempo superiore a quello necessario per elaborarle.

Distribuzione delle informazioni sanitarie

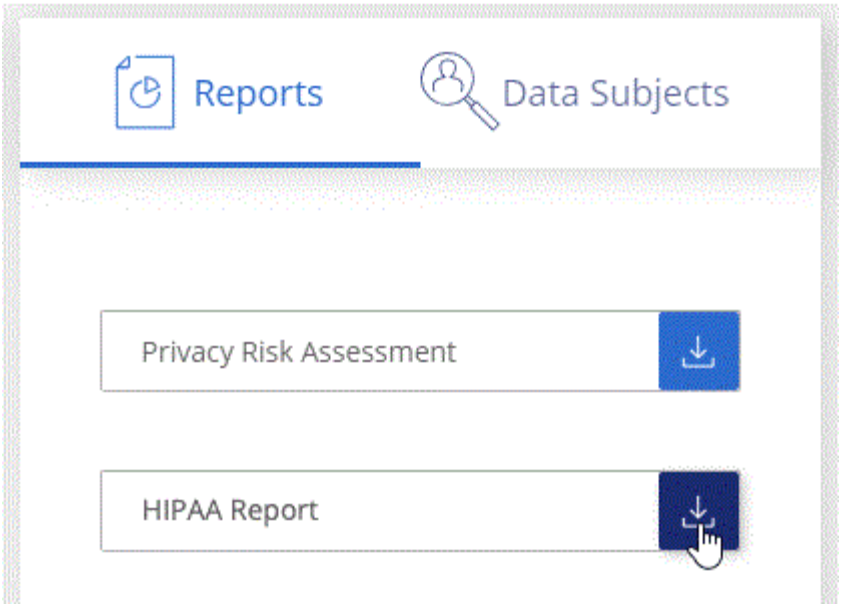
Gli ambienti di lavoro in cui sono state trovate le informazioni di salute e se sono attivate la crittografia e la protezione ransomware.

Generazione del report HIPAA

Accedere alla scheda Compliance per generare il report.

Fasi

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



Risultato

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

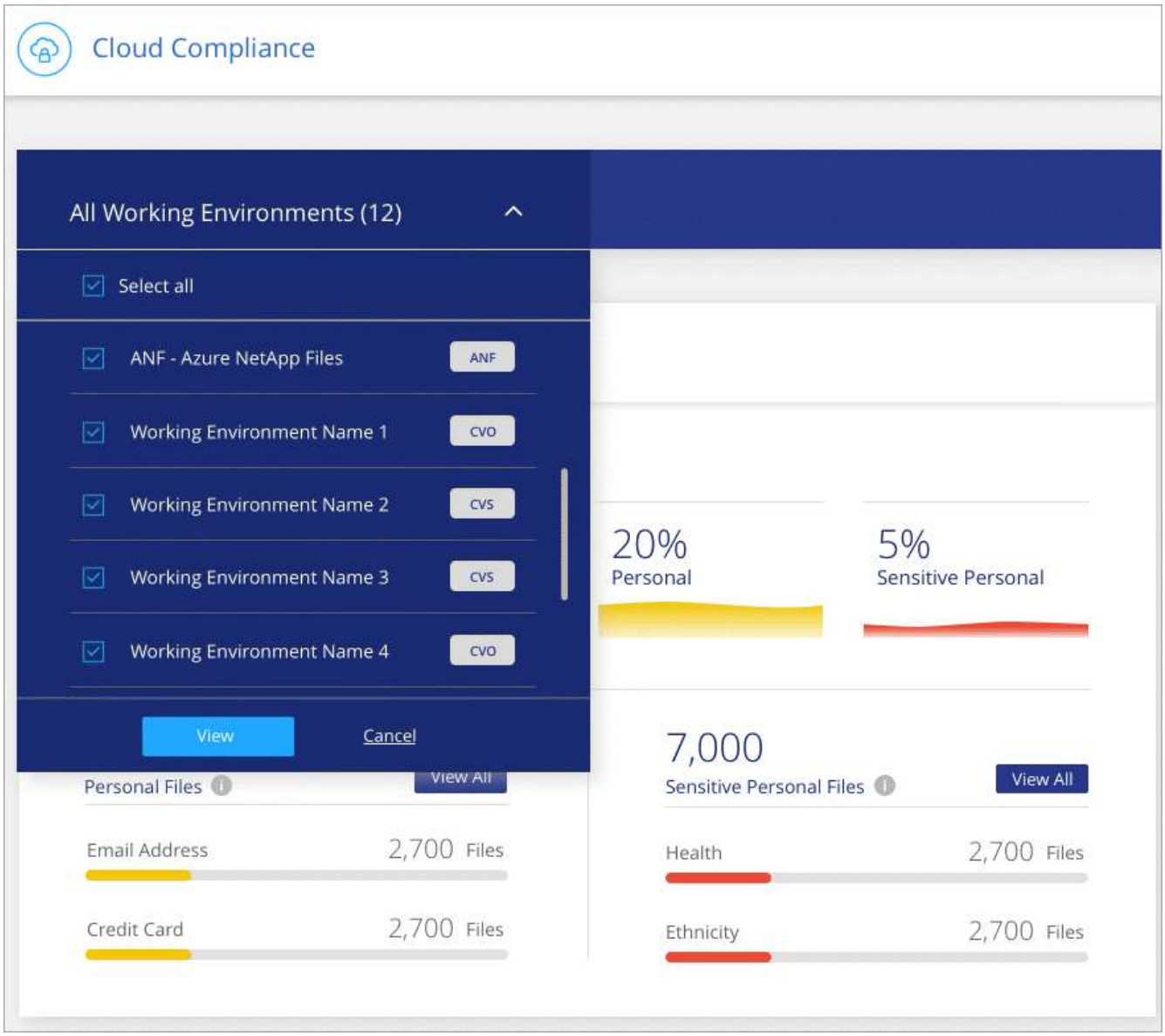
Selezione degli ambienti di lavoro per i report

Puoi filtrare i contenuti della dashboard Cloud Compliance per visualizzare i dati di conformità per tutti gli ambienti di lavoro e i database o solo per ambienti di lavoro specifici.

Quando filtri la dashboard, Cloud Compliance regola i dati di conformità e invia report solo agli ambienti di lavoro selezionati.

Fasi

1. Fare clic sul menu a discesa del filtro, selezionare gli ambienti di lavoro per i quali si desidera visualizzare i dati e fare clic su **View** (Visualizza).



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 di file per 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".

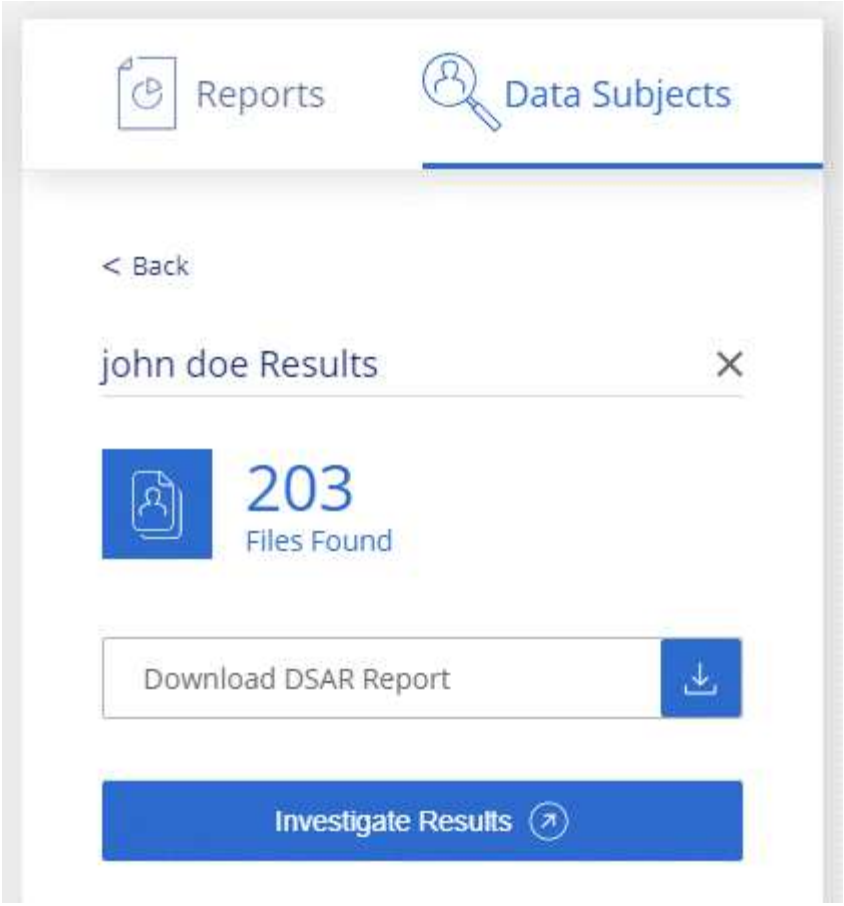
Quando si ricercano i nomi dei soggetti dati, è supportato solo l'inglese. Il supporto per altre lingue verrà aggiunto in un secondo momento.

La ricerca dei dati non è attualmente supportata nei database.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Cloud 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 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.
   - **Investigate Results**: Pagina che consente di analizzare i dati ricercando, ordinando, espandendo i dettagli di un file specifico e scaricando l'elenco dei file.

     Se sono presenti più di 10,000 risultati, nell'elenco dei file vengono visualizzati solo i primi 10,000 risultati.

Disattivazione della conformità al cloud

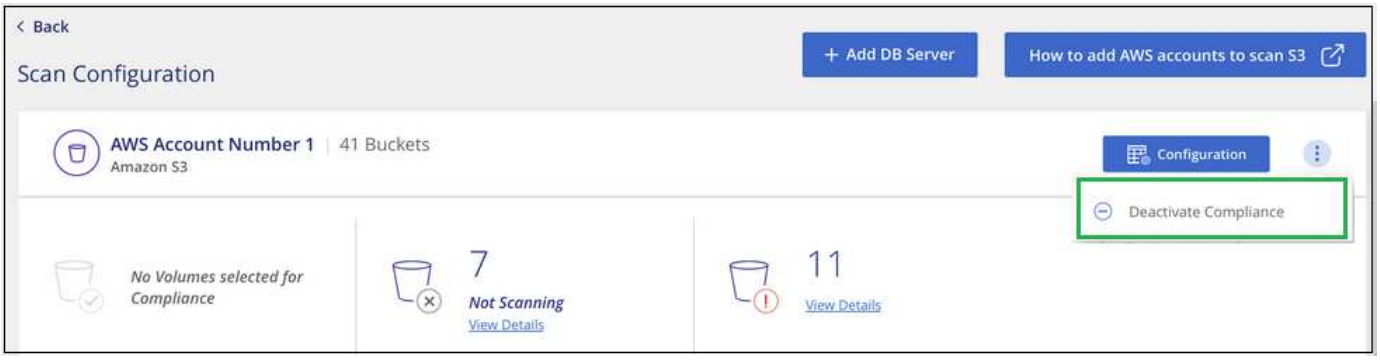
Se necessario, puoi impedire alla conformità cloud di eseguire la scansione di uno o più ambienti di lavoro o database. Puoi anche eliminare l'istanza Cloud Compliance se non desideri più utilizzare Cloud Compliance con i tuoi ambienti di lavoro.

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 conformità dall'istanza Cloud Compliance (i dati dell'ambiente di lavoro o del database stesso non vengono cancellati).

Fasi

Dalla pagina *Scan Configuration*, fare clic su Nella riga dell'ambiente di lavoro, quindi fare clic su **Disattiva conformità**.



È inoltre possibile disattivare le scansioni di conformità per un ambiente di lavoro dal pannello servizi quando si seleziona l'ambiente di lavoro.

Eliminazione dell'istanza di Cloud Compliance

Se non si desidera più utilizzare Cloud Compliance, è possibile eliminare l'istanza di Cloud Compliance. 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?

La conformità al cloud è un'offerta cloud che utilizza la tecnologia basata sull'intelligenza artificiale (ai) per aiutare le organizzazioni a comprendere il contesto dei dati e identificare i dati sensibili nelle configurazioni Azure NetApp Files, nei sistemi Cloud Volumes ONTAP ospitati in AWS o Azure, nei bucket Amazon S3 e nei database.

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, HIPAA 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 da GDPR, CCPA, HIPAA e 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 gestiti da Cloud Volumes ONTAP e Azure NetApp Files. Cloud Compliance può anche eseguire la scansione dei dati memorizzati nei bucket Amazon S3.

Inoltre, Cloud Compliance è in grado di eseguire la scansione di database che si trovano ovunque, non devono essere gestiti da Cloud Manager.

"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?

Cloud Compliance implementa un altro livello di intelligenza artificiale insieme al sistema Cloud Manager e ai sistemi storage. Esegue quindi la scansione dei dati su volumi, bucket e database e indicizza le informazioni sui dati trovate.

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

Quanto costa la Cloud Compliance?

Il costo per l'utilizzo della conformità cloud dipende dalla quantità di dati che si sta scansionando. I primi 1 TB di dati che Cloud Compliance analizza in uno spazio di lavoro di Cloud Manager sono gratuiti. Per continuare a eseguire la scansione dei dati dopo tale data, è necessario un abbonamento ad AWS o Azure Marketplace. Vedere "prezzi" per ulteriori informazioni.

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 PCI DSS
: Consente di identificare la distribuzione delle informazioni sulla carta di credito nei file. "Scopri di più".

Report HIPAA
: Consente di identificare la distribuzione delle informazioni sanitarie tra i file. "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 GP2 da 500 GB.

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

La modifica o il ridimensionamento del tipo di istanza/VM non è supportato. È necessario utilizzare le dimensioni predefinite fornite.

"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.

Quali tipi di file sono supportati?

Cloud Compliance esegue la scansione di tutti i file per individuare informazioni su categorie e metadati e visualizza tutti i tipi di file nella sezione tipi di file della dashboard.

Quando Cloud Compliance rileva le informazioni personali identificabili (PII) o esegue una ricerca DSAR, sono supportati solo i seguenti formati di file: .PDF, .DOCX, .DOC, .PPTX, .XLS, XLSX, .CSV, .TXT, .RTF E .JSON.

Come posso abilitare la conformità al cloud?

Innanzitutto, devi implementare un'istanza di Cloud Compliance in Cloud Manager. Una volta eseguita l'istanza, è possibile abilitarla negli ambienti di lavoro e nei database esistenti dalla scheda **Compliance** 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?

La scansione dei dati direttamente da un ambiente di lavoro ONTAP on-premise non è supportata. Tuttavia, è possibile eseguire la scansione dei dati ONTAP on-premise replicando i dati NFS o CIFS on-premise in un ambiente di lavoro Cloud Volumes ONTAP e attivando la conformità su tali volumi. Stiamo pianificando di supportare la conformità al cloud con offerte cloud aggiuntive come Cloud Volumes Service.

"Scopri di più".

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.

Inoltre, se si desidera consentire a determinati utenti di visualizzare solo i risultati della scansione Cloud Compliance senza avere la possibilità di gestire le impostazioni Cloud Compliance, è possibile assegnare a tali utenti il ruolo *Cloud Compliance Viewer*.

"Scopri di più".

Informazioni sul copyright

Informazioni sul marchio commerciale