



Flussi di lavoro dell'infrastruttura

Astra Automation

NetApp
December 01, 2023

Sommario

- Flussi di lavoro dell'infrastruttura 1
 - Prima di iniziare 1
 - Identità e accesso 1
 - Configurazione LDAP 6
 - Cluster 25
 - Cloud 31
 - Bucket 32
 - Storage 32

Flussi di lavoro dell'infrastruttura

Prima di iniziare

È possibile utilizzare questi flussi di lavoro per creare e gestire l'infrastruttura utilizzata con un'implementazione di Astra Control Center. In molti casi, i flussi di lavoro possono essere utilizzati anche con Astra Control Service.



Questi flussi di lavoro possono essere ampliati e migliorati da NetApp in qualsiasi momento, pertanto è necessario esaminarli periodicamente.

Preparazione generale

Prima di utilizzare uno qualsiasi dei flussi di lavoro Astra, assicurarsi di rivedere ["Preparati a utilizzare i flussi di lavoro"](#).

Categorie di workflow

I flussi di lavoro dell'infrastruttura sono organizzati in diverse categorie per facilitare l'individuazione di quello desiderato.

Categoria	Descrizione
Identità e accesso	Questi flussi di lavoro consentono di gestire l'identità e l'accesso ad Astra. Le risorse includono utenti, credenziali e token.
Configurazione LDAP	È possibile configurare Astra Control Center in modo che utilizzi LDAP per autenticare gli utenti selezionati.
Cluster	È possibile aggiungere cluster Kubernetes gestiti che consentono di proteggere e supportare le applicazioni in essi contenute.
Cloud	Questi flussi di lavoro forniscono l'accesso ai cloud disponibili attraverso l'API REST di Astra Control.
Bucket	È possibile utilizzare questi flussi di lavoro per creare e gestire i bucket S3 utilizzati per memorizzare i backup.
Storage	Questi flussi di lavoro consentono di aggiungere e gestire volumi e backend di storage.

Identità e accesso

Elencare gli utenti

È possibile elencare gli utenti definiti per un account Astra specifico.

1. Elencare gli utenti

Eseguire la seguente chiamata API REST.

Metodo HTTP	Percorso
OTTIENI	/accounts/{account_id}/core/v1/users

Parametri di input aggiuntivi

Oltre ai parametri comuni a tutte le chiamate API REST, negli esempi di curl vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
includi	Query	No	Se si desidera, selezionare i valori che si desidera restituire nella risposta.

Esempio di curl: Restituisce tutti i dati per tutti gli utenti

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/users' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Esempio di curl: Restituisce il nome, il cognome e l'id per tutti gli utenti

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/users?include=first
Name,lastName,id' --header 'Accept: */*' --header 'Authorization: Bearer
<API_TOKEN>'
```

Esempio di output JSON

```
{
  "items": [
    [
      "David",
      "Anderson",
      "844ec6234-11e0-49ea-8434-a992a6270ec1"
    ],
    [
      "Jane",
      "Cohen",
      "2a3e227c-fda7-4145-a86c-ed9aa0183a6c"
    ]
  ],
  "metadata": {}
}
```

Creare un utente

È possibile creare un utente con credenziali specifiche e un ruolo predefinito. È anche possibile limitare l'accesso dell'utente a spazi dei nomi specifici.

1. Selezionare un nome utente

Eseguire il flusso di lavoro ["Elencare gli utenti"](#) e selezionare un nome disponibile non attualmente in uso.

2. Creare l'utente

Eseguire la seguente chiamata API REST per creare un utente. Una volta completata la chiamata, il nuovo utente non sarà ancora utilizzabile.

Metodo HTTP	Percorso
POST	/accounts/{account_id}/core/v1/users

Esempio di input JSON

```
{
  "type" : "application/astra-user",
  "version" : "1.1",
  "firstName" : "John",
  "lastName" : "West",
  "email" : "jwest@example.com"
}
```

Esempio di arricciamento

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/users' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data
@JSONinput
```

Esempio di output JSON

```

{
  "metadata": {
    "creationTimestamp": "2022-11-20T17:23:15Z",
    "modificationTimestamp": "2022-11-20T17:23:15Z",
    "createdBy": "a20e91f3-2c49-443b-b240-615d940ec5f3",
    "labels": []
  },
  "type": "application/astra-user",
  "version": "1.2",
  "id": "d07dac0a-a328-4840-a216-12de16bbd484",
  "authProvider": "local",
  "authID": "jwest@example.com",
  "firstName": "John",
  "lastName": "West",
  "companyName": "",
  "email": "jwest@example.com",
  "postalAddress": {
    "addressCountry": "",
    "addressLocality": "",
    "addressRegion": "",
    "streetAddress1": "",
    "streetAddress2": "",
    "postalCode": ""
  },
  "state": "active",
  "sendWelcomeEmail": "false",
  "isEnabled": "true",
  "isInviteAccepted": "true",
  "enableTimestamp": "2022-11-20T17:23:15Z",
  "lastActTimestamp": ""
}

```

3. Se si desidera, selezionare gli spazi dei nomi consentiti

Eseguire il flusso di lavoro ["Elencare gli spazi dei nomi"](#) e selezionare gli spazi dei nomi a cui si desidera limitare l'accesso.

4. Associare l'utente a un ruolo

Eseguire la seguente chiamata API REST per associare l'utente a un ruolo. Nell'esempio riportato di seguito non sono previste restrizioni per l'accesso allo spazio dei nomi. Vedere ["RBAC migliorato con granularità dello spazio dei nomi"](#) per ulteriori informazioni.

Metodo HTTP	Percorso
POST	/Accounts/{account_id}/core/v1/roleBindings

Esempio di input JSON

```
{
  "type" : "application/astra-roleBinding",
  "version" : "1.1",
  "userID" : "d07dac0a-a328-4840-a216-12de16bbd484",
  "accountID" : "29e1f39f-2bf4-44ba-a191-5b84ef414c95",
  "role" : "viewer",
  "roleConstraints": [ "*" ]
}
```

Esempio di arricciamento

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/roleBindings'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data
@JSONinput
```

5. Creare una credenziale

Eseguire la seguente chiamata API REST per creare una credenziale e associarla all'utente. In questo esempio viene utilizzata una password fornita come valore base64. Il nome La proprietà deve contenere l'ID dell'utente restituito al passaggio precedente. La proprietà di input `change` deve anche essere codificato in base64 e determina se l'utente deve modificare la propria password al primo accesso (`true` oppure `false`).



Questo passaggio è necessario solo con le implementazioni di Astra Control Center che utilizzano l'autenticazione locale. Non è necessario con le implementazioni di Astra Control Center utilizzando LDAP o con le implementazioni di Astra Control Service.

Metodo HTTP	Percorso
POST	/accounts/{account_id}/core/v1/credentials

Esempio di input JSON

```
{
  "type" : "application/astra-credential",
  "version" : "1.1",
  "name" : "d07dac0a-a328-4840-a216-12de16bbd484",
  "keyType" : "passwordHash",
  "keyStore" : {
    "cleartext" : "TmV0QXBwMTIz",
    "change" : "ZmFsc2U="
  },
  "valid" : "true"
}
```

Esempio di arricciamento

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/credentials'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data
@JSONinput
```

Configurazione LDAP

Preparazione per la configurazione LDAP

È possibile integrare Astra Control Center con un server LDAP (Lightweight Directory Access Protocol) per eseguire l'autenticazione per gli utenti Astra selezionati. LDAP è un protocollo standard di settore per l'accesso alle informazioni di directory distribuite e una scelta popolare per l'autenticazione aziendale.

Informazioni correlate

- ["Roadmap delle specifiche tecniche LDAP"](#)
- ["LDAP versione 3"](#)

Panoramica del processo di implementazione

Ad alto livello, è necessario eseguire diversi passaggi per configurare un server LDAP in modo da fornire l'autenticazione agli utenti Astra.



Sebbene i passaggi presentati di seguito siano in sequenza, in alcuni casi è possibile eseguirli in un ordine diverso. Ad esempio, è possibile definire gli utenti e i gruppi Astra prima di configurare il server LDAP.

1. Revisione ["Requisiti e limitazioni"](#) per comprendere le opzioni, i requisiti e le limitazioni.
2. Selezionare un server LDAP e le opzioni di configurazione desiderate (inclusa la protezione).
3. Eseguire il flusso di lavoro ["Configurare Astra per l'utilizzo di un server LDAP"](#) Per integrare Astra con il

server LDAP.

4. Esaminare gli utenti e i gruppi sul server LDAP per assicurarsi che siano definiti correttamente.
5. Eseguire il flusso di lavoro appropriato in ["Aggiungere voci LDAP ad Astra"](#) Identificare gli utenti da autenticare utilizzando LDAP.

Requisiti e limitazioni

Prima di configurare Astra per l'utilizzo di LDAP per l'autenticazione, è necessario esaminare gli elementi essenziali della configurazione di Astra presentati di seguito, incluse le limitazioni e le opzioni di configurazione.

Supportato solo con Astra Control Center

La piattaforma Astra Control offre due modelli di implementazione. L'autenticazione LDAP è supportata solo con le implementazioni di Astra Control Center.

Configurazione mediante API REST o interfaccia utente Web

L'attuale release di Astra Control Center supporta la configurazione dell'autenticazione LDAP utilizzando sia l'API REST di Astra Control che l'interfaccia utente web Astra.

Server LDAP richiesto

Per accettare ed elaborare le richieste di autenticazione Astra, è necessario disporre di un server LDAP. Active Directory di Microsoft è supportata con la release corrente di Astra Control Center.

Connessione sicura al server LDAP

Quando si configura il server LDAP in Astra, è possibile definire una connessione sicura. In questo caso è necessario un certificato per il protocollo LDAPS.

Configurare utenti o gruppi

Selezionare gli utenti da autenticare utilizzando LDAP. È possibile eseguire questa operazione identificando i singoli utenti o un gruppo di utenti. Gli account devono essere definiti sul server LDAP. Inoltre, devono essere identificati in Astra (tipo LDAP), che consente di inoltrare le richieste di autenticazione a LDAP.

Vincolo di ruolo quando si lega un utente o un gruppo

Con l'attuale release di Astra Control Center, l'unico valore supportato per `roleConstraint` è `""`. Questo indica che l'utente non è limitato a un set limitato di spazi dei nomi e può accedere tutti. Vedere ["Aggiungere voci LDAP ad Astra"](#) per ulteriori informazioni.

Credenziali LDAP

Le credenziali utilizzate da LDAP includono il nome utente (indirizzo e-mail) e la password associata.

Indirizzi e-mail univoci

Tutti gli indirizzi e-mail che fungono da nomi utente in un'implementazione di Astra Control Center devono essere univoci. Non è possibile aggiungere un utente LDAP con un indirizzo e-mail già definito in Astra. Se esiste un'email duplicata, devi prima eliminarla da Astra. Vedere ["Rimuovere gli utenti"](#) Per ulteriori informazioni, visitare il sito di documentazione di Astra Control Center.

È possibile definire prima utenti e gruppi LDAP

È possibile aggiungere utenti e gruppi LDAP a Astra Control Center anche se non esistono ancora in LDAP o se il server LDAP non è configurato. Ciò consente di preconfigurare gli utenti e i gruppi prima di configurare il server LDAP.

Un utente definito in più gruppi LDAP

Se un utente LDAP appartiene a più gruppi LDAP e ai gruppi sono stati assegnati ruoli diversi in Astra, il ruolo effettivo dell'utente al momento dell'autenticazione sarà il più privilegiato. Ad esempio, se a un utente è assegnato il `viewer` con il `group1`, ma ha il `member` ruolo nel `group2`, il ruolo dell'utente sarebbe `member`. Si basa sulla gerarchia utilizzata da Astra (dal più alto al più basso):

- Proprietario
- Amministratore
- Membro
- Visualizzatore

Sincronizzazione periodica dell'account

Astra sincronizza gli utenti e i gruppi IT con il server LDAP circa ogni 60 secondi. Quindi, se un utente o un gruppo viene aggiunto o rimosso da LDAP, può essere necessario fino a un minuto prima che sia disponibile in Astra.

Disattivazione e ripristino della configurazione LDAP

Prima di tentare di ripristinare la configurazione LDAP, è necessario disattivare l'autenticazione LDAP. Inoltre, per modificare il server LDAP (`connectionHost`), è necessario eseguire entrambe le operazioni. Vedere ["Disattivare e ripristinare LDAP"](#) per ulteriori informazioni.

Parametri API REST

I flussi di lavoro di configurazione LDAP effettuano chiamate API REST per eseguire le attività specifiche. Ogni chiamata API può includere parametri di input come mostrato negli esempi forniti. Vedere ["Riferimento API online"](#) per informazioni su come individuare la documentazione di riferimento.

Configurare Astra per l'utilizzo di un server LDAP

Selezionare un server LDAP e configurare Astra per utilizzare il server come provider di autenticazione. L'attività di configurazione consiste nei passaggi descritti di seguito. Ogni passaggio include una singola chiamata API REST.

1. Aggiungere un certificato CA

Eeguire la seguente chiamata API REST per aggiungere un certificato CA ad Astra.



Questo passaggio è facoltativo e necessario solo se si desidera che Astra e LDAP comunichino su un canale sicuro utilizzando LDAPS.

Metodo HTTP	Percorso
POST	/accounts/{account_id}/core/v1/certificates

Esempio di input JSON

```
{
  "type": "application/astra-certificate",
  "version": "1.0",
  "certUse": "rootCA",
  "cert": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMyVEN",
  "isSelfSigned": "true"
}
```

Tenere presente quanto segue sui parametri di input:

- `cert` È una stringa JSON contenente un certificato con codifica base64 e formato PKCS-11 (con codifica PEM).
- `isSelfSigned` deve essere impostato su `true` se il certificato è autofirmato. L'impostazione predefinita è `false`.

Esempio di arricciamento

```
curl --location -i --request POST --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/certificates'
--header 'Content-Type: application/astra-certificate+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Esempio di risposta JSON

```

{
  "type": "application/astra-certificate",
  "version": "1.0",
  "id": "a5212e7e-402b-4cff-bba0-63f3c6505199",
  "certUse": "rootCA",
  "cert": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMyVEN",
  "cn": "adldap.example.com",
  "expiryTimestamp": "2023-07-08T20:22:07Z",
  "isSelfSigned": "true",
  "trustState": "trusted",
  "trustStateTransitions": [
    {
      "from": "untrusted",
      "to": [
        "trusted",
        "expired"
      ]
    },
    {
      "from": "trusted",
      "to": [
        "untrusted",
        "expired"
      ]
    },
    {
      "from": "expired",
      "to": [
        "untrusted",
        "trusted"
      ]
    }
  ],
  "trustStateDesired": "trusted",
  "trustStateDetails": [],
  "metadata": {
    "creationTimestamp": "2022-07-21T04:16:06Z",
    "modificationTimestamp": "2022-07-21T04:16:06Z",
    "createdBy": "8a02d2b8-a69d-4064-827f-36851b3e1e6e",
    "modifiedBy": "8a02d2b8-a69d-4064-827f-36851b3e1e6e",
    "labels": []
  }
}

```

2. Aggiungere le credenziali di binding

Eseguire la seguente chiamata API REST per aggiungere le credenziali BIND.

Metodo HTTP	Percorso
POST	/accounts/{account_id}/core/v1/credentials

Esempio di input JSON

```
{
  "name": "ldapBindCredential",
  "type": "application/astra-credential",
  "version": "1.1",
  "keyStore": {
    "bindDn": "dWlkPWFkbWluLG91PXM5c3RlbQ==",
    "password": "cGFzc3dvcmQ="
  }
}
```

Tenere presente quanto segue sui parametri di input:

- `bindDn` e `password` Sono le credenziali bind codificate base64 dell'utente amministratore LDAP in grado di connettersi e cercare nella directory LDAP. `bindDn` È l'indirizzo e-mail dell'utente LDAP.

Esempio di arricciamento

```
curl --location -i --request POST --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/credentials'
--header 'Content-Type: application/astra-credential+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Esempio di risposta JSON

```
{
  "type": "application/astra-credential",
  "version": "1.1",
  "id": "3bd9c8a7-f5a4-4c44-b778-90a85fc7d154",
  "name": "ldapBindCredential",
  "metadata": {
    "creationTimestamp": "2022-07-21T06:53:11Z",
    "modificationTimestamp": "2022-07-21T06:53:11Z",
    "createdBy": "527329f2-662c-41c0-ada9-2f428f14c137"
  }
}
```

Osservare i seguenti parametri di risposta:

- Il `id` della credenziale viene utilizzata nelle fasi successive del flusso di lavoro.

3. Recuperare l'UUID dell'impostazione LDAP

Eseguire la seguente chiamata API REST per recuperare l'UUID di `astra.account.ldap` Impostazione inclusa in Astra Control Center.



Nell'esempio riportato di seguito viene utilizzato un parametro di query per filtrare la raccolta delle impostazioni. È invece possibile rimuovere il filtro per ottenere tutte le impostazioni e quindi cercare `astra.account.ldap`.

Metodo HTTP	Percorso
OTTIENI	<code>/accounts/{account_id}/core/v1/settings</code>

Esempio di arricciamento

```
curl --location -i --request GET
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/settings?filter=name%20eq%20'astra.account.ldap'&include=name,id' --header 'Accept: */*'
--header 'Authorization: Bearer <API_TOKEN>'
```

Esempio di risposta JSON

```
{
  "items": [
    ["astra.account.ldap",
     "12072b56-e939-45ec-974d-2dd83b7815df"]
  ],
  "metadata": {}
}
```

4. Aggiornare l'impostazione LDAP

Eseguire la seguente chiamata API REST per aggiornare l'impostazione LDAP e completare la configurazione. Utilizzare `id` Valore della chiamata API precedente per `<SETTING_ID>` Valore nel percorso URL riportato di seguito.



È possibile inviare una richiesta GET per l'impostazione specifica prima di visualizzare `configSchema`. In questo modo verranno fornite ulteriori informazioni sui campi obbligatori della configurazione.

Metodo HTTP	Percorso
IN PRIMO PIANO	/accounts/{account_id}/core/v1/settings/{setting_id}

Esempio di input JSON

```
{
  "type": "application/astra-setting",
  "version": "1.0",
  "desiredConfig": {
    "connectionHost": "myldap.example.com",
    "credentialId": "3bd9c8a7-f5a4-4c44-b778-90a85fc7d154",
    "groupBaseDN": "OU=groups,OU=astra,DC=example,DC=com",
    "isEnabled": "true",
    "port": 686,
    "secureMode": "LDAPS",
    "userBaseDN": "OU=users,OU=astra,DC=example,dc=com",
    "userSearchFilter": "((objectClass=User))",
    "vendor": "Active Directory"
  }
}
```

Tenere presente quanto segue sui parametri di input:

- `isEnabled` deve essere impostato su `true` oppure si potrebbe verificare un errore.
- `credentialId` è l'id della credenziale bind creata in precedenza.
- `secureMode` deve essere impostato su `LDAP` oppure `LDAPS` in base alla configurazione del passaggio precedente.
- Solo "Active Directory" è supportato come vendor.

Esempio di arricciamento

```
curl --location -i --request PUT --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/settings/<SETTING_ID>' --header 'Content-Type: application/astra-setting+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Se la chiamata ha esito positivo, viene restituita la risposta HTTP 204.

5. Recuperare l'impostazione LDAP

È possibile eseguire la seguente chiamata API REST per recuperare le impostazioni LDAP e confermare l'aggiornamento.

Metodo HTTP	Percorso
OTTIENI	/accounts/{account_id}/core/v1/settings/{setting_id}

Esempio di arricciamento

```
curl --location -i --request GET
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/settings/<SETTING_ID>' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Esempio di risposta JSON

```
{
  "items": [
    {
      "type": "application/astra-setting",
      "version": "1.0",
      "metadata": {
        "creationTimestamp": "2022-06-17T21:16:31Z",
        "modificationTimestamp": "2022-07-21T07:12:20Z",
        "labels": [],
        "createdBy": "system",
        "modifiedBy": "00000000-0000-0000-0000-000000000000"
      },
      "id": "12072b56-e939-45ec-974d-2dd83b7815df",
      "name": "astra.account.ldap",
      "desiredConfig": {
        "connectionHost": "10.193.61.88",
        "credentialId": "3bd9c8a7-f5a4-4c44-b778-90a85fc7d154",
        "groupBaseDN": "ou=groups,ou=astra,dc=example,dc=com",
        "isEnabled": "true",
        "port": 686,
        "secureMode": "LDAPS",
        "userBaseDN": "ou=users,ou=astra,dc=example,dc=com",
        "userSearchFilter": "(objectClass=User)",
        "vendor": "Active Directory"
      },
      "currentConfig": {
        "connectionHost": "10.193.160.209",
        "credentialId": "3bd9c8a7-f5a4-4c44-b778-90a85fc7d154",
        "groupBaseDN": "ou=groups,ou=astra,dc=example,dc=com",
        "isEnabled": "true",
        "port": 686,
        "secureMode": "LDAPS",
        "userBaseDN": "ou=users,ou=astra,dc=example,dc=com",

```



```
"userSearchFilter": "((objectClass=User))",
"vendor": "Active Directory"
},
"configSchema": {
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "astra.account.ldap",
  "type": "object",
  "properties": {
    "connectionHost": {
      "type": "string",
      "description": "The hostname or IP address of your LDAP server."
    },
    "credentialId": {
      "type": "string",
      "description": "The credential ID for LDAP account."
    },
    "groupBaseDN": {
      "type": "string",
      "description": "The base DN of the tree used to start the group
search. The system searches the subtree from the specified location."
    },
    "groupSearchCustomFilter": {
      "type": "string",
      "description": "Type of search that controls the default group
search filter used."
    },
    "isEnabled": {
      "type": "string",
      "description": "This property determines if this setting is
enabled or not."
    },
    "port": {
      "type": "integer",
      "description": "The port on which the LDAP server is running."
    },
    "secureMode": {
      "type": "string",
      "description": "The secure mode LDAPS or LDAP."
    },
    "userBaseDN": {
      "type": "string",
      "description": "The base DN of the tree used to start the user
search. The system searches the subtree from the specified location."
    },
    "userSearchFilter": {
      "type": "string",
```

```

    "description": "The filter used to search for users according a
search criteria."
  },
  "vendor": {
    "type": "string",
    "description": "The LDAP provider you are using.",
    "enum": ["Active Directory"]
  }
},
"additionalProperties": false,
"required": [
  "connectionHost",
  "secureMode",
  "credentialId",
  "userBaseDN",
  "userSearchFilter",
  "groupBaseDN",
  "vendor",
  "isEnabled"
]
},
"state": "valid",
}
],
"metadata": {}
}

```

Individuare il `state` nella risposta che avrà uno dei valori nella tabella seguente.

Stato	Descrizione
in sospeso	Il processo di configurazione è ancora attivo e non ancora completato.
valido	La configurazione è stata completata correttamente e <code>currentConfig</code> nella risposta corrisponde <code>desiredConfig</code> .
errore	Il processo di configurazione LDAP non è riuscito.

Aggiungere voci LDAP ad Astra

Una volta configurato LDAP come provider di autenticazione per Astra Control Center, è possibile selezionare gli utenti LDAP che Astra eseguirà l'autenticazione utilizzando le credenziali LDAP. Ogni utente deve avere un ruolo in Astra prima di poter accedere ad Astra attraverso l'API REST di Astra Control.

Esistono due modi per configurare Astra per assegnare i ruoli. Scegliere quello più adatto al proprio ambiente.

- ["Aggiungere e associare un singolo utente"](#)

- "Aggiungere e associare un gruppo"



Le credenziali LDAP sono sotto forma di nome utente come indirizzo e-mail e password LDAP associata.

Aggiungere e associare un singolo utente

È possibile assegnare un ruolo a ciascun utente Astra utilizzato dopo l'autenticazione LDAP. Ciò è appropriato quando vi è un numero limitato di utenti e ciascuno potrebbe avere caratteristiche amministrative diverse.

1. Aggiungere un utente

Eseguire la seguente chiamata API REST per aggiungere un utente ad Astra e indicare che LDAP è il provider di autenticazione.

Metodo HTTP	Percorso
POST	/accounts/{account_id}/core/v1/users

Esempio di input JSON

```
{
  "type" : "application/astra-user",
  "version" : "1.1",
  "authID" : "cn=JohnDoe,ou=users,ou=astra,dc=example,dc=com",
  "authProvider" : "ldap",
  "firstName" : "John",
  "lastName" : "Doe",
  "email" : "john.doe@example.com"
}
```

Tenere presente quanto segue sui parametri di input:

- Sono necessari i seguenti parametri:
 - authProvider
 - authID
 - email
- authID È il nome distinto (DN) dell'utente in LDAP
- email Deve essere univoco per tutti gli utenti definiti in Astra

Se il email Il valore non è univoco, si verifica un errore e nella risposta viene restituito un codice di stato 409 HTTP.

Esempio di arricchimento

```
curl --location -i --request POST --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/users' --header
'Content-Type: application/astra-user+json' --header 'Accept: */*'
--header 'Authorization: Bearer <API_TOKEN>'
```

Esempio di risposta JSON

```
{
  "metadata": {
    "creationTimestamp": "2022-07-21T17:44:18Z",
    "modificationTimestamp": "2022-07-21T17:44:18Z",
    "createdBy": "8a02d2b8-a69d-4064-827f-36851b3e1e6e",
    "labels": []
  },
  "type": "application/astra-user",
  "version": "1.2",
  "id": "a7b5e674-a1b1-48f6-9729-6a571426d49f",
  "authProvider": "ldap",
  "authID": "cn=JohnDoe,ou=users,ou=astra,dc=example,dc=com",
  "firstName": "John",
  "lastName": "Doe",
  "companyName": "",
  "email": "john.doe@example.com",
  "postalAddress": {
    "addressCountry": "",
    "addressLocality": "",
    "addressRegion": "",
    "streetAddress1": "",
    "streetAddress2": "",
    "postalCode": ""
  },
  "state": "active",
  "sendWelcomeEmail": "false",
  "isEnabled": "true",
  "isInviteAccepted": "true",
  "enableTimestamp": "2022-07-21T17:44:18Z",
  "lastActTimestamp": ""
}
```

2. Aggiungere un'associazione di ruolo per l'utente

Eeguire la seguente chiamata API REST per associare l'utente a un ruolo specifico. È necessario creare l'UUID dell'utente nel passaggio precedente.

Metodo HTTP	Percorso
POST	/Accounts/{account_id}/core/v1/roleBindings

Esempio di input JSON

```
{
  "type": "application/astra-roleBinding",
  "version": "1.1",
  "accountID": "{account_id}",
  "userID": "a7b5e674-a1b1-48f6-9729-6a571426d49f",
  "role": "member",
  "roleConstraints": ["*"]
}
```

Tenere presente quanto segue sui parametri di input:

- Il valore utilizzato in precedenza per `roleConstraint` È l'unica opzione disponibile per la release corrente di Astra. Indica che l'utente non è limitato a un set limitato di spazi dei nomi e può accedervi tutti.

Esempio di arricciamento

```
curl --location -i --request POST --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/roleBindings'
--header 'Content-Type: application/astra-roleBinding+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Esempio di risposta JSON

```

{
  "metadata": {
    "creationTimestamp": "2022-07-21T18:08:24Z",
    "modificationTimestamp": "2022-07-21T18:08:24Z",
    "createdBy": "8a02d2b8-a69d-4064-827f-36851b3e1e6e",
    "labels": []
  },
  "type": "application/astra-roleBinding",
  "principalType": "user",
  "version": "1.1",
  "id": "b02c7e4d-d483-40d1-aaff-e1f900312114",
  "userID": "a7b5e674-a1b1-48f6-9729-6a571426d49f",
  "groupID": "00000000-0000-0000-0000-000000000000",
  "accountID": "d0fdbfa7-be32-4a71-b59d-13d95b42329a",
  "role": "member",
  "roleConstraints": ["*"]
}

```

Tenere presente quanto segue in merito ai parametri di risposta:

- Il valore `user` per `principalType` il campo indica l'aggiunta dell'associazione di ruoli per un utente (non un gruppo).

Aggiungere e associare un gruppo

È possibile assegnare un ruolo a un gruppo Astra che viene utilizzato dopo l'autenticazione LDAP. Ciò è appropriato quando vi è un numero elevato di utenti e ciascuno potrebbe avere caratteristiche amministrative simili.

1. Aggiungere un gruppo

Eseguire la seguente chiamata API REST per aggiungere un gruppo ad Astra e indicare che LDAP è il provider di autenticazione.

Metodo HTTP	Percorso
POST	/accounts/{account_id}/core/v1/groups

Esempio di input JSON

```

{
  "type": "application/astra-group",
  "version": "1.0",
  "name": "Engineering",
  "authProvider": "ldap",
  "authID": "CN=Engineering,OU=groups,OU=astra,DC=example,DC=com"
}

```

Tenere presente quanto segue sui parametri di input:

- Sono necessari i seguenti parametri:
 - authProvider
 - authID

Esempio di arricchimento

```
curl --location -i --request POST --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/groups' --header
'Content-Type: application/astra-group+json' --header 'Accept: */*'
--header 'Authorization: Bearer <API_TOKEN>'
```

Esempio di risposta JSON

```
{
  "type": "application/astra-group",
  "version": "1.0",
  "id": "8b5b54da-ae53-497a-963d-1fc89990525b",
  "name": "Engineering",
  "authProvider": "ldap",
  "authID": "CN=Engineering,OU=groups,OU=astra,DC=example,DC=com",
  "metadata": {
    "creationTimestamp": "2022-07-21T18:42:52Z",
    "modificationTimestamp": "2022-07-21T18:42:52Z",
    "createdBy": "8a02d2b8-a69d-4064-827f-36851b3e1e6e",
    "labels": []
  }
}
```

2. Aggiungere un'associazione di ruolo per il gruppo

Eseguire la seguente chiamata API REST per associare il gruppo a un ruolo specifico. È necessario creare l'UUID del gruppo nel passaggio precedente. Gli utenti che sono membri del gruppo potranno accedere ad Astra dopo che LDAP ha eseguito l'autenticazione.

Metodo HTTP	Percorso
POST	/Accounts/{account_id}/core/v1/roleBindings

Esempio di input JSON

```
{
  "type": "application/astra-roleBinding",
  "version": "1.1",
  "accountID": "{account_id}",
  "groupID": "8b5b54da-ae53-497a-963d-1fc89990525b",
  "role": "viewer",
  "roleConstraints": ["*"]
}
```

Tenere presente quanto segue sui parametri di input:

- Il valore utilizzato in precedenza per `roleConstraint` È l'unica opzione disponibile per la release corrente di Astra. Indica che l'utente non è limitato a determinati spazi dei nomi e può accedervi tutti.

Esempio di arricciamento

```
curl --location -i --request POST --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/roleBindings'
--header 'Content-Type: application/astra-roleBinding+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Esempio di risposta JSON

```
{
  "metadata": {
    "creationTimestamp": "2022-07-21T18:59:43Z",
    "modificationTimestamp": "2022-07-21T18:59:43Z",
    "createdBy": "527329f2-662c-41c0-ada9-2f428f14c137",
    "labels": []
  },
  "type": "application/astra-roleBinding",
  "principalType": "group",
  "version": "1.1",
  "id": "2f91b06d-315e-41d8-ae18-7df7c08fbb77",
  "userID": "00000000-0000-0000-0000-000000000000",
  "groupID": "8b5b54da-ae53-497a-963d-1fc89990525b",
  "accountID": "d0fdbfa7-be32-4a71-b59d-13d95b42329a",
  "role": "viewer",
  "roleConstraints": ["*"]
}
```

Tenere presente quanto segue in merito ai parametri di risposta:

- Il valore `group` per `principalType` il campo indica l'aggiunta dell'associazione di ruoli per un gruppo

(non per un utente).

Disattivare e ripristinare LDAP

Sono disponibili due attività amministrative opzionali, sebbene correlate, che è possibile eseguire in base alle necessità per un'implementazione di Astra Control Center. È possibile disattivare globalmente l'autenticazione LDAP e ripristinare la configurazione LDAP.

Entrambe le attività del flusso di lavoro richiedono l'id per `astra.account.ldap` Impostazione Astra. I dettagli su come recuperare l'id impostazione sono inclusi in **Configurazione del server LDAP**. Vedere ["Recuperare l'UUID dell'impostazione LDAP"](#) per ulteriori informazioni.

- ["Disattiva autenticazione LDAP"](#)
- ["Ripristinare la configurazione di autenticazione LDAP"](#)

Disattiva autenticazione LDAP

È possibile eseguire la seguente chiamata REST API per disattivare globalmente l'autenticazione LDAP per una specifica implementazione Astra. La chiamata aggiorna `astra.account.ldap` e il `isEnabled` il valore è impostato su `false`.

Metodo HTTP	Percorso
IN PRIMO PIANO	<code>/accounts/{account_id}/core/v1/settings/{setting_id}</code>

Esempio di input JSON

```
{
  "type": "application/astra-setting",
  "version": "1.0",
  "desiredConfig": {
    "connectionHost": "myldap.example.com",
    "credentialId": "3bd9c8a7-f5a4-4c44-b778-90a85fc7d154",
    "groupBaseDN": "OU=groups,OU=astra,DC=example,DC=com",
    "isEnabled": "false",
    "port": 686,
    "secureMode": "LDAPS",
    "userBaseDN": "OU=users,OU=astra,DC=example,dc=com",
    "userSearchFilter": "((objectClass=User))",
    "vendor": "Active Directory"
  }
}
```

```
curl --location -i --request PUT --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/settings/<SETTING_ID>' --header 'Content-Type: application/astra-setting+json' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Se la chiamata ha esito positivo, il HTTP 204 la risposta viene restituita. È possibile recuperare di nuovo le impostazioni di configurazione per confermare la modifica.

Ripristinare la configurazione di autenticazione LDAP

È possibile eseguire la seguente chiamata REST API per disconnettere Astra dal server LDAP e reimpostare la configurazione LDAP in Astra. La chiamata aggiorna `astra.account.ldap` e il valore di `connectionHost` è deselezionato.

Il valore di `isEnabled` deve anche essere impostato su `false`. È possibile impostare questo valore prima di effettuare la chiamata di ripristino o come parte della chiamata di ripristino. Nel secondo caso, `connectionHost` devono essere cancellati e `isEnabled` impostare su `false` per la stessa chiamata di ripristino.



Si tratta di un'operazione di interruzione e si consiglia di procedere con cautela. Elimina tutti gli utenti e i gruppi LDAP importati. Inoltre, elimina tutti gli utenti, i gruppi e le associazioni di `roleBinding` Astra (tipo LDAP) creati in Astra Control Center.

Metodo HTTP	Percorso
IN PRIMO PIANO	/accounts/{account_id}/core/v1/settings/{setting_id}

Esempio di input JSON

```
{
  "type": "application/astra-setting",
  "version": "1.0",
  "desiredConfig": {
    "connectionHost": "",
    "credentialId": "3bd9c8a7-f5a4-4c44-b778-90a85fc7d154",
    "groupBaseDN": "OU=groups,OU=astra,DC=example,DC=com",
    "isEnabled": "false",
    "port": 686,
    "secureMode": "LDAPS",
    "userBaseDN": "OU=users,OU=astra,DC=example,dc=com",
    "userSearchFilter": "((objectClass=User))",
    "vendor": "Active Directory"
  }
}
```

Tenere presente quanto segue:

- Per modificare il server LDAP, è necessario disattivare e reimpostare LDAP Changing connectHost su un valore nullo come mostrato nell'esempio precedente.

```
curl --location -i --request PUT --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/settings/<SETTING_ID>' --header 'Content-Type: application/astra-setting+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Se la chiamata ha esito positivo, il HTTP 204 la risposta viene restituita. È possibile recuperare nuovamente la configurazione per confermare la modifica.

Cluster

Elencare i cluster

È possibile elencare i cluster disponibili in un cloud specifico.

1. Selezionare il cloud

Eseguire il flusso di lavoro ["Elencare i cloud"](#) e seleziona il cloud che contiene i cluster.

2. Elencare i cluster

Eseguire la seguente chiamata API REST per elencare i cluster in un cloud specifico.

Metodo HTTP	Percorso
OTTIENI	/accounts/{account_id}/topology/v1/cloud/{cloud_id}/cluster

Esempio di curl: Restituisce tutti i dati per tutti i cluster

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/clouds/<CLOUD_ID>/clusters' --header 'Accept: */*' --header 'Authorization: Bearer
<API_TOKEN>'
```

Esempio di output JSON

```
{
  "items": [
    {
      "type": "application/astra-cluster",
      "version": "1.1",
      "id": "7ce83fba-6aa1-4e0c-a194-26e714f5eb46",
      "name": "openshift-clstr-ol-07",
      "state": "running",
    }
  ]
}
```

```
"stateUnready": [],
"managedState": "managed",
"protectionState": "full",
"protectionStateDetails": [],
"restoreTargetSupported": "true",
"snapshotSupported": "true",
"managedStateUnready": [],
"managedTimestamp": "2022-11-03T15:50:59Z",
"inUse": "true",
"clusterType": "openshift",
"accHost": "true",
"clusterVersion": "1.23",
"clusterVersionString": "v1.23.12+6b34f32",
"namespaces": [
  "default",
  "kube-node-lease",
  "kube-public",
  "kube-system",
  "metallb-system",
  "mysql",
  "mysql-clone1",
  "mysql-clone2",
  "mysql-clone3",
  "mysql-clone4",
  "netapp-acc-operator",
  "netapp-monitoring",
  "openshift",
  "openshift-apiserver",
  "openshift-apiserver-operator",
  "openshift-authentication",
  "openshift-authentication-operator",
  "openshift-cloud-controller-manager",
  "openshift-cloud-controller-manager-operator",
  "openshift-cloud-credential-operator",
  "openshift-cloud-network-config-controller",
  "openshift-cluster-csi-drivers",
  "openshift-cluster-machine-approver",
  "openshift-cluster-node-tuning-operator",
  "openshift-cluster-samples-operator",
  "openshift-cluster-storage-operator",
  "openshift-cluster-version",
  "openshift-config",
  "openshift-config-managed",
  "openshift-config-operator",
  "openshift-console",
  "openshift-console-operator",
```

```
"openshift-console-user-settings",
"openshift-controller-manager",
"openshift-controller-manager-operator",
"openshift-dns",
"openshift-dns-operator",
"openshift-etcd",
"openshift-etcd-operator",
"openshift-host-network",
"openshift-image-registry",
"openshift-infra",
"openshift-ingress",
"openshift-ingress-canary",
"openshift-ingress-operator",
"openshift-insights",
"openshift-kni-infra",
"openshift-kube-apiserver",
"openshift-kube-apiserver-operator",
"openshift-kube-controller-manager",
"openshift-kube-controller-manager-operator",
"openshift-kube-scheduler",
"openshift-kube-scheduler-operator",
"openshift-kube-storage-version-migrator",
"openshift-kube-storage-version-migrator-operator",
"openshift-machine-api",
"openshift-machine-config-operator",
"openshift-marketplace",
"openshift-monitoring",
"openshift-multus",
"openshift-network-diagnostics",
"openshift-network-operator",
"openshift-node",
"openshift-oauth-apiserver",
"openshift-openstack-infra",
"openshift-operator-lifecycle-manager",
"openshift-operators",
"openshift-ovirt-infra",
"openshift-sdn",
"openshift-service-ca",
"openshift-service-ca-operator",
"openshift-user-workload-monitoring",
"openshift-vsphere-infra",
"pcloud",
"postgreql",
"trident"
],
"defaultStorageClass": "4bacbb3c-0727-4f58-b13c-3a2a069baf89",
```

```

    "cloudID": "4f1e1086-f415-4451-a051-c7299cd672ff",
    "credentialID": "7ffd7354-b6c2-4efa-8e7b-cf64d5598463",
    "isMultizonal": "false",
    "tridentManagedStateAllowed": [
      "unmanaged"
    ],
    "tridentVersion": "22.10.0",
    "apiServiceID": "98df44dc-2baf-40d5-8826-e198b1b40909",
    "metadata": {
      "labels": [
        {
          "name": "astra.netapp.io/labels/read-
only/cloudName",
          "value": "private"
        }
      ],
      "creationTimestamp": "2022-11-03T15:50:59Z",
      "modificationTimestamp": "2022-11-04T14:42:32Z",
      "createdBy": "00000000-0000-0000-0000-000000000000"
    }
  }
]
}

```

Aggiungere un cluster utilizzando le credenziali

È possibile aggiungere un cluster in modo che sia disponibile per la gestione da parte di Astra. A partire dalla release Astra 22.11, è possibile aggiungere un cluster con Astra Control Center e Astra Control Service.



L'aggiunta di un cluster non è necessaria quando si utilizza un servizio Kubernetes di uno dei principali provider di cloud (AKS, EKS, GKE).

1. Ottenere il file kubeconfig

È necessario ottenere una copia del file **kubeconfig** dall'amministratore o dal servizio Kubernetes.

Preparare il file kubeconfig

Prima di utilizzare il file **kubeconfig**, eseguire le seguenti operazioni:

Convertire il file dal formato YAML a JSON

Se si riceve il file kubeconfig formattato come YAML, è necessario convertirlo in JSON.

Codificare JSON in base64

È necessario codificare il file JSON in base64.

Esempio

Di seguito viene riportato un esempio di conversione del file kubeconfig da YAML a JSON e di codifica in base64:

```
jq -o=json ~/.kube/config | base64
```

3. Selezionare il cloud

Eseguire il flusso di lavoro ["Elencare i cloud"](#) e selezionare il cloud in cui verrà aggiunto il cluster.



L'unico cloud che puoi selezionare è il cloud **privato**.

4. Creare una credenziale

Eseguire la seguente chiamata API REST per creare una credenziale utilizzando il file kubeconfig.

Metodo HTTP	Percorso
POST	/accounts/{account_id}/core/v1/credentials

Esempio di input JSON

```
{
  "type" : "application/astra-credential",
  "version" : "1.1",
  "name" : "Cloud One",
  "keyType" : "kubeconfig",
  "keyStore" : {
    "base64": encoded_kubeconfig
  },
  "valid" : "true"
}
```

Esempio di arricciamento

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/credentials'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data
@JSONinput
```

5. Aggiungere il cluster

Eseguire la seguente chiamata API REST per aggiungere il cluster al cloud. Il valore di `credentialID` il campo di immissione viene ottenuto dalla chiamata API REST nel passaggio precedente.

Metodo HTTP	Percorso
POST	/accounts/{account_id}/topology/v1/cloud/{cloud_id}/cluster

Esempio di input JSON

```
{
  "type" : "application/astra-cluster",
  "version" : "1.1",
  "credentialID": credential_id
}
```

Esempio di arricciamento

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/clouds/<CLOUD_ID>/clusters' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data @JSONinput
```

Elencare i cluster gestiti

Puoi elencare i cluster Kubernetes attualmente gestiti da Astra.

1. Elencare i cluster gestiti

Eseguire la seguente chiamata API REST.

Metodo HTTP	Percorso
OTTIENI	/Accounts/{account_id}/topology/v1/managedClusters

Esempio di curl: Restituisce tutti i dati per tutti i cluster

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/managedClusters' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Gestire un cluster

È possibile gestire un cluster Kubernetes in modo da poter eseguire la protezione dei dati.

1. Selezionare il cluster da gestire

Eseguire il flusso di lavoro ["Elencare i cluster"](#) e selezionare il cluster desiderato. La proprietà `managedState` del cluster deve essere `unmanaged`.

2. Se si desidera, selezionare la classe di storage

Eseguire il flusso di lavoro come opzione ["Elencare le classi di storage"](#) e selezionare la classe di storage

desiderata.



Se non si fornisce una classe di storage durante la chiamata per gestire il cluster, viene utilizzata la classe di storage predefinita.

3. Gestire il cluster

Eeguire la seguente chiamata API REST per gestire il cluster.

Metodo HTTP	Percorso
POST	/Accounts/{account_id}/topology/v1/managedClusters

Esempio di input JSON

```
{
  "type": "application/astra-managedCluster",
  "version": "1.0",
  "id": "d0fdf455-4330-476d-bb5d-4d109714e07d"
}
```

Esempio di arricciamento

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/managedClusters
' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
--data @JSONinput
```

Cloud

Elencare i cloud

Puoi elencare i cloud definiti e disponibili per un account Astra specifico.

1. Elencare i cloud

Eeguire la seguente chiamata API REST per elencare i cloud.

Metodo HTTP	Percorso
OTTIENI	/accounts/{account_id}/topology/v1/cloud

Esempio di curl: Restituisce tutti i dati per tutti i cloud

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/clouds'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Bucket

Elencare i bucket

È possibile elencare i bucket S3 definiti per un account Astra specifico.

1. Elencare i bucket

Eseguire la seguente chiamata API REST per elencare i bucket.

Metodo HTTP	Percorso
OTTIENI	/accounts/{account_id}/topology/v1/bucket

Esempio di curl: Restituisce tutti i dati per tutti i bucket

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/buckets'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Storage

Elencare le classi di storage

È possibile elencare le classi di storage disponibili.

1. Selezionare il cloud

Eseguire il flusso di lavoro "[Elencare i cloud](#)" e seleziona il cloud in cui lavorerai.

2. Selezionare il cluster

Eseguire il flusso di lavoro "[Elencare i cluster](#)" e selezionare il cluster.

3. Elencare le classi di storage per un cluster specifico

Eseguire la seguente chiamata API REST per elencare le classi di storage per un cluster e un cloud specifici.

Metodo HTTP	Percorso
OTTIENI	/Accounts/{account_id}/topology/v1/cloud/<CLOUD_ID>/Clusters/<CLUSTER_ID>/storageClasses

Esempio di curl: Restituisce tutti i dati per tutte le classi di storage

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/clouds/<CLOUD_ID>/clusters/<CLUSTER_ID>/storageClasses' --header 'Accept: */*' --header
'Authorization: Bearer <API_TOKEN>'
```

Esempio di output JSON

```
{
  "items": [
    {
      "type": "application/astra-storageClass",
      "version": "1.1",
      "id": "4bacbb3c-0727-4f58-b13c-3a2a069baf89",
      "name": "ontap-basic",
      "provisioner": "csi.trident.netapp.io",
      "available": "eligible",
      "allowVolumeExpansion": "true",
      "reclaimPolicy": "Delete",
      "volumeBindingMode": "Immediate",
      "isDefault": "true",
      "metadata": {
        "createdBy": "system",
        "creationTimestamp": "2022-10-26T05:16:19Z",
        "modificationTimestamp": "2022-10-26T05:16:19Z",
        "labels": []
      }
    },
    {
      "type": "application/astra-storageClass",
      "version": "1.1",
      "id": "150fe657-4a42-47a3-abc6-5dafba3de8bf",
      "name": "thin",
      "provisioner": "kubernetes.io/vsphere-volume",
      "available": "ineligible",
      "reclaimPolicy": "Delete",
      "volumeBindingMode": "Immediate",
      "metadata": {
        "createdBy": "system",
        "creationTimestamp": "2022-10-26T04:46:08Z",
        "modificationTimestamp": "2022-11-04T14:58:19Z",
        "labels": []
      }
    }
  ],
}
```

```

{
  "type": "application/astra-storageClass",
  "version": "1.1",
  "id": "7c6a5c58-6a0d-4cb6-98a0-8202ad2de74a",
  "name": "thin-csi",
  "provisioner": "csi.vsphere.vmware.com",
  "available": "ineligible",
  "allowVolumeExpansion": "true",
  "reclaimPolicy": "Delete",
  "volumeBindingMode": "WaitForFirstConsumer",
  "metadata": {
    "createdBy": "system",
    "creationTimestamp": "2022-10-26T04:46:17Z",
    "modificationTimestamp": "2022-10-26T04:46:17Z",
    "labels": []
  }
},
{
  "type": "application/astra-storageClass",
  "version": "1.1",
  "id": "7010ef09-92a5-4c90-a5e5-3118e02dc9a7",
  "name": "vsim-san",
  "provisioner": "csi.trident.netapp.io",
  "available": "eligible",
  "allowVolumeExpansion": "true",
  "reclaimPolicy": "Delete",
  "volumeBindingMode": "Immediate",
  "metadata": {
    "createdBy": "system",
    "creationTimestamp": "2022-11-03T18:40:03Z",
    "modificationTimestamp": "2022-11-03T18:40:03Z",
    "labels": []
  }
}
]
}

```

Elenca i backend di storage

È possibile elencare i backend di storage disponibili.

1. Elencare i backend

Eseguire la seguente chiamata API REST.

Metodo HTTP	Percorso
OTTIENI	/Accounts/{account_id}/topology/v1/storageBackends

Esempio di curl: Restituisce tutti i dati per tutti i backend di storage

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/storageBackends
' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Esempio di output JSON

```

{
  "items": [
    {
      "backendCredentialsName": "10.191.77.177",
      "backendName": "myinchunhcluster-1",
      "backendType": "ONTAP",
      "backendVersion": "9.8.0",
      "configVersion": "Not applicable",
      "health": "Not applicable",
      "id": "46467c16-1585-4b71-8e7f-f0bc5ff9da15",
      "location": "nalab2",
      "metadata": {
        "createdBy": "4c483a7e-207b-4f9a-87b7-799a4629d7c8",
        "creationTimestamp": "2021-07-30T14:26:19Z",
        "modificationTimestamp": "2021-07-30T14:26:19Z"
      },
      "ontap": {
        "backendManagementIP": "10.191.77.177",
        "managementIPs": [
          "10.191.77.177",
          "10.191.77.179"
        ]
      },
      "protectionPolicy": "Not applicable",
      "region": "Not applicable",
      "state": "Running",
      "stateUnready": [],
      "type": "application/astra-storageBackend",
      "version": "1.0",
      "zone": "Not applicable"
    }
  ]
}

```

Abilitare i pool ANF dinamici per i cluster autogestiti

Quando si esegue il backup di un'applicazione gestita in un cluster privato on-premise che dispone di un backend di storage ANF, è necessario attivare la funzione Dynamic ANF Pools. A tale scopo, è necessario fornire un ID di abbonamento da utilizzare per espandere e contrarre i pool di capacità.



Dynamic ANF Pools è una funzionalità delle applicazioni gestite da Astra che utilizzano un backend di storage ANF (Azure NetApp Files). Quando si esegue il backup di queste applicazioni, Astra espande e contrae automaticamente i pool di capacità a cui appartengono i volumi persistenti di un fattore pari a 1.5. In questo modo si garantisce spazio sufficiente per il backup senza dover sostenere costi aggiuntivi permanenti. Vedere "[Backup delle applicazioni Azure](#)" per ulteriori informazioni.

1. Aggiungere l'identificativo dell'abbonamento Azure

Eseguire la seguente chiamata API REST.



È necessario aggiornare l'esempio di input JSON in base all'ambiente in uso, inclusi l'ID di abbonamento e il valore base64 per l'entità del servizio.

Metodo HTTP	Percorso
POST	/accounts/{account_id}/core/v1/credentials

Esempio di input JSON

```
{
  "keyStore": {
    "privKey": "SGkh",
    "pubKey": "UGhpcyCpcyBhbibleGFtcGxlLg==",
    "base64":
    "fwogICAgJmFwcElkIjogIjY4ZmSiODFiLTU0YWYtNDdjNC04ZjUzLWE2NDdlZTUzMGZkZCIsc
    iAgICAgIzG1zcGxheU5hbWUiOiAic3AtYXN0cmEtZGV2LXFhIiwKICAgICJuYW11IjogImh0dHA
    6Ly9zcC1hc3RyYS1kZXYtcWEiLAogICAgInBhc3N3b3JkIjogIlllLQThRfk9IVVJkZWZYM0pST
    WJlLnUeFBleVE0UnNwTG9DcUJjazAiLAogICAgInRlbnFudCI6ICIwMTFjZGY2Yy03NTEyLTQ
    3MDUtYjI0ZS03NzIxYWZkOGNhMzciLAogICAgInN1YnNjcmlwdGlvbklkIjogImIyMDAxNTVmL
    TAwMWEtNDNiZS04N2JlLTNlZGRlODNhY2VmNCIKfQ=="
  },
  "name": "myCert",
  "type": "application/astra-credential",
  "version": "1.1",
  "metadata": {
    "labels": [
      {
        "name": "astra.netapp.io/labels/read-only/credType",
        "value": "service-account"
      },
      {
        "name": "astra.netapp.io/labels/read-only/cloudName",
        "value": "OCP"
      },
      {
        "name": "astra.netapp.io/labels/read-only/azure/subscriptionID",
        "value": "b212156f-001a-43be-87be-3edde83acef5"
      }
    ]
  }
}
```

Esempio di arricciamento

```
curl --location -i --request POST --data @JSONinput
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/credentials'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
--header 'Content-Type: application/astra-credential+json'
```

2. Aggiungere un bucket, se necessario

Se necessario, aggiungere un bucket all'applicazione gestita.

3. Eseguire un backup dell'applicazione gestita

Eseguire il flusso di lavoro "[Creare un backup per un'applicazione](#)". Il pool di capacità in cui è presente il volume persistente originale si espanderà e si ridurrà automaticamente.

4. Esaminare il registro eventi

Gli eventi di attività vengono registrati durante il backup. Eseguire il flusso di lavoro "[Elencare le notifiche](#)" per visualizzare i messaggi.

Informazioni sul copyright

Copyright © 2023 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.