



Implementare la classificazione BlueXP

BlueXP classification

NetApp
April 03, 2024

This PDF was generated from <https://docs.netapp.com/it-it/bluexp-classification/task-deploy-overview.html> on April 03, 2024. Always check docs.netapp.com for the latest.

Sommario

- Implementare la classificazione BlueXP 1
 - Quale implementazione della classificazione BlueXP dovresti utilizzare? 1
 - Implementare la classificazione BlueXP nel cloud utilizzando BlueXP 1
 - Installare la classificazione BlueXP su un host con accesso a Internet 11
 - Installare la classificazione BlueXP su un host Linux senza accesso Internet 31
 - Verificare che l'host Linux sia pronto per installare la classificazione BlueXP 43

Implementare la classificazione BlueXP

Quale implementazione della classificazione BlueXP dovresti utilizzare?

Puoi implementare la classificazione BlueXP in modi diversi. Scopri quale metodo soddisfa le tue esigenze.

La classificazione BlueXP può essere implementata nei seguenti modi:

- ["Implementazione nel cloud con BlueXP"](#). BlueXP implementerà l'istanza di classificazione BlueXP nella stessa rete di provider cloud del connettore BlueXP.
- ["Installazione su un host Linux con accesso a Internet"](#). Installare la classificazione BlueXP su un host Linux nella rete o su un host Linux nel cloud che dispone di accesso a Internet. Questo tipo di installazione può essere una buona opzione se preferisci analizzare i sistemi ONTAP in loco utilizzando un'istanza di classificazione BlueXP che si trova anche on-premise, ma non è un requisito.
- ["Installazione su un host Linux in un sito locale senza accesso a Internet"](#), Noto anche come *private mode*. questo tipo di installazione, che utilizza uno script di installazione, è utile per i siti protetti.

Sia l'installazione su un host Linux con accesso a Internet che l'installazione in loco su un host Linux senza accesso a Internet utilizzano uno script di installazione. Lo script inizia controllando se il sistema e l'ambiente soddisfano i prerequisiti. Se i prerequisiti vengono soddisfatti, viene avviata l'installazione. Se si desidera verificare i prerequisiti indipendentemente dall'esecuzione dell'installazione di classificazione BlueXP, è possibile scaricare un pacchetto software separato che esegue solo i prerequisiti.

Fare riferimento a ["Verificare che l'host Linux sia pronto per installare la classificazione BlueXP"](#).

Implementare la classificazione BlueXP nel cloud utilizzando BlueXP

Completare alcuni passaggi per implementare la classificazione BlueXP nel cloud. BlueXP implementerà l'istanza di classificazione BlueXP nella stessa rete di provider cloud del connettore BlueXP.

Nota: È anche possibile ["Installare la classificazione BlueXP su un host Linux con accesso a Internet"](#). Questo tipo di installazione può essere una buona opzione se si preferisce eseguire la scansione dei sistemi ONTAP on-premise utilizzando un'istanza di classificazione BlueXP che si trova anche on-premise, ma non è un requisito. Il software funziona esattamente allo stesso modo, indipendentemente dal metodo di installazione scelto.

Avvio rapido

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



Creare un connettore

Se non si dispone già di un connettore, crearne uno. Vedere ["Creazione di un connettore in AWS"](#), ["Creazione](#)

di un connettore in Azure", o. ["Creazione di un connettore in GCP"](#).

Puoi anche farlo ["Installare il connettore on-premise"](#) Su un host Linux nella rete o su un host Linux nel cloud.

2

Esaminare i prerequisiti

Assicurarsi che l'ambiente soddisfi i prerequisiti. Ciò include l'accesso a Internet in uscita per l'istanza, la connettività tra il connettore e la classificazione BlueXP sulla porta 443 e altro ancora. [Consulta l'elenco completo](#).

3

Implementare la classificazione BlueXP

Avviare l'installazione guidata per implementare l'istanza di classificazione BlueXP nel cloud.

4

Iscriviti al servizio di classificazione BlueXP

I primi 1 TB di dati che la classificazione BlueXP scansiona in BlueXP sono gratuiti per 30 giorni. Per continuare a eseguire la scansione dei dati dopo tale data, è necessario un abbonamento BlueXP tramite il proprio provider cloud Marketplace o una licenza BYOL di NetApp.

Creare un connettore

Se non disponi già di un connettore, crea un connettore nel tuo cloud provider. Vedere ["Creazione di un connettore in AWS"](#) oppure ["Creazione di un connettore in Azure"](#), o. ["Creazione di un connettore in GCP"](#). Nella maggior parte dei casi, probabilmente si dispone di un connettore configurato prima di tentare di attivare la classificazione BlueXP, perché la maggior parte ["Le funzionalità di BlueXP richiedono un connettore"](#), ma in alcuni casi è necessario impostarne uno ora.

Esistono alcuni scenari in cui è necessario utilizzare un connettore implementato in uno specifico cloud provider:

- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in AWS, Amazon FSX per ONTAP o nei bucket 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.
 - Per Azure NetApp Files, deve essere implementato nella stessa regione dei volumi che si desidera sottoporre a scansione.
- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in GCP, si utilizza un connettore in GCP.

I sistemi ONTAP on-premise, le condivisioni di file non NetApp, lo storage a oggetti S3 generico, i database, le cartelle OneDrive, gli account SharePoint e gli account Google Drive possono essere sottoposti a scansione quando si utilizza uno di questi connettori cloud.

Nota: È anche possibile ["Installare il connettore on-premise"](#) Su un host Linux nella rete o nel cloud. Alcuni utenti che intendono installare BlueXP classification on-premise possono anche scegliere di installare il connettore on-premise.

Come puoi vedere, potrebbero esserci alcune situazioni in cui devi utilizzare ["Connettori multipli"](#).

Supporto per le regioni governative

La classificazione BlueXP è supportata quando il connettore viene implementato in un'area governativa (AWS GovCloud, Azure Gov o Azure DoD). Se implementato in questo modo, la classificazione BlueXP presenta le seguenti restrizioni:

- Impossibile eseguire la scansione di account OneDrive, SharePoint e Google Drive.
- La funzionalità dell'etichetta AIP (Microsoft Azure Information Protection) non può essere integrata.

["Ulteriori informazioni sull'implementazione del connettore in un'area pubblica"](#).

Esaminare i prerequisiti

Esaminare i seguenti prerequisiti per assicurarsi di disporre di una configurazione supportata prima di implementare la classificazione BlueXP nel cloud. Quando si implementa la classificazione BlueXP nel cloud, si trova nella stessa subnet del connettore.

Abilitare l'accesso a Internet in uscita dalla classificazione BlueXP

La classificazione BlueXP richiede l'accesso a Internet in uscita. Se la rete fisica o virtuale utilizza un server proxy per l'accesso a Internet, assicurarsi che l'istanza di classificazione BlueXP disponga dell'accesso a Internet in uscita per contattare i seguenti endpoint. Il proxy deve essere non trasparente, al momento non supportiamo proxy trasparenti.

Esaminare la tabella appropriata riportata di seguito a seconda che si stia implementando la classificazione BlueXP in AWS, Azure o GCP.

Endpoint richiesti per AWS

Endpoint	Scopo
https://api.bluexp.netapp.com	Comunicazione con il servizio BlueXP, che include gli account NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicazione con il sito Web BlueXP 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 https://user-feedback-store-prod.s3.us-west-2.amazonaws.com https://customer-data-production.s3.us-west-2.amazonaws.com	Abilita la classificazione BlueXP per accedere e scaricare manifesti e modelli e per inviare registri e metriche.

Endpoint richiesti per Azure

Endpoint	Scopo
https://api.bluexp.netapp.com	Comunicazione con il servizio BlueXP, che include gli account NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicazione con il sito Web BlueXP per l'autenticazione utente centralizzata.
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Fornisce accesso a immagini software, manifesti, modelli e per inviare registri e metriche.
https://support.compliance.api.bluexp.netapp.com/	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.

Endpoint richiesti per GCP

Endpoint	Scopo
https://api.bluexp.netapp.com	Comunicazione con il servizio BlueXP, che include gli account NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicazione con il sito Web BlueXP per l'autenticazione utente centralizzata.

Endpoint	Scopo
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srrn.cloudfront.net/ https://production.cloudflare.docker.com/	Fornisce accesso a immagini software, manifesti, modelli e per inviare registri e metriche.
https://support.compliance.api.bluexp.netapp.com/	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.

Assicurarsi che BlueXP disponga delle autorizzazioni necessarie

Assicurarsi che BlueXP disponga delle autorizzazioni per distribuire le risorse e creare gruppi di protezione per l'istanza di classificazione BlueXP. Le autorizzazioni BlueXP più recenti sono disponibili in ["Le policy fornite da NetApp"](#).

Assicurarsi che BlueXP Connector possa accedere alla classificazione BlueXP

Garantire la connettività tra il connettore e l'istanza di classificazione BlueXP. Il gruppo di protezione per il connettore deve consentire il traffico in entrata e in uscita sulla porta 443 da e verso l'istanza di classificazione BlueXP. Questa connessione consente l'implementazione dell'istanza di classificazione BlueXP e consente di visualizzare le informazioni nelle schede Compliance e Governance. La classificazione BlueXP è supportata nelle regioni governative di AWS e Azure.

Per le implementazioni di AWS e AWS GovCloud sono richieste regole aggiuntive per i gruppi di sicurezza in entrata e in uscita. Vedere ["Regole per il connettore in AWS"](#) per ulteriori informazioni.

Per le implementazioni di Azure e Azure Government sono richieste regole aggiuntive per i gruppi di sicurezza in entrata e in uscita. Vedere ["Regole per il connettore in Azure"](#) per ulteriori informazioni.

Assicurarsi che sia possibile mantenere in esecuzione la classificazione BlueXP

L'istanza di classificazione BlueXP deve rimanere attiva per eseguire una scansione continua dei dati.

Garantire la connettività del browser Web alla classificazione BlueXP

Una volta attivata la classificazione BlueXP, assicurarsi che gli utenti accedano all'interfaccia BlueXP da un host che dispone di una connessione all'istanza di classificazione BlueXP.

L'istanza di classificazione BlueXP 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 BlueXP deve disporre di una connessione a tale indirizzo IP privato. Tale connessione può provenire da una connessione diretta al provider cloud (ad esempio, una VPN) o da un host all'interno della stessa rete dell'istanza di classificazione BlueXP.

Controllare i limiti della vCPU

Assicurati che il limite vCPU del tuo cloud provider consenta l'implementazione di un'istanza con il numero necessario di core. È necessario verificare il limite vCPU per la famiglia di istanze pertinente nella regione in cui è in esecuzione BlueXP. ["Vedere i tipi di istanza richiesti"](#).

Per ulteriori informazioni sui limiti delle vCPU, consultare i seguenti collegamenti:

- ["Documentazione AWS: Quote di servizio Amazon EC2"](#)
- ["Documentazione di Azure: Quote vCPU delle macchine virtuali"](#)

- ["Documentazione di Google Cloud: Quote delle risorse"](#)

Si noti che è possibile implementare la classificazione BlueXP su un'istanza in ambienti cloud AWS con meno CPU e meno RAM, ma l'utilizzo di questi sistemi presenta delle limitazioni. Vedere ["Utilizzando un tipo di istanza più piccolo"](#) per ulteriori informazioni.

Implementare la classificazione BlueXP nel cloud

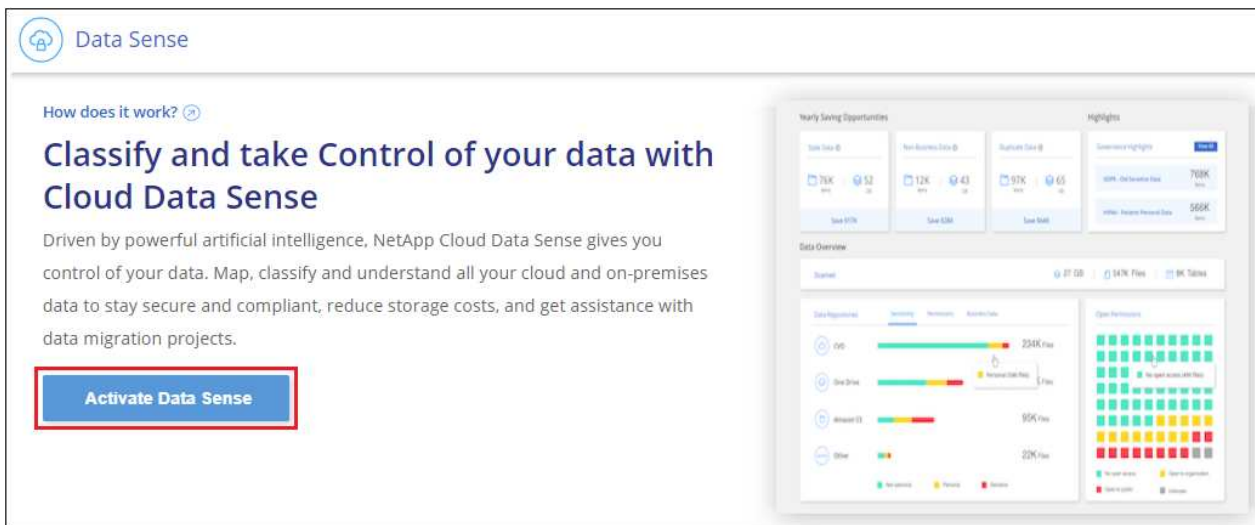
Seguire questi passaggi per implementare un'istanza della classificazione BlueXP nel cloud. Il connettore implementerà l'istanza nel cloud, quindi installerà il software di classificazione BlueXP su tale istanza.

Quando si implementa la classificazione BlueXP da un connettore BlueXP in un ambiente AWS, è possibile selezionare la dimensione predefinita dell'istanza oppure scegliere tra due tipi di istanze più piccoli. ["Vedere i tipi di istanze e le limitazioni disponibili"](#). Nelle regioni in cui il tipo di istanza predefinito non è disponibile, la classificazione BlueXP viene eseguita su un ["tipo di istanza alternativo"](#).

Implementazione in AWS

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**.



2. Fare clic su **Activate Data Sense** (attiva rilevamento dati).
3. Dalla pagina *Installation*, fare clic su **Deploy > Deploy** per utilizzare le dimensioni dell'istanza "Large" e avviare la procedura guidata di implementazione del cloud.
4. La procedura guidata visualizza lo stato di avanzamento durante le fasi di implementazione. In caso di problemi, il sistema si arresta e richiede l'immissione.



5. Una volta implementata l'istanza e installata la classificazione BlueXP, fare clic su **Continue to Configuration** (continua alla configurazione) per accedere alla pagina *Configuration* (Configurazione).

Implementazione in Azure

Fasi

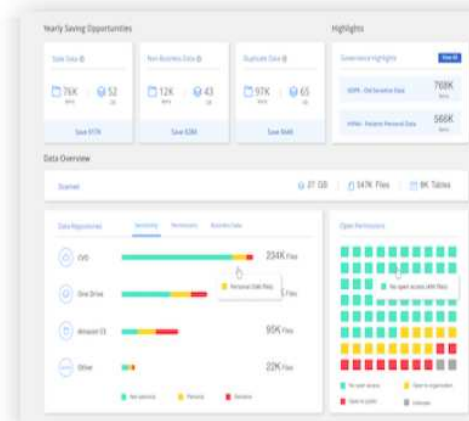
1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Activate Data Sense** (attiva rilevamento dati).

How does it work? ⓘ

Classify and take Control of your data with Cloud Data Sense

Driven by powerful artificial intelligence, NetApp Cloud Data Sense gives you control of your data. Map, classify and understand all your cloud and on-premises data to stay secure and compliant, reduce storage costs, and get assistance with data migration projects.

Activate Data Sense



3. Fare clic su **Deploy** per avviare la procedura guidata di implementazione del cloud.

Install your Data Sense instance

Select your preferred deployment location:

[Learn more about deploying Data Sense ⓘ](#)

Cloud Environment

I want BlueXP to deploy the instance and install Data Sense

> BlueXP will deploy a new machine automatically in the chosen cloud environment.
 > You will be taken to an installation wizard where you can configure your Data Sense installation.

Deploy

On Premise

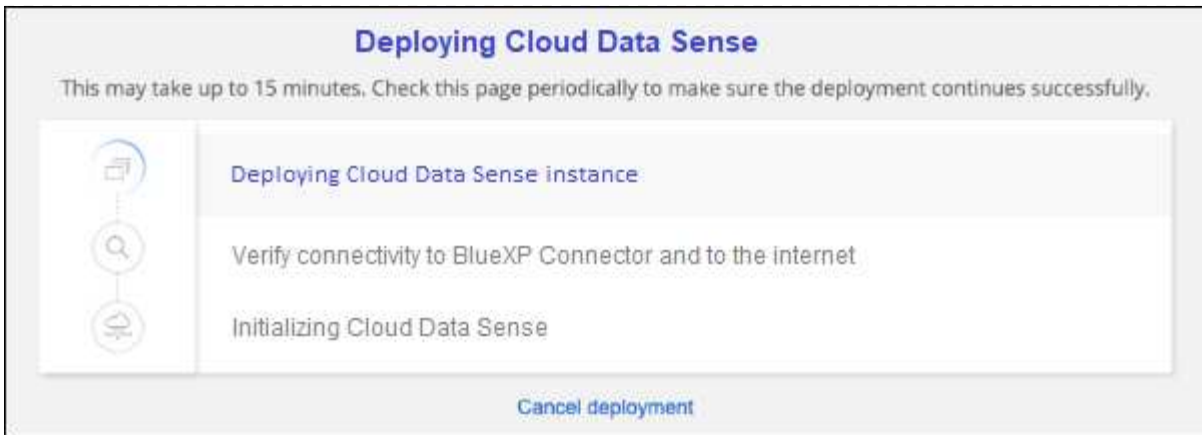
I deployed an instance and I'm ready to install Data Sense

Deploy

I prepared a local machine and I'm ready to install Data Sense

Deploy

4. La procedura guidata visualizza lo stato di avanzamento durante le fasi di implementazione. In caso di problemi, il sistema si arresta e richiede l'immissione.

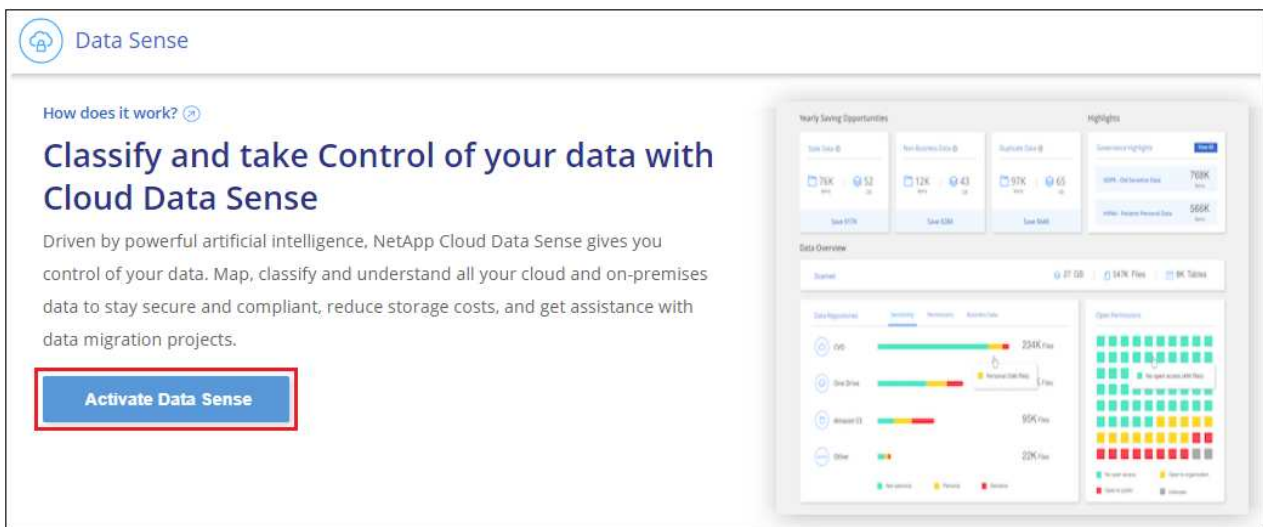


- Una volta implementata l'istanza e installata la classificazione BlueXP, fare clic su **Continue to Configuration** (continua alla configurazione) per accedere alla pagina *Configuration* (Configurazione).

Implementazione in Google Cloud

Fasi

- Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**.
- Fare clic su **Activate Data Sense** (attiva rilevamento dati).




- Fare clic su **Deploy** per avviare la procedura guidata di implementazione del cloud.

Install your Data Sense instance

Select your preferred deployment location:

[Learn more about deploying Data Sense](#)

Cloud Environment




I want BlueXP to deploy the instance and install Data Sense

> BlueXP will deploy a new machine automatically in the chosen cloud environment.
> You will be taken to an installation wizard where you can configure your Data Sense installation.

Deploy

^




I deployed an instance and I'm ready to install Data Sense

Deploy

v

On Premise



I prepared a local machine and I'm ready to install Data Sense

Deploy

v

4. La procedura guidata visualizza lo stato di avanzamento durante le fasi di implementazione. In caso di problemi, il sistema si arresta e richiede l'immissione.

Deploying Cloud Data Sense

This may take up to 15 minutes. Check this page periodically to make sure the deployment continues successfully.







Deploying Cloud Data Sense instance

Verify connectivity to BlueXP Connector and to the internet

Initializing Cloud Data Sense

Cancel deployment

5. Una volta implementata l'istanza e installata la classificazione BlueXP, fare clic su **Continue to Configuration** (continua alla configurazione) per accedere alla pagina *Configuration* (Configurazione).

Risultato

BlueXP implementa l'istanza di classificazione BlueXP nel tuo cloud provider.

Gli aggiornamenti al software di classificazione BlueXP Connector e BlueXP sono automatizzati purché le istanze dispongano di connettività Internet.

Cosa c'è di nuovo

Dalla pagina di configurazione è possibile selezionare le origini dati da sottoporre a scansione.

Puoi anche farlo ["Impostare la licenza per la classificazione BlueXP"](#) a questo punto. Non ti verrà addebitato alcun costo fino al termine della prova gratuita di 30 giorni.

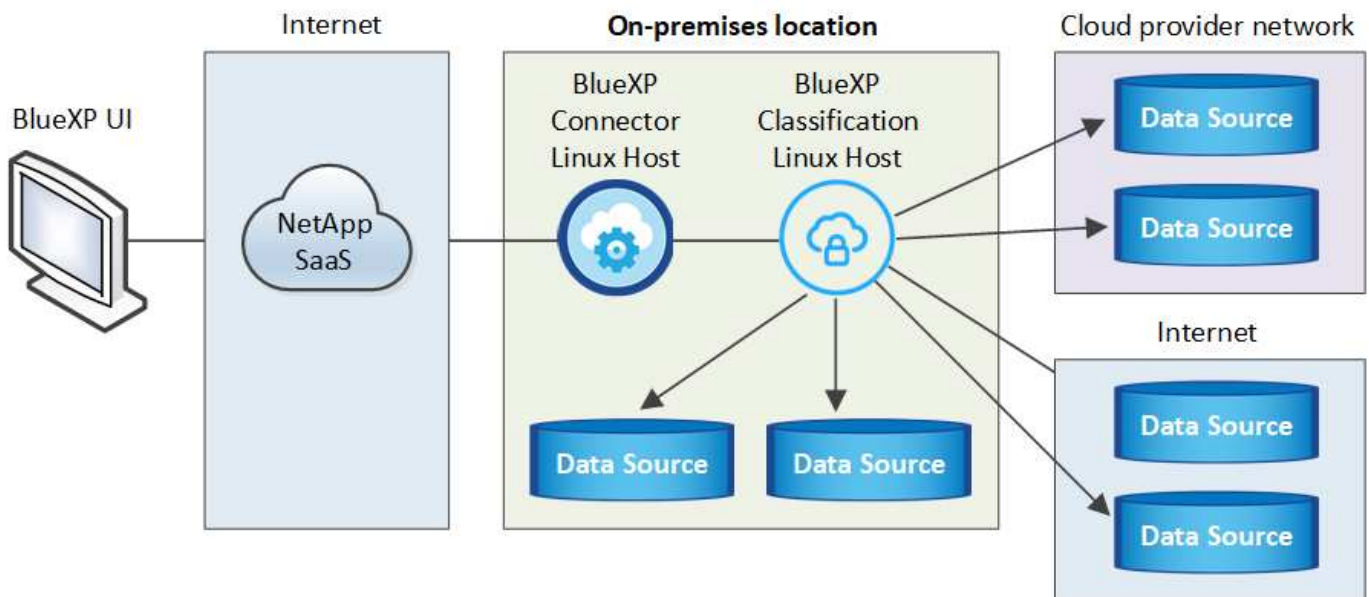
Installare la classificazione BlueXP su un host con accesso a Internet

Completare alcuni passaggi per installare la classificazione BlueXP su un host Linux nella rete o su un host Linux nel cloud con accesso a Internet. Come parte di questa installazione, sarà necessario implementare manualmente l'host Linux nella rete o nel cloud.

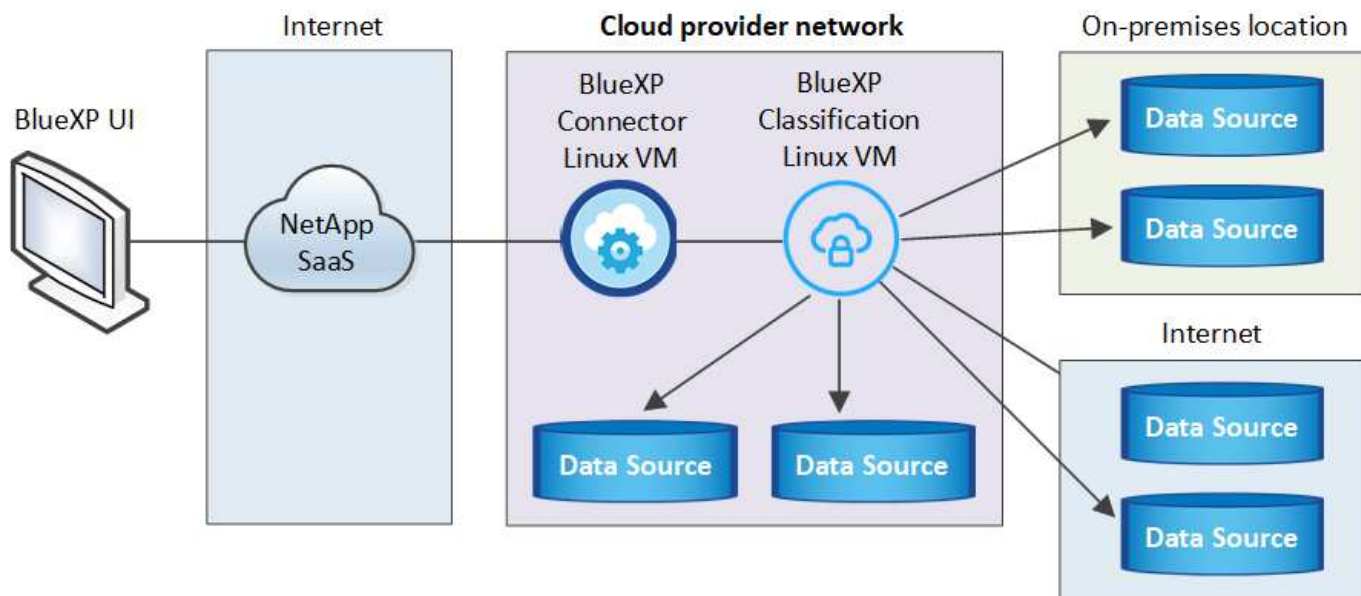
L'installazione on-premise potrebbe essere una buona opzione se si preferisce eseguire la scansione dei sistemi ONTAP on-premise utilizzando un'istanza di classificazione BlueXP che si trova anche on-premise, ma questo non è un requisito. Il software funziona esattamente allo stesso modo, indipendentemente dal metodo di installazione scelto.

Lo script di installazione della classificazione BlueXP inizia verificando se il sistema e l'ambiente soddisfano i prerequisiti richiesti. Se tutti i prerequisiti sono soddisfatti, viene avviata l'installazione. Se si desidera verificare i prerequisiti indipendentemente dall'esecuzione dell'installazione di classificazione BlueXP, è possibile scaricare un pacchetto software separato che esegue solo i prerequisiti. ["Scopri come verificare se il tuo host Linux è pronto per installare la classificazione BlueXP"](#).

L'installazione tipica su un host Linux *in sede* ha i seguenti componenti e connessioni.



L'installazione tipica su un host Linux *nel cloud* ha i seguenti componenti e connessioni.



Per configurazioni molto grandi in cui si eseguono scansioni di petabyte di dati, è possibile includere più host per fornire ulteriore potenza di elaborazione. Quando si utilizzano più sistemi host, il sistema primario è denominato *nodo Manager* e i sistemi aggiuntivi che forniscono potenza di elaborazione aggiuntiva sono denominati *nodi scanner*.

Nota: È anche possibile ["Installare la classificazione BlueXP in un sito on-premise che non dispone di accesso a Internet"](#) per siti completamente sicuri.

Avvio rapido

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

1

Creare un connettore

Se non si dispone già di un connettore, ["Implementare il connettore on-premise"](#) Su un host Linux nella rete o su un host Linux nel cloud.

Puoi anche creare un connettore con il tuo cloud provider. Vedere ["Creazione di un connettore in AWS"](#), ["Creazione di un connettore in Azure"](#), o ["Creazione di un connettore in GCP"](#).

2

Esaminare i prerequisiti

Assicurarsi che l'ambiente soddisfi i prerequisiti. Ciò include l'accesso a Internet in uscita per l'istanza, la connettività tra il connettore e la classificazione BlueXP sulla porta 443 e altro ancora. [Consulta l'elenco completo](#).

È inoltre necessario un sistema Linux che soddisfi i requisiti di [requisiti seguenti](#).

3

Scarica e implementa la classificazione BlueXP

Scarica il software di classificazione Cloud BlueXP dal sito di supporto NetApp e copia il file di installazione sull'host Linux che intendi utilizzare. Quindi, avviare l'installazione guidata e seguire le istruzioni per

implementare l'istanza di classificazione BlueXP.

4

Iscriviti al servizio di classificazione BlueXP

I primi 1 TB di dati che la classificazione BlueXP scansiona in BlueXP sono gratuiti per 30 giorni. Per continuare a eseguire la scansione dei dati dopo tale data, è necessario un abbonamento al tuo provider cloud Marketplace o una licenza BYOL di NetApp.

Creare un connettore

Prima di installare e utilizzare la classificazione BlueXP, è necessario un connettore BlueXP. Nella maggior parte dei casi, probabilmente si dispone di un connettore configurato prima di tentare di attivare la classificazione BlueXP, perché la maggior parte ["Le funzionalità di BlueXP richiedono un connettore"](#), ma in alcuni casi è necessario impostarne uno ora.

Per crearne uno nel tuo ambiente di cloud provider, consulta la sezione ["Creazione di un connettore in AWS"](#), ["Creazione di un connettore in Azure"](#), o ["Creazione di un connettore in GCP"](#).

Esistono alcuni scenari in cui è necessario utilizzare un connettore implementato in uno specifico cloud provider:

- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in AWS, Amazon FSx per ONTAP o nei bucket 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.

Per Azure NetApp Files, deve essere implementato nella stessa regione dei volumi che si desidera sottoporre a scansione.

- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in GCP, si utilizza un connettore in GCP.

I sistemi ONTAP on-premise, le condivisioni di file non NetApp, lo storage a oggetti S3 generico, i database, le cartelle OneDrive, gli account SharePoint e gli account Google Drive possono essere sottoposti a scansione utilizzando uno di questi connettori cloud.

Nota: È anche possibile ["Implementare il connettore on-premise"](#) Su un host Linux nella rete o su un host Linux nel cloud. Alcuni utenti che intendono installare BlueXP classification on-premise possono anche scegliere di installare il connettore on-premise.

Come puoi vedere, potrebbero esserci alcune situazioni in cui devi utilizzare ["Connettori multipli"](#).

Quando si installa la classificazione BlueXP, è necessario l'indirizzo IP o il nome host del sistema di connessione. Queste informazioni saranno disponibili se il connettore è stato installato nella propria sede. Se il connettore è implementato nel cloud, è possibile trovare queste informazioni dalla console BlueXP: Fare clic sull'icona della Guida, selezionare **Support** e fare clic su **BlueXP Connector**.

Preparare il sistema host Linux

Il software di classificazione BlueXP deve essere eseguito su un host che soddisfi requisiti specifici del sistema operativo, requisiti di RAM, requisiti software e così via. L'host Linux può trovarsi nella rete o nel cloud.

Assicurarsi che sia possibile mantenere in esecuzione la classificazione BlueXP. Il sistema di classificazione BlueXP deve rimanere attivo per eseguire una scansione continua dei dati.

- La classificazione BlueXP non è supportata su un host condiviso con altre applicazioni: L'host deve essere un host dedicato.
- Quando si costruisce il sistema host in sede, è possibile scegliere tra tre dimensioni del sistema a seconda delle dimensioni del set di dati che si prevede di sottoporre a scansione di classificazione BlueXP.

Dimensioni del sistema	CPU	RAM (la memoria di swap deve essere disattivata)	Disco
Molto grande	32 CPU	128 GB DI RAM	1 TiB SSD su /, o. - 100 GiB disponibile su /opt 895 GiB disponibile su /var/lib/docker - 5 GiB su /tmp
Grande	16 CPU	64 GB DI RAM	500 GiB SSD ON /, OR - 100 GiB disponibile su /opt - 395 GiB disponibile su /var/lib/docker - 5 GiB su /tmp
Medio	8 CPU	32 GB DI RAM	200 GiB SSD ON /, OR - 50 GiB disponibile su /opt - 145 GiB disponibile su /var/lib/docker - 5 GiB su /tmp
Piccolo	8 CPU	16 GB DI RAM	100 GiB SSD ON /, OR - 50 GiB disponibile su /opt - 45 GiB disponibile su /var/lib/docker - 5 GiB su /tmp

Tenere presente che esistono limitazioni quando si utilizzano sistemi di dimensioni inferiori. Vedere ["Utilizzando un tipo di istanza più piccolo"](#) per ulteriori informazioni.

- Quando si implementa un'istanza di calcolo nel cloud per l'installazione della classificazione BlueXP, si consiglia di utilizzare un sistema che soddisfi i requisiti di sistema "grandi" indicati in precedenza:
 - **Tipo di istanza AWS EC2:** Si consiglia "m6i.4xlarge". ["Vedere altri tipi di istanze AWS"](#).
 - **Dimensione delle macchine virtuali Azure:** Si consiglia "Standard_D16s_v3". ["Vedere altri tipi di istanze di Azure"](#).
 - **Tipo di macchina GCP:** Si consiglia "n2-standard-16". ["Vedere altri tipi di istanze GCP"](#).
- **UNIX folder permissions:** Sono richieste le seguenti autorizzazioni minime per UNIX:

Cartella	Permessi minimi
/tmp	rwxrwxrwt
/opz	rwxr-xr-x
/var/lib/docker	rwx-----
/usr/lib/systemd/system	rwxr-xr-x

- **Sistema operativo:**

- I seguenti sistemi operativi richiedono l'utilizzo del motore dei container Docker:
 - Red Hat Enterprise Linux versione 7,8 e 7,9
 - CentOS versione 7,8 e 7,9
 - Ubuntu 22,04 (richiede la classificazione BlueXP versione 1,23 o superiore)
- I seguenti sistemi operativi richiedono l'utilizzo del motore del container Podman e richiedono la classificazione BlueXP versione 1,30 o superiore:
 - Red Hat Enterprise Linux versione 8,8, 9,0, 9,1, 9,2 e 9,3

Tenere presente che le seguenti funzioni non sono attualmente supportate quando si utilizzano RHEL 8.x e RHEL 9.x:

- Installazione in un luogo buio
- Scansione distribuita, utilizzando un nodo scanner master e nodi scanner remoti

• **Red Hat Subscription Management:** L'host deve essere registrato con Red Hat Subscription Management. Se non è registrato, il sistema non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione.

• **Software aggiuntivo:** È necessario installare il seguente software sull'host prima di installare la classificazione BlueXP:

- A seconda del sistema operativo in uso, è necessario installare uno dei motori container:
 - Docker Engine versione 19.3.1 o superiore. "[Visualizzare le istruzioni di installazione](#)".

"[Guarda questo video](#)" Per una rapida dimostrazione dell'installazione di Docker su CentOS.

- Podman versione 4 o superiore. Per installare Podman, aggiorna i pacchetti di sistema (`sudo yum update -y`), quindi installare Podman (`sudo yum install netavark -y`).

• Python versione 3,6 o superiore. "[Visualizzare le istruzioni di installazione](#)".

- **Considerazioni NTP:** NetApp consiglia di configurare il sistema di classificazione BlueXP per utilizzare un servizio NTP (Network Time Protocol). L'ora deve essere sincronizzata tra il sistema di classificazione BlueXP e il sistema del connettore BlueXP.
- **Considerazioni su Firewalld:** Se si intende utilizzare `firewalld`, Si consiglia di abilitarla prima di installare la classificazione BlueXP. Eseguire i seguenti comandi per configurare `firewalld` In modo che sia compatibile con la classificazione BlueXP:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

Se si prevede di utilizzare altri host di classificazione BlueXP come nodi scanner, aggiungere queste regole al sistema primario in questo momento:

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

+

Devi riavviare Docker o Podman ogni volta che abiliti o aggiorni il sistema `firewalld` impostazioni.



L'indirizzo IP del sistema host di classificazione BlueXP non può essere modificato dopo l'installazione.

Abilitare l'accesso a Internet in uscita dalla classificazione BlueXP

La classificazione BlueXP richiede l'accesso a Internet in uscita. Se la rete fisica o virtuale utilizza un server proxy per l'accesso a Internet, assicurarsi che l'istanza di classificazione BlueXP disponga dell'accesso a Internet in uscita per contattare i seguenti endpoint.

Endpoint	Scopo
https://api.bluexp.netapp.com	Comunicazione con il servizio BlueXP, che include gli account NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicazione con il sito Web BlueXP per l'autenticazione utente centralizzata.
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Fornisce accesso a immagini software, manifesti, modelli e per inviare registri e metriche.
https://support.compliance.api.bluexp.netapp.com/	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://github.com/docker https://download.docker.com	Fornisce pacchetti prerequisiti per l'installazione di docker.
http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	Fornisce pacchetti prerequisiti per l'installazione di CentOS.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Fornisce pacchetti prerequisiti per l'installazione di Ubuntu.

Verificare che tutte le porte richieste siano attivate

Assicurarsi che tutte le porte richieste siano aperte per la comunicazione tra il connettore, la classificazione BlueXP, Active Directory e le origini dati.

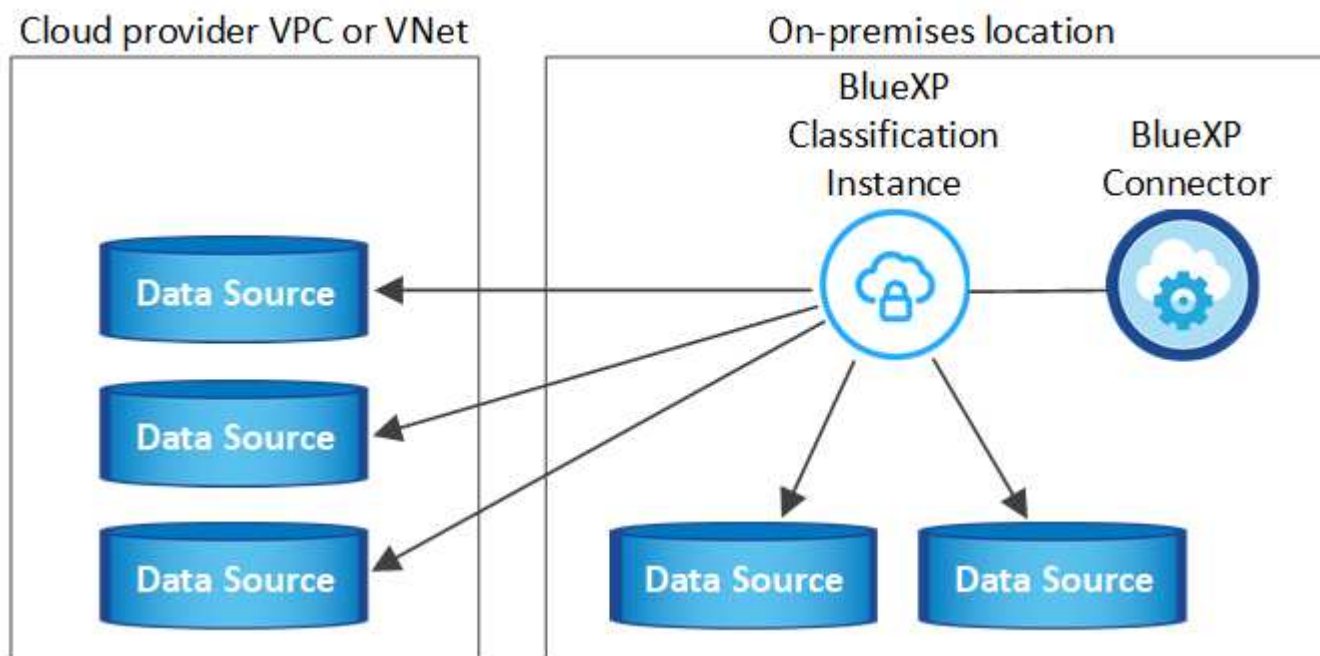
Tipo di connessione	Porte	Descrizione
Connettore <> classificazione BlueXP	8080 (TCP), 443 (TCP) e 80	Il firewall o le regole di routing per il connettore devono consentire il traffico in entrata e in uscita sulla porta 443 da e verso l'istanza di classificazione BlueXP. Assicurarsi che la porta 8080 sia aperta in modo da visualizzare l'avanzamento dell'installazione in BlueXP.
Connettore <> ONTAP cluster (NAS)	443 (TCP)	<p>BlueXP rileva i cluster ONTAP utilizzando HTTPS. Se si utilizzano criteri firewall personalizzati, questi devono soddisfare i seguenti requisiti:</p> <ul style="list-style-type: none"> • L'host del connettore deve consentire l'accesso HTTPS in uscita attraverso la porta 443. Se il connettore si trova nel cloud, tutte le comunicazioni in uscita sono consentite dal firewall predefinito o dalle regole di routing. • Il cluster ONTAP deve consentire l'accesso HTTPS in entrata attraverso la porta 443. Il criterio firewall predefinito "mgmt" consente l'accesso HTTPS in entrata da tutti gli indirizzi IP. Se questo criterio predefinito è stato modificato o se è stato creato un criterio firewall personalizzato, è necessario associare il protocollo HTTPS a tale criterio e abilitare l'accesso dall'host del connettore.
Classificazione BlueXP <> cluster ONTAP	<ul style="list-style-type: none"> • Per NFS - 111 (TCP/UDP) e 2049 (TCP/UDP) • Per CIFS - 139 (TCP/UDP) e 445 (TCP/UDP) 	<p>La classificazione BlueXP richiede una connessione di rete a ogni subnet Cloud Volumes ONTAP o sistema ONTAP on-premise. I firewall o le regole di routing per Cloud Volumes ONTAP devono consentire le connessioni in entrata dall'istanza di classificazione BlueXP.</p> <p>Assicurarsi che queste porte siano aperte per l'istanza di classificazione BlueXP:</p> <ul style="list-style-type: none"> • Per NFS - 111 e 2049 • Per CIFS - 139 e 445 <p>I criteri di esportazione dei volumi NFS devono consentire l'accesso dall'istanza di classificazione BlueXP.</p>

Tipo di connessione	Porte	Descrizione
Classificazione BlueXP <> Active Directory	389 (TCP E UDP), 636 (TCP), 3268 (TCP) E 3269 (TCP)	<p>È necessario che sia già stata configurata una Active Directory per gli utenti della società. Inoltre, la classificazione BlueXP richiede le credenziali di Active Directory per eseguire la scansione dei volumi CIFS.</p> <p>È necessario disporre delle informazioni per Active Directory:</p> <ul style="list-style-type: none"> • DNS Server IP Address (Indirizzo IP server DNS) o Multiple IP Address (indirizzi IP multipli) • Nome utente e password del server • Domain Name (Nome di Active Directory) (Nome di dominio) • Se si utilizza o meno LDAP sicuro (LDAPS) • Porta server LDAP (generalmente 389 per LDAP e 636 per LDAP sicuro)

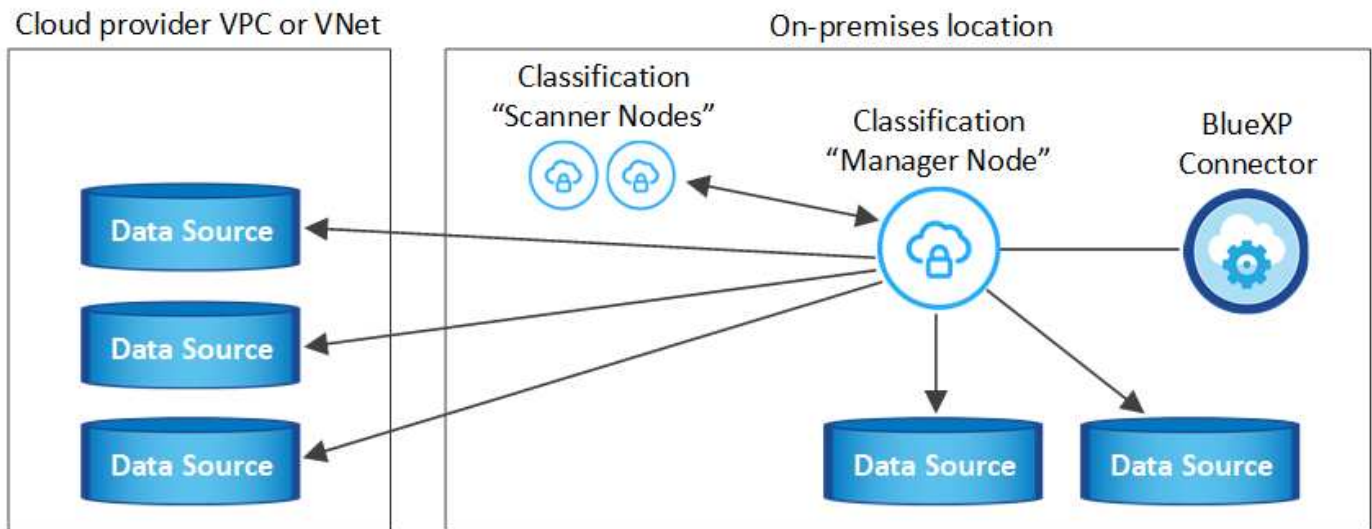
Se si utilizzano più host di classificazione BlueXP per fornire ulteriore potenza di elaborazione per eseguire la scansione delle origini dati, è necessario attivare porte/protocolli aggiuntivi. ["Vedere i requisiti aggiuntivi per le porte"](#).

Installare la classificazione BlueXP sull'host Linux

Per le configurazioni tipiche, il software viene installato su un singolo sistema host. [Consulta questa procedura](#).



Per configurazioni molto grandi in cui si eseguono scansioni di petabyte di dati, è possibile includere più host per fornire ulteriore potenza di elaborazione. [Consulta questa procedura](#).



Vedere [Preparazione del sistema host Linux](#) e [Verifica dei prerequisiti](#) Per l'elenco completo dei requisiti prima di implementare la classificazione BlueXP.

Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.



La classificazione BlueXP non è attualmente in grado di eseguire la scansione dei bucket S3, Azure NetApp Files o FSX per ONTAP quando il software è installato on-premise. In questi casi, è necessario implementare un connettore separato e un'istanza della classificazione BlueXP nel cloud e. ["Passare da un connettore all'altro"](#) per le diverse origini dati.

Installazione a host singolo per configurazioni tipiche

Esaminare i requisiti e seguire questi passaggi quando si installa il software di classificazione BlueXP su un singolo host on-premise.

["Guarda questo video"](#) Per scoprire come installare la classificazione BlueXP.

Tenere presente che tutte le attività di installazione vengono registrate durante l'installazione della classificazione BlueXP. In caso di problemi durante l'installazione, è possibile visualizzare il contenuto del registro di controllo dell'installazione. È scritto a. `/opt/netapp/install_logs/`. ["Per ulteriori informazioni, fare clic qui"](#).

Di cosa hai bisogno

- Verificare che il sistema Linux soddisfi i requisiti [requisiti dell'host](#).
- Verificare che sul sistema siano installati i due pacchetti software prerequisiti (Docker Engine o Podman e Python 3).
- Assicurarsi di disporre dei privilegi di root sul sistema Linux.
- Se si utilizza un proxy per l'accesso a Internet:
 - Sono necessarie le informazioni sul server proxy (indirizzo IP o nome host, porta di connessione, schema di connessione: https o http, nome utente e password).
 - Se il proxy sta eseguendo l'intercettazione TLS, è necessario conoscere il percorso del sistema Linux di classificazione BlueXP in cui sono memorizzati i certificati della CA TLS.
 - Il proxy deve essere non trasparente, al momento non supportiamo proxy trasparenti.

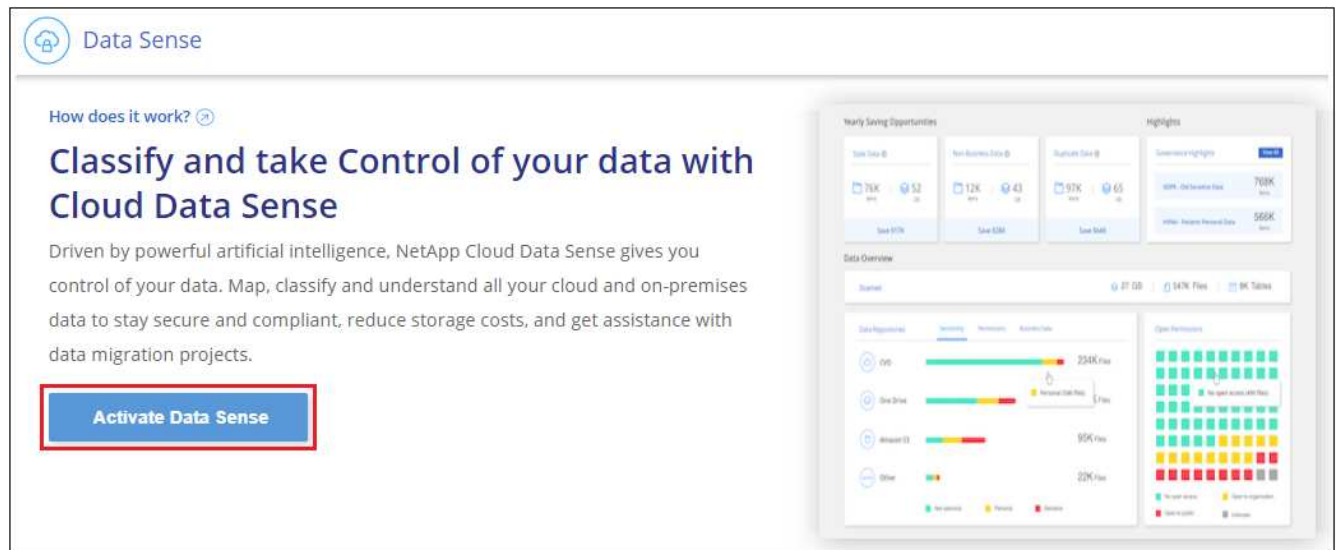
- L'utente deve essere un utente locale. Gli utenti di dominio non sono supportati.
- Verificare che l'ambiente offline soddisfi i requisiti [permessi e connettività](#).

Fasi

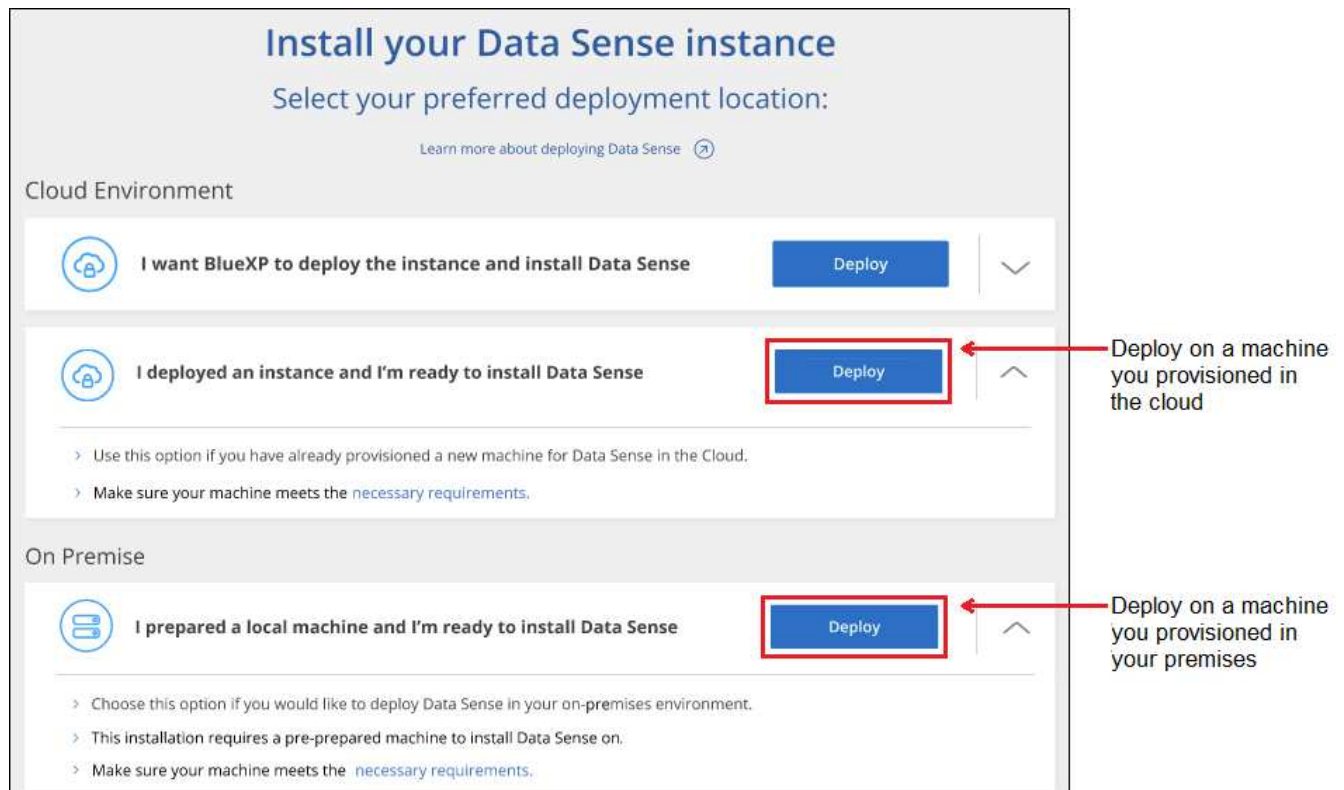
1. Scaricare il software di classificazione BlueXP dal "[Sito di supporto NetApp](#)". Il file da selezionare è **DATASENSE-INSTALLER-<version>.tar.gz**.
2. Copiare il file del programma di installazione sull'host Linux che si desidera utilizzare (utilizzando scp o qualche altro metodo).
3. Decomprimere il file del programma di installazione sul computer host, ad esempio:

```
tar -xzf DATASENSE-INSTALLER-V1.25.0.tar.gz
```

4. In BlueXP, selezionare **Governance > Classification**.
5. Fare clic su **Activate Data Sense** (attiva rilevamento dati).



6. A seconda che si stia installando la classificazione BlueXP su un'istanza preparata nel cloud o su un'istanza preparata in sede, fare clic sul pulsante **Deploy** appropriato per avviare l'installazione della classificazione BlueXP.



- Viene visualizzata la finestra di dialogo *Deploy Data Sense on Premise*. Copiare il comando fornito (ad esempio: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`) e incollarlo in un file di testo per poterlo utilizzare in un secondo momento. Quindi fare clic su **Chiudi** per chiudere la finestra di dialogo.
- Sul computer host, immettere il comando copiato e seguire una serie di prompt oppure fornire il comando completo che include tutti i parametri richiesti come argomenti della riga di comando.

Tenere presente che il programma di installazione esegue una pre-verifica per assicurarsi che i requisiti di sistema e di rete siano stati soddisfatti per una corretta installazione. "[Guarda questo video](#)" comprendere i messaggi di pre-controllo e le implicazioni.

Inserire i parametri come richiesto:	Immettere il comando completo:
<p>a. Incollare il comando copiato dal punto 7: <code>sudo ./install.sh -a <account_id> -c <client_id> -t <user_token></code></p> <p>Se si esegue l'installazione su un'istanza cloud (non on-premise), aggiungere <code>--manual -cloud-install <cloud_provider></code>.</p> <p>b. Immettere l'indirizzo IP o il nome host del computer host di classificazione BlueXP in modo che sia possibile accedervi dal sistema di connettori.</p> <p>c. Inserire l'indirizzo IP o il nome host del computer host BlueXP Connector in modo che sia possibile accedervi dal sistema di classificazione BlueXP.</p> <p>d. Inserire i dettagli del proxy come richiesto. Se il connettore BlueXP utilizza già un proxy, non è necessario inserire nuovamente queste informazioni, poiché la classificazione BlueXP utilizzerà automaticamente il proxy utilizzato dal connettore.</p>	<p>In alternativa, è possibile creare l'intero comando in anticipo, fornendo i parametri host e proxy necessari:</p> <pre>sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --manual-cloud-install <cloud_provider> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy-user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir></pre>

Valori variabili:

- *Account_id* = ID account NetApp
- *Client_id* = ID client del connettore (aggiungere il suffisso "client" all'ID client se non è già presente)
- *User_token* = token di accesso utente JWT
- *Ds_host* = indirizzo IP o nome host del sistema Linux di classificazione BlueXP.
- *Cm_host* = indirizzo IP o nome host del sistema BlueXP Connector.
- *Cloud_provider* = durante l'installazione su un'istanza di cloud, immettere "AWS", "Azure" o "Gcp" a seconda del provider di cloud.
- *Proxy_host* = IP o nome host del server proxy se l'host si trova dietro un server proxy.
- *Porta_proxy* = porta per la connessione al server proxy (impostazione predefinita: 80).
- *Schema_proxy* = Schema di connessione: https o http (http predefinito).
- *Proxy_user* = utente autenticato per la connessione al server proxy, se è richiesta l'autenticazione di base. L'utente deve essere un utente locale - gli utenti di dominio non sono supportati.
- *Proxy_password* = Password per il nome utente specificato.
- *Ca_cert_dir* = percorso del sistema Linux di classificazione BlueXP contenente bundle di certificati CA TLS aggiuntivi. Richiesto solo se il proxy sta eseguendo l'intercettazione TLS.

Risultato

Il programma di installazione della classificazione BlueXP installa i pacchetti, registra l'installazione e installa la classificazione BlueXP. L'installazione può richiedere da 10 a 20 minuti.

Se la connessione tra il computer host e l'istanza del connettore avviene tramite la porta 8080, l'avanzamento dell'installazione viene visualizzato nella scheda classificazione BlueXP in BlueXP.

Cosa c'è di nuovo

Dalla pagina di configurazione è possibile selezionare le origini dati da sottoporre a scansione.

Puoi anche farlo "[Impostare la licenza per la classificazione BlueXP](#)" a questo punto. Non ti verrà addebitato alcun costo fino al termine della prova gratuita di 30 giorni.

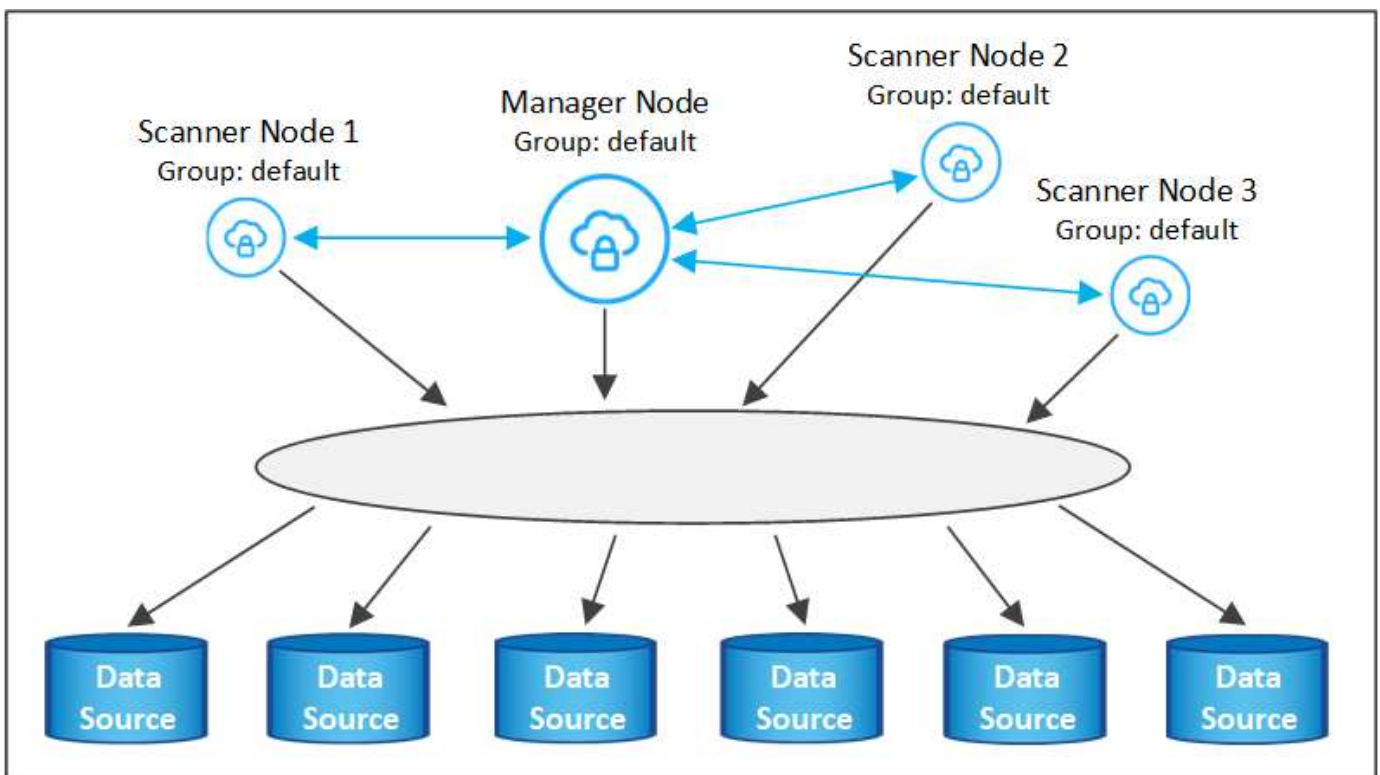
Aggiunta di nodi scanner a un'implementazione esistente

È possibile aggiungere altri nodi dello scanner se si ha bisogno di una maggiore potenza di elaborazione della scansione per eseguire la scansione delle origini dati. È possibile aggiungere i nodi dello scanner subito dopo l'installazione del nodo manager oppure aggiungere un nodo scanner in un secondo momento. Ad esempio, se si comprende che la quantità di dati in una delle origini dati è raddoppiata o triplicata dopo 6 mesi, è possibile aggiungere un nuovo nodo scanner per agevolare la scansione dei dati.

Esistono due modi per aggiungere nodi scanner aggiuntivi:

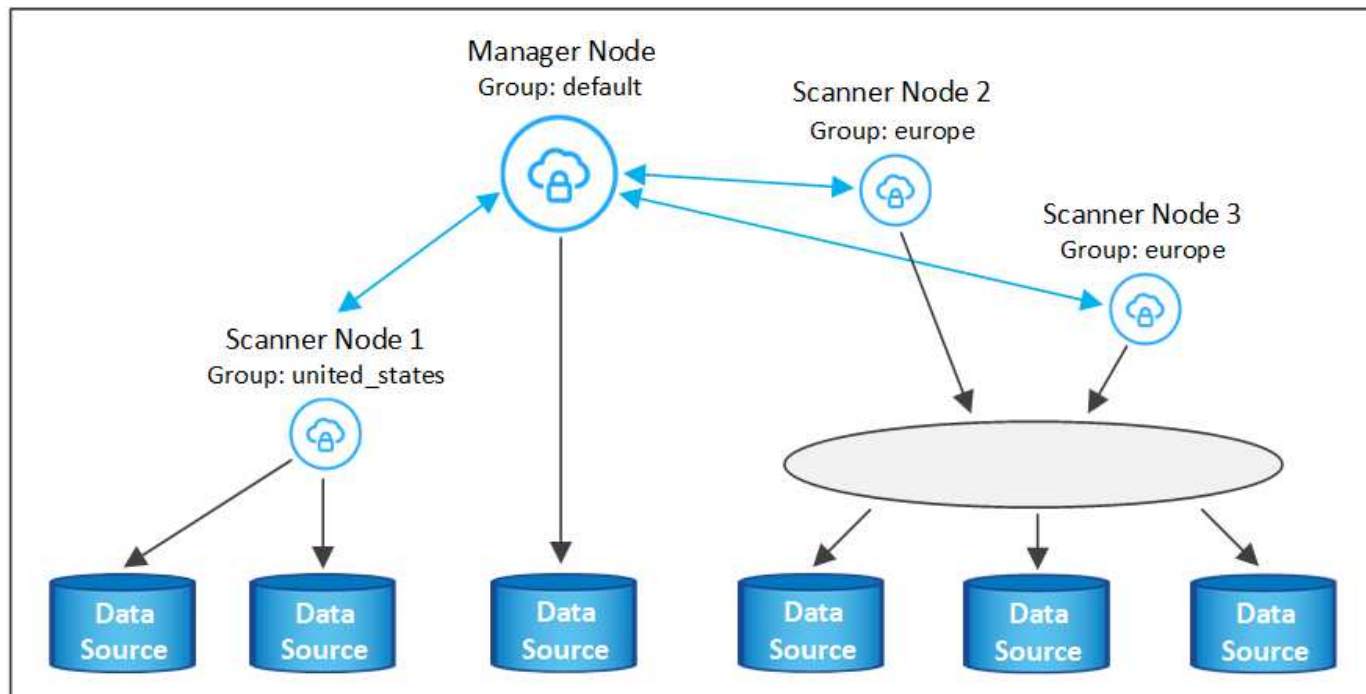
- aggiungere un nodo per facilitare la scansione di tutte le origini dati
- aggiunta di un nodo per agevolare la scansione di una specifica origine dati o di un gruppo specifico di origini dati (in genere in base alla posizione)

Per impostazione predefinita, i nuovi nodi dello scanner aggiunti vengono aggiunti al pool generale di risorse di scansione. Questo è chiamato "gruppo scanner predefinito". Nell'immagine riportata di seguito, sono presenti 1 nodo Manager e 3 nodi scanner nel gruppo "default" che sono tutti dati di scansione da tutte e 6 le origini dati.



Se si desidera eseguire la scansione di determinate origini dati da parte di nodi scanner fisicamente più vicini alle origini dati, è possibile definire un nodo scanner o un gruppo di nodi scanner per eseguire la scansione di una specifica origine dati o di un gruppo di origini dati. Nell'immagine seguente sono presenti 1 nodo Manager e 3 nodi scanner.

- Il nodo Manager si trova nel gruppo "default" e sta eseguendo la scansione di un'origine dati
- Il nodo scanner 1 si trova nel gruppo "united_states" e sta eseguendo la scansione di 2 origini dati
- I nodi scanner 2 e 3 fanno parte del gruppo "europa" e condividono le attività di scansione per 3 origini dati



I gruppi di scanner di classificazione BlueXP possono essere definiti come aree geografiche separate in cui sono memorizzati i dati. È possibile implementare più nodi scanner di classificazione BlueXP in tutto il mondo e scegliere un gruppo di scanner per ciascun nodo. In questo modo, ciascun nodo dello scanner eseguirà la scansione dei dati più vicini. Più vicino è il nodo dello scanner ai dati, meglio è perché riduce il più possibile la latenza di rete durante la scansione dei dati.

È possibile scegliere i gruppi di scanner da aggiungere alla classificazione BlueXP ed è possibile sceglierne i nomi. La classificazione BlueXP non impone l'implementazione in Europa di un nodo mappato a un gruppo di scanner denominato "europa".

Seguire questi passaggi per installare altri nodi scanner di classificazione BlueXP:

1. Preparare i sistemi host Linux che fungeranno da nodi scanner
2. Scarica il software Data Sense su questi sistemi Linux
3. Eseguire un comando sul nodo Manager per identificare i nodi scanner
4. Seguire la procedura per implementare il software sui nodi scanner (e, facoltativamente, definire un "gruppo scanner" per alcuni nodi scanner)
5. Se è stato definito un gruppo di scanner, nel nodo Manager:
 - a. Aprire il file "Working_Environment_to_scanner_group_config.yml" e definire gli ambienti di lavoro che verranno sottoposti a scansione da ciascun gruppo di scanner
 - b. Eseguire il seguente script per registrare queste informazioni di mappatura con tutti i nodi scanner:
`update_we_scanner_group_from_config_file.sh`

Di cosa hai bisogno

- Verificare che tutti i sistemi Linux per i nodi scanner soddisfino il [requisiti dell'host](#).

- Verificare che sui sistemi siano installati i due pacchetti software prerequisiti (Docker Engine o Podman e Python 3).
- Assicurarsi di disporre dei privilegi di root sui sistemi Linux.
- Verificare che l'ambiente soddisfi i requisiti [permessi e connettività](#).
- È necessario disporre degli indirizzi IP degli host del nodo scanner che si stanno aggiungendo.
- È necessario disporre dell'indirizzo IP del sistema host del nodo BlueXP Classification Manager
- È necessario disporre dell'indirizzo IP o del nome host del sistema di connessione, dell'ID account NetApp, dell'ID client del connettore e del token di accesso dell'utente. Se si intende utilizzare gruppi di scanner, è necessario conoscere l'ID dell'ambiente di lavoro per ciascuna origine dati nell'account. Per ottenere queste informazioni, vedere **Prerequisite Steps** di seguito.
- Su tutti gli host devono essere attivati i seguenti protocolli e porte:

Porta	Protocolli	Descrizione
2377	TCP	Comunicazioni per la gestione del cluster
7946	TCP, UDP	Comunicazione tra nodi
4789	UDP	Sovrapporre il traffico di rete
50	ESP	Traffico ESP (Encrypted IPsec Overlay Network)
111	TCP, UDP	Server NFS per la condivisione dei file tra gli host (necessario da ciascun nodo scanner al nodo manager)
2049	TCP, UDP	Server NFS per la condivisione dei file tra gli host (necessario da ciascun nodo scanner al nodo manager)

- Se si utilizza `firewalld` Sulle macchine di classificazione BlueXP, si consiglia di attivarlo prima di installare la classificazione BlueXP. Eseguire i seguenti comandi per configurare `firewalld` In modo che sia compatibile con la classificazione BlueXP:

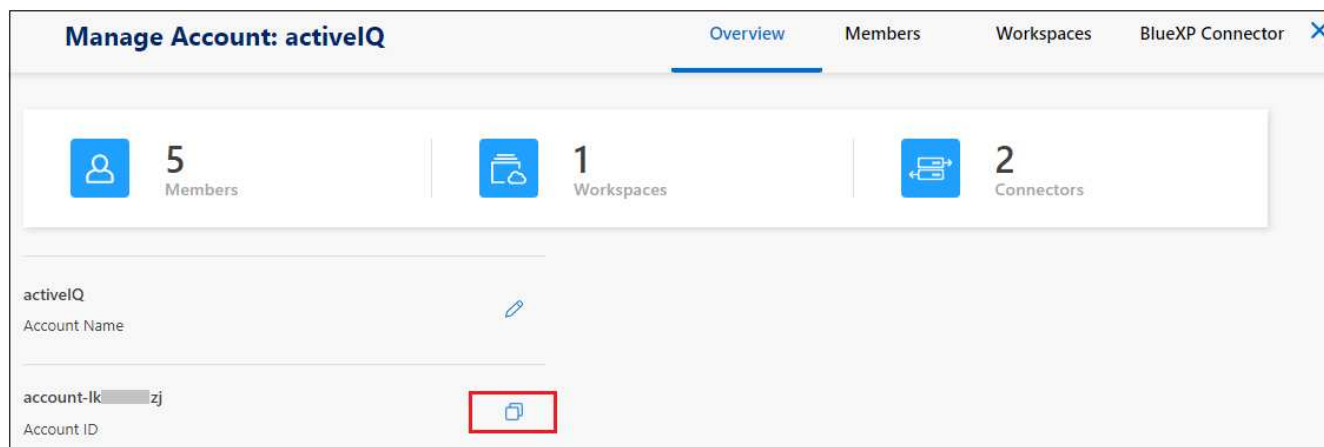
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
firewall-cmd --reload
```

Devi riavviare Docker o Podman ogni volta che abiliti o aggiorni il sistema `firewalld` impostazioni.

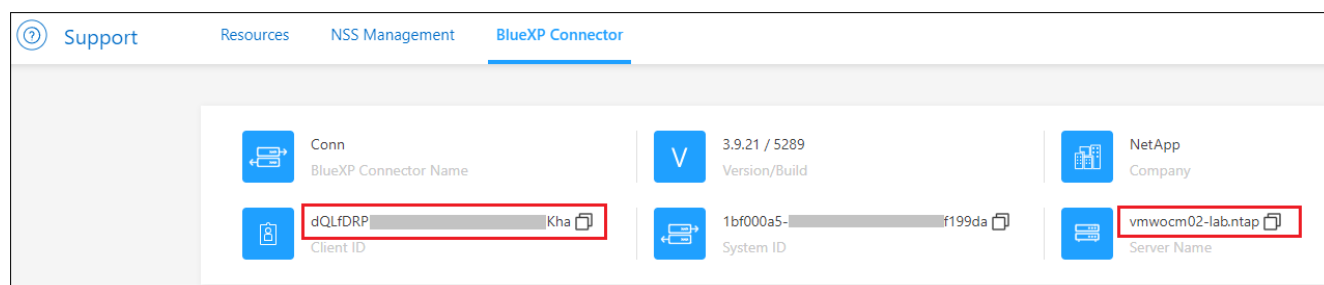
Fasi preliminari

Seguire questa procedura per ottenere l'ID account NetApp, l'ID client del connettore, il nome del server del connettore e il token di accesso dell'utente necessari per aggiungere i nodi dello scanner.

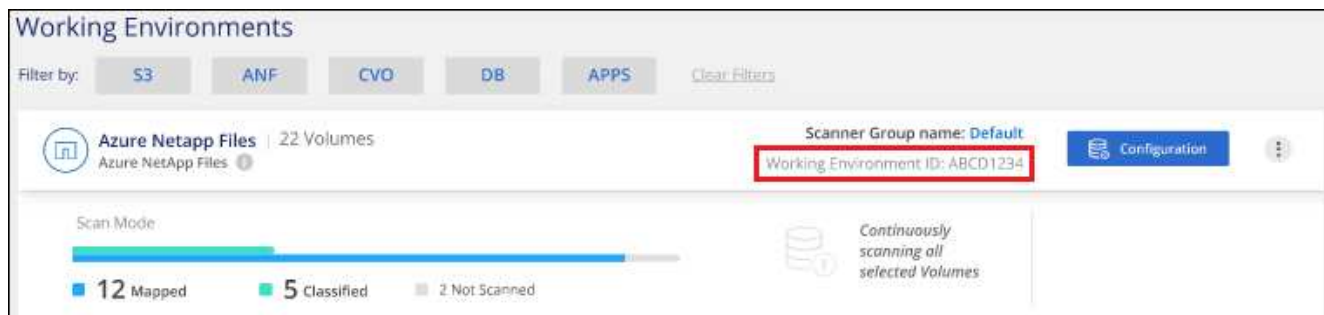
1. Dalla barra dei menu di BlueXP, fare clic su **account > Gestisci account**.



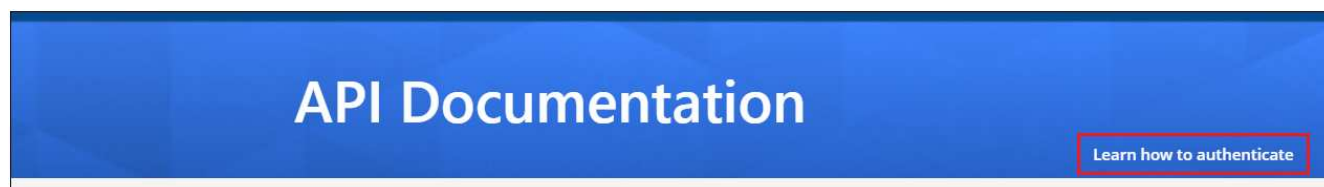
2. Copia l' *ID account*.
3. Dalla barra dei menu di BlueXP, fare clic su **Help > Support > BlueXP Connector**.



4. Copiare il connettore *ID client* e il *Nome server*.
5. Se si intende utilizzare gruppi di scanner, dalla scheda Configurazione classificazione BlueXP, copiare l'ID dell'ambiente di lavoro per ciascun ambiente di lavoro che si desidera aggiungere a un gruppo di scanner.



6. Accedere alla "[API Documentation Developer Hub](#)" E fare clic su **Scopri come autenticare**.



7. Seguire le istruzioni di autenticazione, utilizzando il nome utente e la password dell'account admin nei parametri "Username" (Nome utente) e "password".

8. Quindi, copiare il *token di accesso* dalla risposta.

Fasi

1. Nel nodo di gestione della classificazione BlueXP, eseguire lo script "add_scanner_node.sh". Ad esempio, questo comando aggiunge 2 nodi scanner:

```
sudo ./add_scanner_node.sh -a <account_id> -c <client_id> -m <cm_host> -h  
<ds_manager_ip> -n <node_private_ip_1,node_private_ip_2> -t <user_token>
```

Valori variabili:

- *Account_id* = ID account NetApp
 - *Client_id* = ID client del connettore (aggiungere il suffisso "client" all'ID client copiato nei passaggi del prerequisito)
 - *Cm_host* = indirizzo IP o nome host del sistema di connessione
 - *Ds_manager_ip* = Indirizzo IP privato del sistema di nodi BlueXP Classification Manager
 - *Node_private_ip* = indirizzi IP dei sistemi a nodi scanner di classificazione BlueXP (gli IP di più nodi scanner sono separati da una virgola)
 - *User_token* = token di accesso utente JWT
2. Prima del completamento dello script add_scanner_node, viene visualizzata una finestra di dialogo con il comando di installazione necessario per i nodi dello scanner. Copiare il comando (ad esempio: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j`) e salvarlo in un file di testo.
 3. Su **ciascun** host nodo scanner:
 - a. Copiare il file di installazione di Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) sul computer host (utilizzando `scp` o qualche altro metodo).
 - b. Decomprimere il file di installazione.
 - c. Incollare ed eseguire il comando copiato al punto 2.
 - d. Se si desidera aggiungere un nodo scanner in un "gruppo scanner", aggiungere il parametro **-r <scanner_group_name>** al comando. In caso contrario, il nodo scanner viene aggiunto al gruppo "default".

Quando l'installazione termina su tutti i nodi dello scanner e sono stati Uniti al nodo manager, termina anche lo script "add_scanner_node.sh". L'installazione può richiedere da 10 a 20 minuti.
 4. Se sono stati aggiunti nodi scanner in un gruppo di scanner, tornare al nodo Manager ed eseguire le seguenti 2 operazioni:
 - a. Aprire il file `"/opt/netapp/config/custom_Configuration/working_environment_to_scanner_group_config.yml"` e immettere la mappatura per cui i gruppi di scanner eseguiranno la scansione di specifici ambienti di lavoro. È necessario disporre dell' *ID ambiente di lavoro* per ogni origine dati. Ad esempio, le seguenti voci aggiungono 2 ambienti di lavoro al gruppo scanner "europa" e 2 al gruppo scanner "stati_uniti":

```

scanner_groups:
  europe:
    working_environments:
      - "working_environment_id1"
      - "working_environment_id2"
  united_states:
    working_environments:
      - "working_environment_id3"
      - "working_environment_id4"

```

Tutti gli ambienti di lavoro non aggiunti all'elenco vengono sottoposti a scansione dal gruppo "predefinito". Nel gruppo "predefinito" deve essere presente almeno un nodo del gestore o dello scanner.

- b. Eseguire il seguente script per registrare queste informazioni di mappatura con tutti i nodi scanner:
- ```
/opt/netapp/Datasense/tools/update_we_scanner_group_from_config_file.sh
```

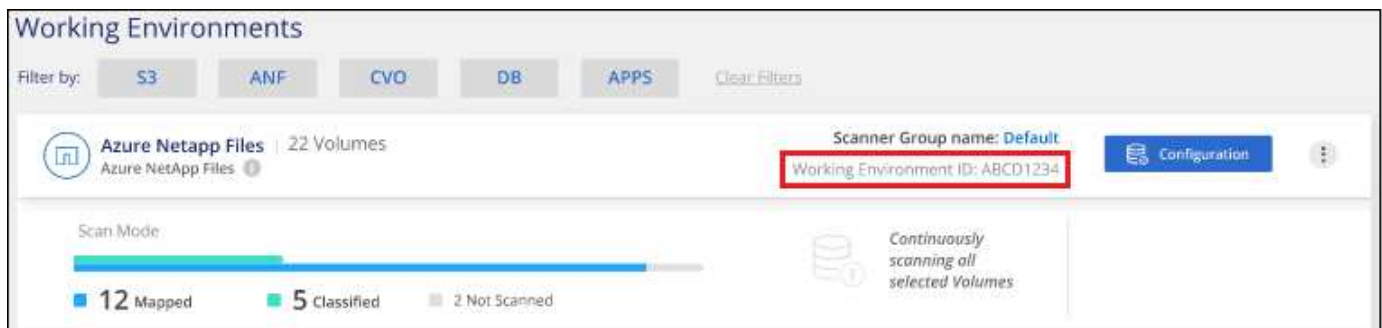
## Risultato

La classificazione BlueXP viene impostata con Manager e scanner Node per eseguire la scansione di tutte le origini dati.

## Cosa c'è di nuovo

Dalla pagina di configurazione è possibile selezionare le origini dati da sottoporre a scansione, se non è già stato fatto. Se sono stati creati gruppi scanner, ogni origine dati viene sottoposta a scansione dai nodi scanner del rispettivo gruppo.

Il nome del gruppo di scanner per ciascun ambiente di lavoro viene visualizzato nella pagina di configurazione.



È inoltre possibile visualizzare l'elenco di tutti i gruppi di scanner, l'indirizzo IP e lo stato di ciascun nodo dello scanner nel gruppo nella parte inferiore della pagina di configurazione.

Scanner Groups

Search

Scanner Group: Default

Scanner nodes

2 Scanner nodes

| Scanner node host name      | IP      | Last active time | Status | Error |
|-----------------------------|---------|------------------|--------|-------|
| ip-172-...us-west-2.compute | 172-... | 23/09/2022 14:32 | Active |       |
| ip-172-...us-west-2.compute | 172-... | 23/09/2022 14:32 | Active |       |

Scanner Group: United\_States

Scanner nodes

2 Scanner nodes

| Scanner node host name      | IP      | Last active time | Status | Error |
|-----------------------------|---------|------------------|--------|-------|
| ip-172-...us-west-2.compute | 172-... | 23/09/2022 14:32 | Active |       |
| ip-172-...us-west-2.compute | 172-... | 23/09/2022 14:32 | Active |       |

Scanner Group: Europe

Scanner nodes

È possibile ["Impostare la licenza per la classificazione BlueXP"](#) a questo punto. Non ti verrà addebitato alcun costo fino al termine della prova gratuita di 30 giorni.

## Installazione multi-host per configurazioni di grandi dimensioni

Per configurazioni molto grandi in cui si eseguono scansioni di petabyte di dati, è possibile includere più host per fornire ulteriore potenza di elaborazione. Quando si utilizzano più sistemi host, il sistema primario è denominato *nodo Manager* e i sistemi aggiuntivi che forniscono potenza di elaborazione aggiuntiva sono denominati *nodi scanner*.

Seguire questi passaggi quando si installa il software di classificazione BlueXP su più host on-premise contemporaneamente. Tenere presente che non è possibile utilizzare "gruppi di scanner" quando si implementano più host in questo modo.

### Di cosa hai bisogno

- Verificare che tutti i sistemi Linux per i nodi Manager e scanner soddisfino il [requisiti dell'host](#).
- Verificare che sui sistemi siano installati i due pacchetti software prerequisiti (Docker o Podman Engine e Python 3).
- Assicurarsi di disporre dei privilegi di root sui sistemi Linux.
- Verificare che l'ambiente soddisfi i requisiti [permessi e connettività](#).
- È necessario disporre degli indirizzi IP degli host dei nodi dello scanner che si intende utilizzare.
- Su tutti gli host devono essere attivati i seguenti protocolli e porte:

| Porta | Protocolli | Descrizione                               |
|-------|------------|-------------------------------------------|
| 2377  | TCP        | Comunicazioni per la gestione del cluster |



| Porta | Protocolli | Descrizione                                                                                               |
|-------|------------|-----------------------------------------------------------------------------------------------------------|
| 7946  | TCP, UDP   | Comunicazione tra nodi                                                                                    |
| 4789  | UDP        | Sovrapporre il traffico di rete                                                                           |
| 50    | ESP        | Traffico ESP (Encrypted IPsec Overlay Network)                                                            |
| 111   | TCP, UDP   | Server NFS per la condivisione dei file tra gli host (necessario da ciascun nodo scanner al nodo manager) |
| 2049  | TCP, UDP   | Server NFS per la condivisione dei file tra gli host (necessario da ciascun nodo scanner al nodo manager) |

## Fasi

1. Seguire i passi da 1 a 7 dal [Installazione su host singolo](#) sul nodo manager.
2. Come illustrato nel passaggio 8, quando richiesto dal programma di installazione, è possibile immettere i valori richiesti in una serie di prompt oppure fornire i parametri richiesti come argomenti della riga di comando al programma di installazione.

Oltre alle variabili disponibili per un'installazione a singolo host, viene utilizzata una nuova opzione **-n <node\_ip>** per specificare gli indirizzi IP dei nodi dello scanner. Gli IP di più nodi dello scanner sono separati da una virgola.

Ad esempio, questo comando aggiunge 3 nodi scanner:

```
sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host
<ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --proxy
-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme>
--proxy-user <proxy_user> --proxy-password <proxy_password>
```

3. Prima del completamento dell'installazione del nodo manager, viene visualizzata una finestra di dialogo con il comando di installazione necessario per i nodi dello scanner. Copiare il comando (ad esempio, `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`) e salvarlo in un file di testo.
4. Su **ciascun** host nodo scanner:
  - a. Copiare il file di installazione di Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) sul computer host (utilizzando `scp` o qualche altro metodo).
  - b. Decomprimere il file di installazione.
  - c. Incollare ed eseguire il comando copiato al punto 3.

Una volta completata l'installazione su tutti i nodi dello scanner e collegati al nodo manager, l'installazione del nodo manager viene completata.

## Risultato

Il programma di installazione della classificazione BlueXP completa l'installazione dei pacchetti e registra l'installazione. L'installazione può richiedere da 10 a 20 minuti.

## Cosa c'è di nuovo

Dalla pagina di configurazione è possibile selezionare le origini dati da sottoporre a scansione.

Puoi anche farlo "[Impostare la licenza per la classificazione BlueXP](#)" a questo punto. Non ti verrà addebitato alcun costo fino al termine della prova gratuita di 30 giorni.



# Installare la classificazione BlueXP su un host Linux senza accesso Internet

Completa alcuni passaggi per installare la classificazione BlueXP su un host Linux in un sito on-premise che non dispone di accesso a Internet, anche noto come *private mode*. Questo tipo di installazione è perfetto per i siti sicuri.

["Scopri le diverse modalità di implementazione per la classificazione BlueXP Connector e BlueXP"](#).

Nota: È anche possibile ["Implementare la classificazione BlueXP in un sito on-premise con accesso a Internet"](#).

Lo script di installazione della classificazione BlueXP inizia verificando se il sistema e l'ambiente soddisfano i prerequisiti richiesti. Se tutti i prerequisiti sono soddisfatti, viene avviata l'installazione. Se si desidera verificare i prerequisiti indipendentemente dall'esecuzione dell'installazione di classificazione BlueXP, è possibile scaricare un pacchetto software separato che esegue solo i prerequisiti. ["Scopri come verificare se il tuo host Linux è pronto per installare la classificazione BlueXP"](#).

## Origini dati supportate

Quando viene installata la modalità privata (talvolta chiamata sito "offline" o "dark"), la classificazione BlueXP può eseguire la scansione dei dati solo da origini dati locali al sito on-premise. Al momento, la classificazione BlueXP è in grado di eseguire la scansione delle seguenti origini dati **locali**:

- Sistemi ONTAP on-premise
- Schemi di database
- Account SharePoint on-premise (SharePoint Server)
- Condivisioni di file NFS o CIFS non NetApp
- Storage a oggetti che utilizza il protocollo S3 (Simple Storage Service)

Attualmente non è disponibile alcun supporto per la scansione di Cloud Volumes ONTAP, Azure NetApp Files, FSX per ONTAP, AWS S3 o Google Drive, OneDrive o SharePoint Online quando la classificazione BlueXP viene implementata in modalità privata.

## Limitazioni

La maggior parte delle funzionalità di classificazione BlueXP funziona quando viene implementato in un sito senza accesso a Internet. Tuttavia, alcune funzioni che richiedono l'accesso a Internet non sono supportate, ad esempio:

- Gestione delle etichette AIP (Microsoft Azure Information Protection)
- Invio di avvisi e-mail agli utenti di BlueXP quando alcuni criteri critici restituiscono risultati
- Impostazione dei ruoli BlueXP per diversi utenti (ad esempio, account Admin o Compliance Viewer)
- Copia e sincronizzazione dei file di origine utilizzando la copia e la sincronizzazione BlueXP
- Ricezione del feedback dell'utente
- Aggiornamenti software automatici da BlueXP

Sia il connettore BlueXP che la classificazione BlueXP richiederanno aggiornamenti manuali periodici per abilitare nuove funzionalità. La versione della classificazione BlueXP è disponibile nella parte inferiore delle

pagine dell'interfaccia utente di classificazione BlueXP. Controllare ["Classificazione BlueXP - Note di rilascio"](#) per vedere le nuove funzionalità di ciascuna release e se si desidera. Quindi, seguire i passaggi da a. ["Aggiornare BlueXP Connector"](#) e [Aggiorna il software di classificazione BlueXP](#).

## Avvio rapido

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

1

### Installare il connettore BlueXP

Se non si dispone già di un connettore installato in modalità privata, ["Implementare il connettore"](#) Su un host Linux.

2

### Esaminare i prerequisiti di classificazione di BlueXP

Assicurarsi che il sistema Linux soddisfi i requisiti [requisiti dell'host](#), che abbia installato tutto il software necessario e che il tuo ambiente offline soddisfi i requisiti [permessi e connettività](#).

3

### Scarica e implementa la classificazione BlueXP

Scaricare il software di classificazione BlueXP dal NetApp Support Site e copiare il file di installazione sull'host Linux che si desidera utilizzare. Quindi, avviare l'installazione guidata e seguire le istruzioni per implementare l'istanza di classificazione BlueXP.

4

### Iscriviti al servizio di classificazione BlueXP

I primi 1 TB di dati che la classificazione BlueXP scansiona in BlueXP sono gratuiti per 30 giorni. Una licenza BYOL di NetApp è necessaria per continuare la scansione dei dati dopo tale data.

## Installare il connettore BlueXP

Se BlueXP Connector non è già installato in modalità privata, ["Implementare il connettore"](#) Su un host Linux nel tuo sito offline.

## Preparare il sistema host Linux

Il software di classificazione BlueXP deve essere eseguito su un host che soddisfi requisiti specifici del sistema operativo, requisiti di RAM, requisiti software e così via.

- La classificazione BlueXP non è supportata su un host condiviso con altre applicazioni: L'host deve essere un host dedicato.
- Quando si costruisce il sistema host in sede, è possibile scegliere tra tre dimensioni del sistema a seconda delle dimensioni del set di dati che si prevede di sottoporre a scansione di classificazione BlueXP.

| Dimensioni del sistema | CPU    | RAM (la memoria di swap deve essere disattivata) | Disco                                                                                                                |
|------------------------|--------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Molto grande</b>    | 32 CPU | 128 GB DI RAM                                    | 1 TiB SSD su /, o.<br>- 100 GiB disponibile su /opt<br>895 GiB disponibile su /var/lib/docker<br>- 5 GiB su /tmp     |
| <b>Grande</b>          | 16 CPU | 64 GB DI RAM                                     | 500 GiB SSD ON /, OR<br>- 100 GiB disponibile su /opt<br>- 395 GiB disponibile su /var/lib/docker<br>- 5 GiB su /tmp |
| <b>Medio</b>           | 8 CPU  | 32 GB DI RAM                                     | 200 GiB SSD ON /, OR<br>- 50 GiB disponibile su /opt<br>- 145 GiB disponibile su /var/lib/docker<br>- 5 GiB su /tmp  |
| <b>Piccolo</b>         | 8 CPU  | 16 GB DI RAM                                     | 100 GiB SSD ON /, OR<br>- 50 GiB disponibile su /opt<br>- 45 GiB disponibile su /var/lib/docker<br>- 5 GiB su /tmp   |

Tenere presente che esistono limitazioni quando si utilizzano sistemi di dimensioni inferiori. Vedere ["Utilizzando un tipo di istanza più piccolo"](#) per ulteriori informazioni.

- Quando si implementa un'istanza di calcolo nel cloud per l'installazione della classificazione BlueXP, si consiglia di utilizzare un sistema che soddisfi i requisiti di sistema "grandi" indicati in precedenza:
  - **Tipo di istanza AWS EC2:** Si consiglia "m6i.4xlarge". ["Vedere altri tipi di istanze AWS"](#).
  - **Dimensione delle macchine virtuali Azure:** Si consiglia "Standard\_D16s\_v3". ["Vedere altri tipi di istanze di Azure"](#).
  - **Tipo di macchina GCP:** Si consiglia "n2-standard-16". ["Vedere altri tipi di istanze GCP"](#).
- **UNIX folder permissions:** Sono richieste le seguenti autorizzazioni minime per UNIX:

| Cartella                | Permessi minimi |
|-------------------------|-----------------|
| /tmp                    | rw-rw-rwt       |
| /opt                    | rw-r-xr-x       |
| /var/lib/docker         | rw- - - - -     |
| /usr/lib/systemd/system | rw-r-xr-x       |

- **Sistema operativo:**
  - I seguenti sistemi operativi richiedono l'utilizzo del motore dei container Docker:
    - Red Hat Enterprise Linux versione 7,8 e 7,9
    - CentOS versione 7,8 e 7,9

- Ubuntu 22,04 (richiede la classificazione BlueXP versione 1,23 o superiore)
- I seguenti sistemi operativi richiedono l'utilizzo del motore del container Podman e richiedono la classificazione BlueXP versione 1,30 o superiore:
  - Red Hat Enterprise Linux versione 8,8, 9,0, 9,1, 9,2 e 9,3

Tenere presente che le seguenti funzioni non sono attualmente supportate quando si utilizzano RHEL 8.x e RHEL 9.x:

- Installazione in un luogo buio
  - Scansione distribuita, utilizzando un nodo scanner master e nodi scanner remoti
  - **Red Hat Subscription Management:** L'host deve essere registrato con Red Hat Subscription Management. Se non è registrato, il sistema non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione.
  - **Software aggiuntivo:** È necessario installare il seguente software sull'host prima di installare la classificazione BlueXP:
    - A seconda del sistema operativo in uso, è necessario installare uno dei motori container:
      - Docker Engine versione 19.3.1 o superiore. "[Visualizzare le istruzioni di installazione](#)".
- ["Guarda questo video"](#) Per una rapida dimostrazione dell'installazione di Docker su CentOS.
- Podman versione 4 o superiore. Per installare Podman, aggiorna i pacchetti di sistema (`sudo yum update -y`), quindi installare Podman (`sudo yum install netavark -y`).
  - Python versione 3,6 o superiore. "[Visualizzare le istruzioni di installazione](#)".
    - **Considerazioni NTP:** NetApp consiglia di configurare il sistema di classificazione BlueXP per utilizzare un servizio NTP (Network Time Protocol). L'ora deve essere sincronizzata tra il sistema di classificazione BlueXP e il sistema del connettore BlueXP.
    - **Considerazioni su Firewalld:** Se si intende utilizzare `firewalld`, Si consiglia di abilitarla prima di installare la classificazione BlueXP. Eseguire i seguenti comandi per configurare `firewalld` in modo che sia compatibile con la classificazione BlueXP:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

Devi riavviare Docker o Podman ogni volta che abiliti o aggiorni il sistema `firewalld` impostazioni.



L'indirizzo IP del sistema host di classificazione BlueXP non può essere modificato dopo l'installazione.

## Verificare i prerequisiti di classificazione di BlueXP e BlueXP

Esaminare i seguenti prerequisiti per assicurarsi di disporre di una configurazione supportata prima di implementare la classificazione BlueXP.

- Assicurarsi che il connettore disponga delle autorizzazioni per distribuire le risorse e creare gruppi di protezione per l'istanza di classificazione BlueXP. Le autorizzazioni BlueXP più recenti sono disponibili in ["Le policy fornite da NetApp"](#).
- Assicurarsi che sia possibile mantenere in esecuzione la classificazione BlueXP. L'istanza di classificazione BlueXP deve rimanere attiva per eseguire una scansione continua dei dati.
- Garantire la connettività del browser Web alla classificazione BlueXP. Una volta attivata la classificazione BlueXP, assicurarsi che gli utenti accedano all'interfaccia BlueXP da un host che dispone di una connessione all'istanza di classificazione BlueXP.

L'istanza di classificazione BlueXP utilizza un indirizzo IP privato per garantire che i dati indicizzati non siano accessibili ad altri. Di conseguenza, il browser Web utilizzato per accedere a BlueXP deve disporre di una connessione a tale indirizzo IP privato. Tale connessione può provenire da un host che si trova all'interno della stessa rete dell'istanza di classificazione BlueXP.

## Verificare che tutte le porte richieste siano attivate

Assicurarsi che tutte le porte richieste siano aperte per la comunicazione tra il connettore, la classificazione BlueXP, Active Directory e le origini dati.

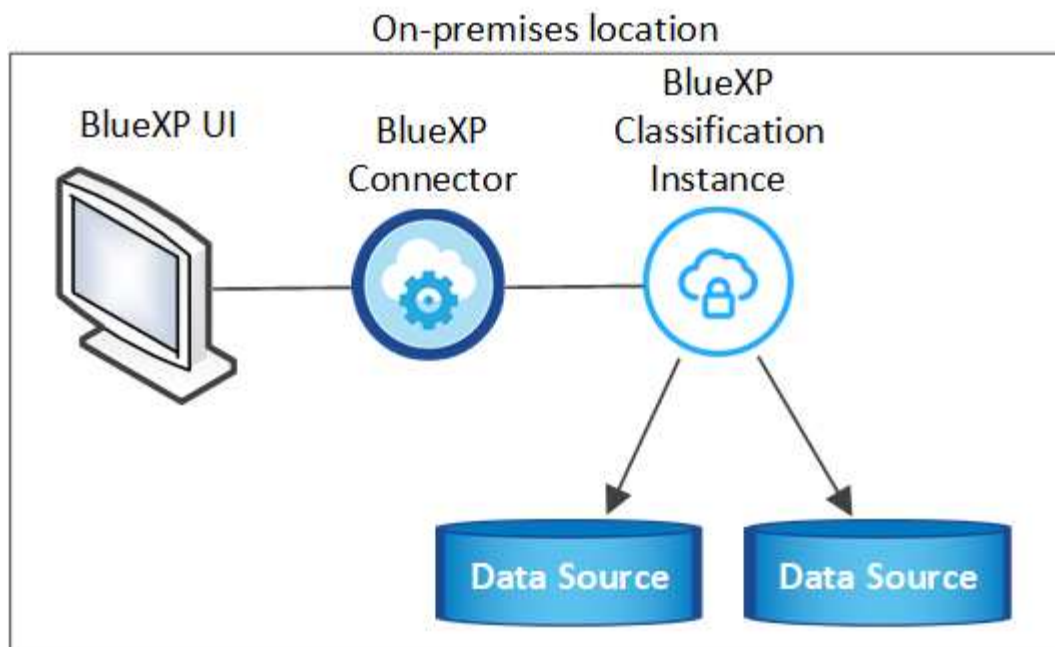
| Tipo di connessione                  | Porte                                  | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connettore <> classificazione BlueXP | 8080 (TCP), 6000 (TCP), 443 (TCP) E 80 | <p>Il gruppo di sicurezza per il connettore deve consentire il traffico in entrata e in uscita sulle porte 6000 e 443 da e verso l'istanza di classificazione BlueXP.</p> <ul style="list-style-type: none"> <li>• È necessaria la porta 6000 per fare in modo che la licenza BYOL di classificazione BlueXP funzioni in un sito oscuro.</li> <li>• La porta 8080 dovrebbe essere aperta in modo da poter vedere l'avanzamento dell'installazione in BlueXP.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                       |
| Connettore <> ONTAP cluster (NAS)    | 443 (TCP)                              | <p>BlueXP rileva i cluster ONTAP utilizzando HTTPS. Se si utilizzano criteri firewall personalizzati, questi devono soddisfare i seguenti requisiti:</p> <ul style="list-style-type: none"> <li>• L'host del connettore deve consentire l'accesso HTTPS in uscita attraverso la porta 443. Se il connettore si trova nel cloud, tutte le comunicazioni in uscita sono consentite dal gruppo di sicurezza predefinito.</li> <li>• Il cluster ONTAP deve consentire l'accesso HTTPS in entrata attraverso la porta 443. Il criterio firewall predefinito "mgmt" consente l'accesso HTTPS in entrata da tutti gli indirizzi IP. Se questo criterio predefinito è stato modificato o se è stato creato un criterio firewall personalizzato, è necessario associare il protocollo HTTPS a tale criterio e abilitare l'accesso dall'host del connettore.</li> </ul> |

| Tipo di connessione                        | Porte                                                                                                                                            | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Classificazione BlueXP <> cluster ONTAP    | <ul style="list-style-type: none"> <li>• Per NFS - 111 (TCP/UDP) e 2049 (TCP/UDP)</li> <li>• Per CIFS - 139 (TCP/UDP) e 445 (TCP/UDP)</li> </ul> | <p>La classificazione BlueXP richiede una connessione di rete a ogni subnet Cloud Volumes ONTAP o sistema ONTAP on-premise. I gruppi di protezione per Cloud Volumes ONTAP devono consentire le connessioni in entrata dall'istanza di classificazione BlueXP.</p> <p>Assicurarsi che queste porte siano aperte per l'istanza di classificazione BlueXP:</p> <ul style="list-style-type: none"> <li>• Per NFS - 111 e 2049</li> <li>• Per CIFS - 139 e 445</li> </ul> <p>I criteri di esportazione dei volumi NFS devono consentire l'accesso dall'istanza di classificazione BlueXP.</p>                                                                                                                   |
| Classificazione BlueXP <> Active Directory | 389 (TCP E UDP), 636 (TCP), 3268 (TCP) E 3269 (TCP)                                                                                              | <p>È necessario che sia già stata configurata una Active Directory per gli utenti della società. Inoltre, la classificazione BlueXP richiede le credenziali di Active Directory per eseguire la scansione dei volumi CIFS.</p> <p>È necessario disporre delle informazioni per Active Directory:</p> <ul style="list-style-type: none"> <li>• DNS Server IP Address (Indirizzo IP server DNS) o Multiple IP Address (indirizzi IP multipli)</li> <li>• Nome utente e password del server</li> <li>• Domain Name (Nome di Active Directory) (Nome di dominio)</li> <li>• Se si utilizza o meno LDAP sicuro (LDAPS)</li> <li>• Porta server LDAP (generalmente 389 per LDAP e 636 per LDAP sicuro)</li> </ul> |

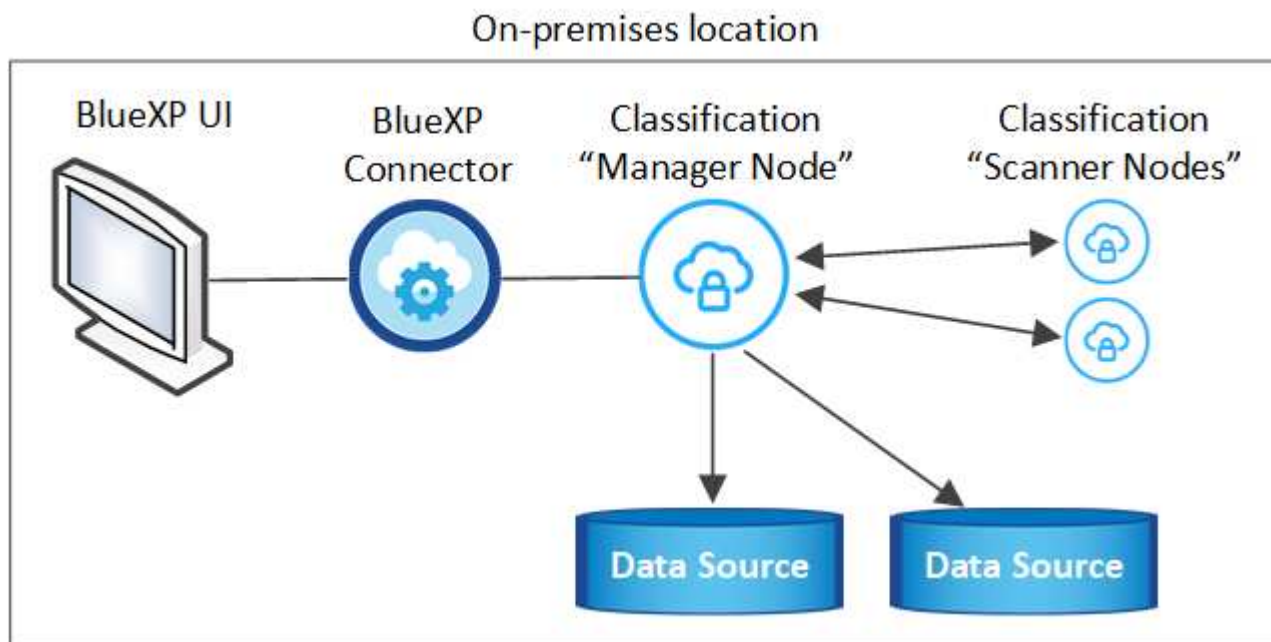
Se si utilizzano più host di classificazione BlueXP per fornire ulteriore potenza di elaborazione per eseguire la scansione delle origini dati, è necessario attivare porte/protocolli aggiuntivi. ["Vedere i requisiti aggiuntivi per le porte"](#).

## Installare la classificazione BlueXP sull'host Linux on-premise

Per le configurazioni tipiche, il software viene installato su un singolo sistema host. ["Consulta questa procedura"](#).



Per configurazioni molto grandi in cui si eseguono scansioni di petabyte di dati, è possibile includere più host per fornire ulteriore potenza di elaborazione. ["Consulta questa procedura"](#).



### Installazione a host singolo per configurazioni tipiche

Seguire questi passaggi quando si installa il software di classificazione BlueXP su un singolo host on-premise in un ambiente offline.

Tenere presente che tutte le attività di installazione vengono registrate durante l'installazione della classificazione BlueXP. In caso di problemi durante l'installazione, è possibile visualizzare il contenuto del registro di controllo dell'installazione. È scritto a `/opt/netapp/install_logs/`. ["Per ulteriori informazioni, fare clic qui"](#).

### Di cosa hai bisogno



- Verificare che il sistema Linux soddisfi i requisiti [requisiti dell'host](#).
- Verificare di aver installato i due pacchetti software prerequisiti (Docker Engine o Podman e Python 3).
- Assicurarsi di disporre dei privilegi di root sul sistema Linux.
- Verificare che l'ambiente offline soddisfi i requisiti [permessi e connettività](#).

## Fasi

1. Su un sistema configurato tramite Internet, scaricare il software di classificazione BlueXP dal "[Sito di supporto NetApp](#)". Il file da selezionare è denominato **DataSense-offline-bundle-<version>.tar.gz**.
2. Copiare il pacchetto di installazione sull'host Linux che si intende utilizzare in modalità privata.
3. Decomprimere il pacchetto di installazione sul computer host, ad esempio:

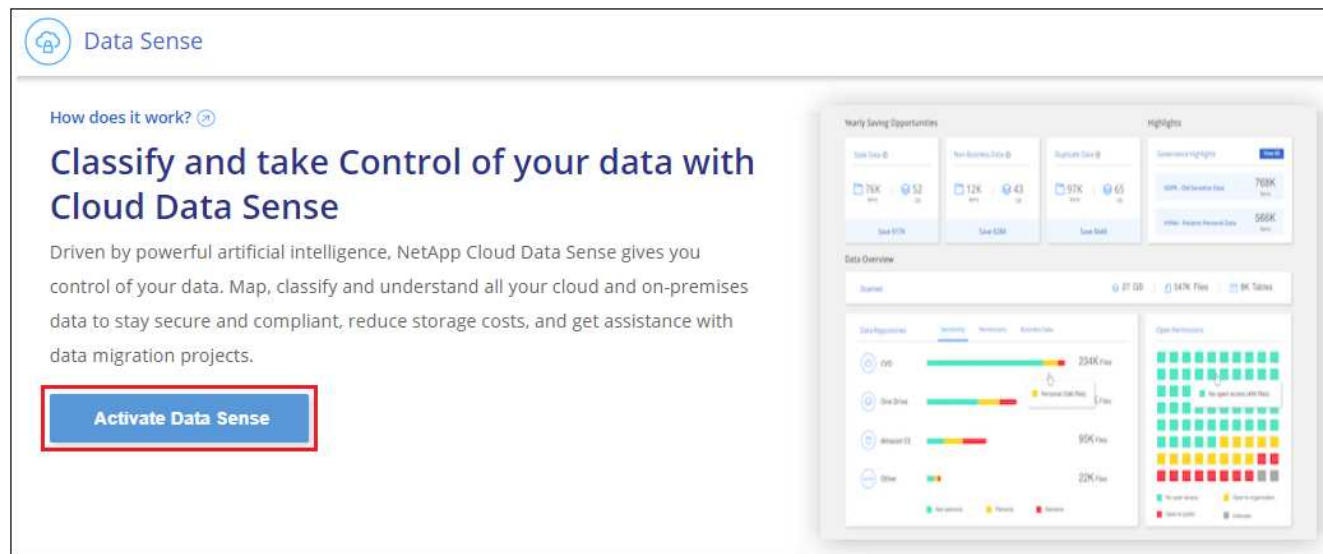
```
tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
```

In questo modo si estraggono il software richiesto e il file di installazione **cc\_onrem\_installer.tar.gz**.

4. Decomprimere il file di installazione sul computer host, ad esempio:

```
tar -xzf cc_onrem_installer.tar.gz
```

5. Avviare BlueXP e selezionare **Governance > Classification**.
6. Fare clic su **Activate Data Sense** (attiva rilevamento dati).



7. Fare clic su **Deploy** per avviare l'installazione on-premise.




## Install your Data Sense instance


Select your preferred deployment location:

[Learn more about deploying Data Sense](#)

### Cloud Environment




I want BlueXP to deploy the instance and install Data Sense
Deploy



I deployed an instance and I'm ready to install Data Sense
Deploy

### On Premise



I prepared a local machine and I'm ready to install Data Sense
Deploy

Choose this option if you would like to deploy Data Sense in your on-premises environment.

This installation requires a pre-prepared machine to install Data Sense on.

Make sure your machine meets the [necessary requirements](#).

8. Viene visualizzata la finestra di dialogo *Deploy Data Sense on Premise*. Copiare il comando fornito (ad esempio: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite`) e incollarlo in un file di testo per poterlo utilizzare in un secondo momento. Quindi fare clic su **Chiudi** per chiudere la finestra di dialogo.
9. Sul computer host, immettere il comando copiato e seguire una serie di prompt oppure fornire il comando completo che include tutti i parametri richiesti come argomenti della riga di comando.

Tenere presente che il programma di installazione esegue una pre-verifica per assicurarsi che i requisiti di sistema e di rete siano stati soddisfatti per una corretta installazione.

| Inserire i parametri come richiesto:                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Immettere il comando completo:                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>a. Incollare le informazioni copiate dal passaggio 8:</p> <pre>sudo ./install.sh -a &lt;account_id&gt; -c &lt;client_id&gt; -t &lt;user_token&gt; --darksite</pre> <p>b. Immettere l'indirizzo IP o il nome host del computer host di classificazione BlueXP in modo che sia possibile accedervi dal sistema di connettori.</p> <p>c. Inserire l'indirizzo IP o il nome host del computer host BlueXP Connector in modo che sia possibile accedervi dal sistema di classificazione BlueXP.</p> | <p>In alternativa, è possibile creare l'intero comando in anticipo, fornendo i parametri host necessari:</p> <pre>sudo ./install.sh -a &lt;account_id&gt; -c &lt;client_id&gt; -t &lt;user_token&gt; --host &lt;ds_host&gt; --manager-host &lt;cm_host&gt; --no-proxy --darksite</pre> |

Valori variabili:

- *Account\_id* = ID account NetApp
- *Client\_id* = ID client del connettore (aggiungere il suffisso "client" all'ID client se non è già presente)
- *User\_token* = token di accesso utente JWT
- *Ds\_host* = indirizzo IP o nome host del sistema di classificazione BlueXP.
- *Cm\_host* = indirizzo IP o nome host del sistema BlueXP Connector.

## Risultato

Il programma di installazione della classificazione BlueXP installa i pacchetti, registra l'installazione e installa la classificazione BlueXP. L'installazione può richiedere da 10 a 20 minuti.

Se la connessione tra il computer host e l'istanza del connettore avviene tramite la porta 8080, l'avanzamento dell'installazione viene visualizzato nella scheda classificazione BlueXP in BlueXP.

## Cosa c'è di nuovo

Dalla pagina di configurazione è possibile selezionare il locale ["Cluster ONTAP on-premise"](#) e ["database"](#) che si desidera acquisire.

Puoi anche farlo ["Impostare la licenza BYOL per la classificazione BlueXP"](#) Dalla pagina del portafoglio digitale BlueXP. Non ti verrà addebitato alcun costo fino al termine della prova gratuita di 30 giorni.

## Installazione multi-host per configurazioni di grandi dimensioni

Per configurazioni molto grandi in cui si eseguono scansioni di petabyte di dati, è possibile includere più host per fornire ulteriore potenza di elaborazione. Quando si utilizzano più sistemi host, il sistema primario è denominato *nodo Manager* e i sistemi aggiuntivi che forniscono potenza di elaborazione aggiuntiva sono denominati *nodi scanner*.

Seguire questi passaggi quando si installa il software di classificazione BlueXP su più host on-premise in un ambiente offline.

## Di cosa hai bisogno

- Verificare che tutti i sistemi Linux per i nodi Manager e scanner soddisfino il [requisiti dell'host](#).
- Verificare di aver installato i due pacchetti software prerequisiti (Docker Engine o Podman e Python 3).
- Assicurarsi di disporre dei privilegi di root sui sistemi Linux.
- Verificare che l'ambiente offline soddisfi i requisiti [permessi e connettività](#).
- È necessario disporre degli indirizzi IP degli host dei nodi dello scanner che si intende utilizzare.
- Su tutti gli host devono essere attivati i seguenti protocolli e porte:

| Porta | Protocolli | Descrizione                                                                                               |
|-------|------------|-----------------------------------------------------------------------------------------------------------|
| 2377  | TCP        | Comunicazioni per la gestione del cluster                                                                 |
| 7946  | TCP, UDP   | Comunicazione tra nodi                                                                                    |
| 4789  | UDP        | Sovrapporre il traffico di rete                                                                           |
| 50    | ESP        | Traffico ESP (Encrypted IPsec Overlay Network)                                                            |
| 111   | TCP, UDP   | Server NFS per la condivisione dei file tra gli host (necessario da ciascun nodo scanner al nodo manager) |

| Porta | Protocolli | Descrizione                                                                                               |
|-------|------------|-----------------------------------------------------------------------------------------------------------|
| 2049  | TCP, UDP   | Server NFS per la condivisione dei file tra gli host (necessario da ciascun nodo scanner al nodo manager) |

## Fasi

1. Seguire i passi da 1 a 8 dal ["Installazione su host singolo"](#) sul nodo manager.
2. Come illustrato al punto 9, quando richiesto dal programma di installazione, è possibile immettere i valori richiesti in una serie di prompt oppure fornire i parametri richiesti come argomenti della riga di comando al programma di installazione.

Oltre alle variabili disponibili per un'installazione a singolo host, viene utilizzata una nuova opzione **-n <node\_ip>** per specificare gli indirizzi IP dei nodi dello scanner. Gli IP di più nodi sono separati da una virgola.

Ad esempio, questo comando aggiunge 3 nodi scanner:

```
sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host
<ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --no
-proxy --darksite
```

3. Prima del completamento dell'installazione del nodo manager, viene visualizzata una finestra di dialogo con il comando di installazione necessario per i nodi dello scanner. Copiare il comando (ad esempio: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`) e salvarlo in un file di testo.
4. Su **ciascun** host nodo scanner:
  - a. Copiare il file del programma di installazione Data Sense (**cc\_onrem\_installer.tar.gz**) sul computer host.
  - b. Decomprimere il file di installazione.
  - c. Incollare ed eseguire il comando copiato al punto 3.

Una volta completata l'installazione su tutti i nodi dello scanner e collegati al nodo manager, l'installazione del nodo manager viene completata.

## Risultato

Il programma di installazione della classificazione BlueXP completa l'installazione dei pacchetti e registra l'installazione. L'installazione può richiedere da 15 a 25 minuti.

## Cosa c'è di nuovo

Dalla pagina di configurazione è possibile selezionare il locale ["Cluster ONTAP on-premise"](#) e locale ["database"](#) che si desidera acquisire.

Puoi anche farlo ["Impostare la licenza BYOL per la classificazione BlueXP"](#) Dalla pagina del portafoglio digitale BlueXP. Non ti verrà addebitato alcun costo fino al termine della prova gratuita di 30 giorni.

## Aggiornare il software di classificazione BlueXP

Poiché il software di classificazione BlueXP viene aggiornato regolarmente con nuove funzionalità, è necessario iniziare una routine per verificare periodicamente la presenza di nuove versioni per assicurarsi di utilizzare il software e le funzionalità più recenti. Sarà necessario aggiornare manualmente il software di classificazione BlueXP perché non è disponibile alcuna connessione a Internet per eseguire l'aggiornamento.

automaticamente.

### Prima di iniziare

- Si consiglia di aggiornare il software BlueXP Connector alla versione più recente disponibile. "[Consultare la procedura di aggiornamento del connettore](#)".
- A partire dalla classificazione BlueXP versione 1.24, è possibile eseguire aggiornamenti a qualsiasi versione futura del software.

Se il software di classificazione BlueXP esegue una versione precedente alla 1.24, è possibile aggiornare solo una versione principale alla volta. Ad esempio, se è installata la versione 1.21.x, è possibile eseguire l'aggiornamento solo alla versione 1.22.x. Se si dispone di alcune versioni principali, sarà necessario aggiornare il software più volte.

### Fasi

1. Su un sistema configurato tramite Internet, scaricare il software di classificazione BlueXP dal "[Sito di supporto NetApp](#)". Il file da selezionare è denominato **DataSense-offline-bundle-<version>.tar.gz**.
2. Copiare il bundle software sull'host Linux in cui è installata la classificazione BlueXP nel sito buio.
3. Decomprimere il bundle software sul computer host, ad esempio:

```
tar -xvf DataSense-offline-bundle-v1.25.0.tar.gz
```

In questo modo si estrae il file di installazione **cc\_onrem\_installer.tar.gz**.

4. Decomprimere il file di installazione sul computer host, ad esempio:

```
tar -xzf cc_onrem_installer.tar.gz
```

In questo modo si estrae lo script di aggiornamento **start\_darksite\_upgrade.sh** e qualsiasi software di terze parti richiesto.

5. Eseguire lo script di aggiornamento sul computer host, ad esempio:

```
start_darksite_upgrade.sh
```

### Risultato

Il software di classificazione BlueXP viene aggiornato sull'host. L'aggiornamento può richiedere da 5 a 10 minuti.

Tenere presente che non è necessario alcun aggiornamento sui nodi dello scanner se è stata implementata la classificazione BlueXP su sistemi host multipli per la scansione di configurazioni molto grandi.

Per verificare che il software sia stato aggiornato, controllare la versione nella parte inferiore delle pagine dell'interfaccia utente di classificazione di BlueXP.

# Verificare che l'host Linux sia pronto per installare la classificazione BlueXP

Prima di installare manualmente la classificazione BlueXP su un host Linux, è possibile eseguire uno script sull'host per verificare che tutti i prerequisiti siano stati implementati per l'installazione della classificazione BlueXP. È possibile eseguire questo script su un host Linux nella rete o su un host Linux nel cloud. L'host può essere connesso a Internet, oppure può risiedere in un sito che non dispone di accesso a Internet (un *sito scuro*).

Esiste anche uno script di test prerequisito che fa parte dello script di installazione della classificazione BlueXP. Lo script qui descritto è stato progettato specificamente per gli utenti che desiderano verificare l'host Linux indipendentemente dall'esecuzione dello script di installazione della classificazione BlueXP.

## Per iniziare

Eseguire le seguenti operazioni.

1. Se necessario, installare un connettore BlueXP, se non ne è già installato uno. È possibile eseguire lo script di test senza aver installato un connettore, ma lo script verifica la connettività tra il connettore e il computer host di classificazione BlueXP, pertanto si consiglia di disporre di un connettore.
2. Preparare il computer host e verificare che soddisfi tutti i requisiti.
3. Abilitare l'accesso a Internet in uscita dal computer host di classificazione BlueXP.
4. Verificare che tutte le porte richieste siano attivate su tutti i sistemi.
5. Scaricare ed eseguire lo script del test dei prerequisiti.

## Creare un connettore

Prima di installare e utilizzare la classificazione BlueXP, è necessario un connettore BlueXP. Tuttavia, è possibile eseguire lo script Prerequisiti senza un connettore.

È possibile ["Installare il connettore on-premise"](#) Su un host Linux nella rete o su un host Linux nel cloud. Alcuni utenti che intendono installare BlueXP classification on-premise possono anche scegliere di installare il connettore on-premise.

Per creare un connettore nel tuo ambiente di cloud provider, consulta ["Creazione di un connettore in AWS"](#), ["Creazione di un connettore in Azure"](#), o ["Creazione di un connettore in GCP"](#).

Quando si esegue lo script Prerequisiti, è necessario l'indirizzo IP o il nome host del sistema di connessione. Queste informazioni saranno disponibili se il connettore è stato installato nella propria sede. Se il connettore è implementato nel cloud, è possibile trovare queste informazioni dalla console BlueXP: Fare clic sull'icona della Guida, selezionare **Support** e fare clic su **BlueXP Connector**.

## Verificare i requisiti dell'host

Il software di classificazione BlueXP deve essere eseguito su un host che soddisfi requisiti specifici del sistema operativo, requisiti di RAM, requisiti software e così via.

- La classificazione BlueXP non è supportata su un host condiviso con altre applicazioni: L'host deve essere un host dedicato.

- Quando si costruisce il sistema host in sede, è possibile scegliere tra tre dimensioni del sistema a seconda delle dimensioni del set di dati che si prevede di sottoporre a scansione di classificazione BlueXP.

| Dimensioni del sistema | CPU    | RAM (la memoria di swap deve essere disattivata) | Disco                                                                                                                |
|------------------------|--------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Molto grande</b>    | 32 CPU | 128 GB DI RAM                                    | 1 TiB SSD su /, o.<br>- 100 GiB disponibile su /opt<br>895 GiB disponibile su /var/lib/docker<br>- 5 GiB su /tmp     |
| <b>Grande</b>          | 16 CPU | 64 GB DI RAM                                     | 500 GiB SSD ON /, OR<br>- 100 GiB disponibile su /opt<br>- 395 GiB disponibile su /var/lib/docker<br>- 5 GiB su /tmp |
| <b>Medio</b>           | 8 CPU  | 32 GB DI RAM                                     | 200 GiB SSD ON /, OR<br>- 50 GiB disponibile su /opt<br>- 145 GiB disponibile su /var/lib/docker<br>- 5 GiB su /tmp  |
| <b>Piccolo</b>         | 8 CPU  | 16 GB DI RAM                                     | 100 GiB SSD ON /, OR<br>- 50 GiB disponibile su /opt<br>- 45 GiB disponibile su /var/lib/docker<br>- 5 GiB su /tmp   |

Tenere presente che esistono limitazioni quando si utilizzano sistemi di dimensioni inferiori. Vedere ["Utilizzando un tipo di istanza più piccolo"](#) per ulteriori informazioni.

- Quando si implementa un'istanza di calcolo nel cloud per l'installazione della classificazione BlueXP, si consiglia di utilizzare un sistema che soddisfi i requisiti di sistema "grandi" indicati in precedenza:
  - **Tipo di istanza AWS EC2:** Si consiglia "m6i.4xlarge". ["Vedere altri tipi di istanze AWS"](#).
  - **Dimensione delle macchine virtuali Azure:** Si consiglia "Standard\_D16s\_v3". ["Vedere altri tipi di istanze di Azure"](#).
  - **Tipo di macchina GCP:** Si consiglia "n2-standard-16". ["Vedere altri tipi di istanze GCP"](#).
- **UNIX folder permissions:** Sono richieste le seguenti autorizzazioni minime per UNIX:

| Cartella                | Permessi minimi |
|-------------------------|-----------------|
| /tmp                    | rwxrwxrwt       |
| /opz                    | rwxr-xr-x       |
| /var/lib/docker         | rwX-----        |
| /usr/lib/systemd/system | rwxr-xr-x       |

- **Sistema operativo:**
  - I seguenti sistemi operativi richiedono l'utilizzo del motore dei container Docker:

- Red Hat Enterprise Linux versione 7,8 e 7,9
- CentOS versione 7,8 e 7,9
- Ubuntu 22,04 (richiede la classificazione BlueXP versione 1,23 o superiore)
- I seguenti sistemi operativi richiedono l'utilizzo del motore del container Podman e richiedono la classificazione BlueXP versione 1,30 o superiore:
  - Red Hat Enterprise Linux versione 8,8, 9,0, 9,1, 9,2 e 9,3

Tenere presente che le seguenti funzioni non sono attualmente supportate quando si utilizzano RHEL 8.x e RHEL 9.x:

- Installazione in un luogo buio
- Scansione distribuita, utilizzando un nodo scanner master e nodi scanner remoti

- **Red Hat Subscription Management:** L'host deve essere registrato con Red Hat Subscription Management. Se non è registrato, il sistema non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione.

- **Software aggiuntivo:** È necessario installare il seguente software sull'host prima di installare la classificazione BlueXP:

- A seconda del sistema operativo in uso, è necessario installare uno dei motori container:
  - Docker Engine versione 19.3.1 o superiore. ["Visualizzare le istruzioni di installazione"](#).

["Guarda questo video"](#) Per una rapida dimostrazione dell'installazione di Docker su CentOS.

- Podman versione 4 o superiore. Per installare Podman, aggiorna i pacchetti di sistema (`sudo yum update -y`), quindi installare Podman (`sudo yum install netavark -y`).

- Python versione 3,6 o superiore. ["Visualizzare le istruzioni di installazione"](#).

- **Considerazioni NTP:** NetApp consiglia di configurare il sistema di classificazione BlueXP per utilizzare un servizio NTP (Network Time Protocol). L'ora deve essere sincronizzata tra il sistema di classificazione BlueXP e il sistema del connettore BlueXP.
- **Considerazioni su FirewallD:** Se si intende utilizzare `firewalld`, Si consiglia di abilitarla prima di installare la classificazione BlueXP. Eseguire i seguenti comandi per configurare `firewalld` In modo che sia compatibile con la classificazione BlueXP:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

Se si prevede di utilizzare altri host di classificazione BlueXP come nodi scanner (in un modello distribuito), aggiungere queste regole al sistema primario in questo momento:

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

+

Devi riavviare Docker o Podman ogni volta che abiliti o aggiorni il sistema `firewalld` impostazioni.

## Abilitare l'accesso a Internet in uscita dalla classificazione BlueXP

La classificazione BlueXP richiede l'accesso a Internet in uscita. Se la rete fisica o virtuale utilizza un server proxy per l'accesso a Internet, assicurarsi che l'istanza di classificazione BlueXP disponga dell'accesso a Internet in uscita per contattare i seguenti endpoint.



Questa sezione non è necessaria per i sistemi host installati in siti senza connettività Internet.

| Endpoint                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Scopo                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Comunicazione con il servizio BlueXP, che include gli account NetApp.                       |
| <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a><br><a href="https://auth0.com">https://auth0.com</a>                                                                                                                                                                                                                                                                                                                                                                                                                                       | Comunicazione con il sito Web BlueXP per l'autenticazione utente centralizzata.             |
| <a href="https://support.compliance.api.bluexp.netapp.com/">https://support.compliance.api.bluexp.netapp.com/</a> <a href="https://hub.docker.com">https://hub.docker.com</a><br><a href="https://auth.docker.io">https://auth.docker.io</a> <a href="https://registry-1.docker.io">https://registry-1.docker.io</a> <a href="https://index.docker.io/">https://index.docker.io/</a><br><a href="https://dseasb33srmrn.cloudfront.net/">https://dseasb33srmrn.cloudfront.net/</a><br><a href="https://production.cloudflare.docker.com/">https://production.cloudflare.docker.com/</a> | Fornisce accesso a immagini software, manifesti, modelli e per inviare registri e metriche. |
| <a href="https://support.compliance.api.bluexp.netapp.com/">https://support.compliance.api.bluexp.netapp.com/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Consente a NetApp di eseguire lo streaming dei dati dai record di audit.                    |
| <a href="https://github.com/docker">https://github.com/docker</a><br><a href="https://download.docker.com">https://download.docker.com</a>                                                                                                                                                                                                                                                                                                                                                                                                                                             | Fornisce pacchetti prerequisiti per l'installazione di docker.                              |
| <a href="http://mirror.centos.org">http://mirror.centos.org</a><br><a href="http://mirrorlist.centos.org">http://mirrorlist.centos.org</a><br><a href="http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm">http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm</a>                                                                                                                                                                                                                        | Fornisce pacchetti prerequisiti per l'installazione di CentOS.                              |
| <a href="http://packages.ubuntu.com/">http://packages.ubuntu.com/</a><br><a href="http://archive.ubuntu.com">http://archive.ubuntu.com</a>                                                                                                                                                                                                                                                                                                                                                                                                                                             | Fornisce pacchetti prerequisiti per l'installazione di Ubuntu.                              |

## Verificare che tutte le porte richieste siano attivate

Assicurarsi che tutte le porte richieste siano aperte per la comunicazione tra il connettore, la classificazione BlueXP, Active Directory e le origini dati.



| Tipo di connessione                  | Porte                      | Descrizione                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connettore <> classificazione BlueXP | 8080 (TCP), 443 (TCP) e 80 | Il firewall o le regole di routing per il connettore devono consentire il traffico in entrata e in uscita sulla porta 443 da e verso l'istanza di classificazione BlueXP. Assicurarsi che la porta 8080 sia aperta in modo da visualizzare l'avanzamento dell'installazione in BlueXP.                                                |
| Connettore <> ONTAP cluster (NAS)    | 443 (TCP)                  | BlueXP rileva i cluster ONTAP utilizzando HTTPS. Se si utilizzano criteri firewall personalizzati, l'host del connettore deve consentire l'accesso HTTPS in uscita attraverso la porta 443. Se il connettore si trova nel cloud, tutte le comunicazioni in uscita sono consentite dal firewall predefinito o dalle regole di routing. |

## Eseguire lo script dei prerequisiti di classificazione BlueXP

Seguire questa procedura per eseguire lo script dei prerequisiti di classificazione BlueXP.

["Guarda questo video"](#) Per vedere come eseguire lo script Prerequisites e interpretare i risultati.

### Di cosa hai bisogno

- Verificare che il sistema Linux soddisfi i requisiti [requisiti dell'host](#).
- Verificare che sul sistema siano installati i due pacchetti software prerequisiti (Docker Engine o Podman e Python 3).
- Assicurarsi di disporre dei privilegi di root sul sistema Linux.

### Fasi

1. Scaricare lo script dei prerequisiti di classificazione BlueXP dal ["Sito di supporto NetApp"](#). Il file da selezionare è denominato **standalone-pre-requisito-tester-<version>**.
2. Copiare il file sull'host Linux che si desidera utilizzare (utilizzando `scp` o qualche altro metodo).
3. Assegnare le autorizzazioni per eseguire lo script.

```
chmod +x standalone-pre-requisite-tester-v1.25.0
```

4. Eseguire lo script utilizzando il seguente comando.

```
./standalone-pre-requisite-tester-v1.25.0 <--darksite>
```

Aggiungere l'opzione `--darksite` solo se si esegue lo script su un host che non dispone di accesso a Internet. Alcuni test dei prerequisiti vengono ignorati quando l'host non è connesso a Internet.

5. Lo script richiede l'indirizzo IP del computer host di classificazione BlueXP.
  - Inserire l'indirizzo IP o il nome host.
6. Lo script chiede se si dispone di un connettore BlueXP installato.

- Immettere **N** se non si dispone di un connettore installato.
  - Inserire **Y** se si dispone di un connettore installato. Quindi, immettere l'indirizzo IP o il nome host del connettore BlueXP in modo che lo script di test possa verificare questa connettività.
7. Lo script esegue una serie di test sul sistema e visualizza i risultati man mano che procede. Al termine, scrive un log della sessione in un file denominato `prerequisites-test-<timestamp>.log` nella directory `/opt/netapp/install_logs`.

## Risultato

Se tutti i test dei prerequisiti sono stati eseguiti correttamente, è possibile installare la classificazione BlueXP sull'host quando si è pronti.

Se sono stati rilevati problemi, questi vengono classificati come "consigliati" o "richiesti" per essere risolti. I problemi consigliati in genere sono elementi che rallenterebbero le attività di classificazione e scansione di BlueXP. Questi elementi non devono essere corretti, ma è possibile che si desideri affrontarli.

In caso di problemi "obbligatori", è necessario risolvere i problemi ed eseguire nuovamente lo script di test Prerequisiti.

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.