# Utilizzo della console VMware Cloud Services

VMware Cloud services

È possibile trovare la documentazione tecnica più aggiornata sul sito Web di VMware all'indirizzo:

https://docs.vmware.com/it/

**VMware, Inc.**
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

**VMware, Inc.**
Centro Leoni Palazzo A
Via Spadolini 5
Ground Floor
Milan, MI 20121
tel: +39 02 30412700
fax: +39 02 30412701
www.vmware.com/it

# Sommario

# Cos'è Cloud Services Console

1

VMware console di Cloud Services consente di gestire l'intero portafoglio di VMware Cloud services in cloud pubblici nativi e ibridi.

Per informazioni su come gestire utenti e gruppi, assegnare loro ruoli alle risorse e ai servizi dell'Organizzazione, nonché visualizzare le app OAuth che hanno accesso all'Organizzazione, vedere la documentazione Gestione identità e accessi.

Si stanno cercando informazioni sui costi correnti e i più recenti dettagli di fatturazione? È necessario gestire i metodi di pagamento o modificare il metodo di pagamento predefinito? Si desiderano informazioni su come aggiungere crediti promozionali e impegni? Vedere la documentazione Fatturazione e sottoscrizioni.

Per vedere come gestire le Organizzazioni, creare app OAuth nell'Organizzazione e, se si appartiene a più Organizzazioni, passare da un'Organizzazione all'altra, vedere Gestione delle Organizzazioni.

Si desidera modificare la lingua e la formattazione regionale, proteggere l'account con MFA, generare token API e modificare il profilo utente? Non cercare oltre. Consultare Gestione dell'account.

# Come registrarsi in VMware Cloud Services

2

Che tu abbia bisogno di effettuare la migrazione al cloud, unificare le operazioni multi-cloud, organizzare la scalabilità su richiesta o creare app moderne, all'indirizzo VMware Cloud troverai la soluzione per le tue necessità.

Esistono diversi modi per iniziare a utilizzare VMware Cloud services. Un utente di VMware Cloud services nuovo o esistente può eseguire l'onboarding di un servizio in uno dei seguenti modi:

- Acquistare un servizio dal sito Web VMware Marketing.
- Iscriversi a un servizio gratuito o di prova dal sito Web VMware Marketing.
- Acquistare un servizio dall'ufficio vendite di VMware
- Acquistare un servizio da un rivenditore partner VMware.

In base al servizio di cui si sta effettuando l'onboarding, possono essere presenti differenze nel workflow di onboarding.

Se l'azienda utilizza già VMware Cloud services, è possibile eseguire l'onboarding in un'Organizzazione esistente richiedendo l'accesso all'Organizzazione. La procedura per richiedere e ricevere il primo accesso a un'Organizzazione VMware Cloud services può variare in base all'account.

- Se l'account non è federato, vedere Come eseguire l'onboarding come utente in VMware Cloud Services.
- Se l'account è federato, vedere Come eseguire l'onboarding in qualità di utente con un account federato.

La sequenza di passaggi tipica per l'iscrizione a VMware Cloud services tramite l'onboarding del servizio è la seguente:

**Procedura**

1. Avvia il processo di onboarding al momento della registrazione al servizio o tramite il link fornito nell'invito.
2. Se non si dispone di un account VMware, seguire i passaggi per crearne uno.
3. Se si dispone già di un account VMware, accedere a VMware Cloud Services.
4. Seleziona o crea Organizzazione VMware Cloud services in cui eseguire l'onboarding del servizio.

5 Una volta eseguito l'onboarding del servizio in un'Organizzazione, si diventa Proprietario dell'Organizzazione, un ruolo che consente di invitare altri utenti e concedere l'accesso all'Organizzazione e ai relativi servizi:

   a Nel menu principale a sinistra, selezionare **Identità e accessi > Utenti attivi**.

   b Fare clic su **Aggiungi utenti**.

   c Digitare l'indirizzo e-mail dell'utente che si desidera invitare.

   d Selezionare i ruoli dell'Organizzazione e del servizio.

   e Selezionare la casella di controllo per l'invito tramite e-mail da inviare al nuovo utente e quindi fare clic su **Aggiungi**.

      L'utente riceve un'e-mail di invito con un collegamento per eseguire l'onboarding nell'Organizzazione con i ruoli assegnati.

Operazioni successive

Per ulteriori informazioni e procedure dettagliate per i diversi workflow di onboarding del servizio, vedere la guida Guida introduttiva a VMware Cloud Services.

# Come eseguire l'onboarding come utente in VMware Cloud Services

Per iniziare a utilizzare VMware Cloud Services come nuovo utente senza accesso ad alcuna Organizzazione e con un account non federato, è innanzitutto necessario ottenere l'accesso all'Organizzazione e al servizio da un **Proprietario dell'Organizzazione**.

La richiesta dell'accesso iniziale a VMware Cloud Services è un processo offline che può essere avviato dall'utente o dal **Proprietario dell'Organizzazione**. In genere, dopo aver ricevuto dal **Proprietario dell'Organizzazione** i ruoli dell'Organizzazione e del servizio nell'Organizzazione, si riceve un'e-mail con un collegamento all'Organizzazione.

1 Fare clic sul collegamento **Visualizza i miei ruoli** per accedere all'Organizzazione.

2 Se non si dispone di un account VMware, verrà richiesto di crearne uno.

3 Se si dispone già di un account VMware, è possibile accedere all'Organizzazione e iniziare a utilizzare i servizi in base ai ruoli dell'Organizzazione e all'accesso ai servizi di cui si dispone.

Se si desidera richiedere ruoli aggiuntivi nell'Organizzazione, vedere Come richiedere ruoli aggiuntivi.

# Come eseguire l'onboarding in qualità di utente con un account federato

In qualità di utente non membro dell'Organizzazione con un dominio federato, il primo accesso a VMware Cloud services con l'account aziendale dà l'avvio a un workflow di onboarding.

Durante il processo di onboarding, è possibile richiedere l'accesso selezionando in autonomia Organizzazioni, servizi, ruoli di Organizzazione e servizio. Le richieste devono essere approvate dai **proprietari dell'Organizzazione**. Questa operazione potrebbe richiedere del tempo.

Le Organizzazioni selezionabili nel workflow di onboarding sono Organizzazioni presenti nel proprio dominio federato aziendale attivate per l'Identity Governance and Administration (IGA). Se è necessario ottenere l'accesso a un'Organizzazione non attivata per l'IGA, occorre ricevere un link di invito da un **Proprietario dell'Organizzazione** per eseguire l'onboarding.

Procedura

1 Andare in https://cloud.vmware.com/ e fare clic su **Accedi**.

2 Nella schermata di benvenuto di VMware Cloud services, inserire le credenziali dell'account aziendale.

   Il primo passaggio del workflow di onboarding mostra l'elenco delle Organizzazioni attivate per l'IGA associate alla propria azienda.

3 Selezionare l'Organizzazione a cui si desidera accedere e fare clic su **Continua**.

4 Selezionare il ruolo nell'Organizzazione specificata.

   Il ruolo dell'Organizzazione determina il livello di accesso e le autorizzazioni di cui si dispone nell'Organizzazione. Quando si esegue l'onboarding con un account federato, è possibile richiedere solo il ruolo di **Membro dell'Organizzazione** predefinito. Dopo l'onboarding, è possibile richiedere ulteriori ruoli. Per ulteriori informazioni, vedere Come richiedere ruoli nelle Organizzazioni attivate per la governance.

5 Fare clic su **Continua**.

   Nel passaggio del workflow **Seleziona ruoli di servizio** sono visualizzati i servizi disponibili nell'Organizzazione selezionata.

6 Per ogni servizio a cui si desidera accedere come **Membro dell'Organizzazione**, utilizzare gli elenchi a discesa per selezionare i ruoli di servizio.

   **Nota** I ruoli di servizio sono specifici del servizio. Se non si è sicuri dei ruoli di servizio necessari, consultare la documentazione del servizio a cui si desidera accedere.

7 Fare clic su **Continua**.

8 Nel passaggio del workflow di onboarding **Finalizza richiesta**, definire il periodo di tempo per la richiesta di accesso al servizio.

9 Nella casella di testo **Giustificazione aziendale** digitare un messaggio per il **Proprietario dell'Organizzazione**, quindi fare clic su **Continua**.

   La richiesta viene visualizzata nell'elenco **Richieste in sospeso**, in attesa dell'approvazione da parte di un **Proprietario dell'Organizzazione**.

10 Per richiedere l'accesso a un'altra Organizzazione attivata per l'IGA nel proprio dominio federato, fare clic su **Invia nuova richiesta**.

11 Ripetere i passaggi da 3 a 9.

### Operazioni successive

L'approvazione per i ruoli di Organizzazione e servizio richiesti può richiedere qualche minuto. Fino ad allora, è possibile accedere alla console di Cloud Services per controllare lo stato delle richieste inviate, annullare una richiesta creata o crearne una nuova.

# Come accedere a Console Cloud Services

3

Un utente di VMware Cloud Services può accedere a console di Cloud Services con le credenziali dell'account VMware. Se l'account è federato, si accede utilizzando le credenziali dell'account aziendale.

Quando un utente accede a VMware Cloud Services e dopo l'esito positivo dell'autenticazione, vengono generati un token di accesso e di aggiornamento per la sessione di accesso dell'utente. Entrambi i token vengono generati in background utilizzando l'app OAuth 2.0 e hanno valori TTL (Time to Live) predefiniti:

- TTL di 30 minuti per il token di accesso.
- TTL di 24 ore per il token di aggiornamento.

Questo significa che dopo aver eseguito correttamente l'accesso, il token di accesso rimane valido solo per 30 minuti. In seguito, diventa non valido e il token di aggiornamento viene utilizzato per rigenerare il token di accesso in modo che l'utente possa continuare con la sessione di accesso. Dopo 24 ore, il token di aggiornamento scade e l'utente deve eseguire nuovamente l'accesso.

Al momento, i valori TTL predefiniti per i token di accesso e di aggiornamento non possono essere modificati.

### Prerequisiti

- È necessario disporre di un ruolo organizzazione in una o più organizzazioni di VMware Cloud Services.

### Procedura

1. Aprire una finestra del browser e passare a https://console.cloud.vmware.com/.
2. Immettere l'e-mail dell'account e fare clic su **Avanti**.
3. Digitare la password e fare clic su **Accedi**.

### Risultati

Una volta completato l'accesso, nella home page di VMware Cloud Services vengono visualizzati i servizi disponibili nell'Organizzazione.

# Che cos'è un'Organizzazione di servizi cloud?

4

VMware Cloud utilizza le Organizzazioni per fornire accesso controllato a uno o più servizi.

In qualità di azienda che utilizza più servizi cloud, le Organizzazioni forniscono un modo semplice per mappare i gruppi e i processi di business in Organizzazioni diverse.

Per gestire l'Organizzazione e le relative risorse, si utilizza console di Cloud Services, ad esempio:

- Ruoli e autorizzazioni di utenti e gruppi.
- Onboarding di ulteriori servizi.
- Recupero di informazioni su fatturazione e sottoscrizioni.
- Visualizzazione dei dati di utilizzo dei servizi dell'Organizzazione.
- Impostare i criteri di autenticazione nell'Organizzazione.
- Controllo dei registri degli eventi.
- Ricezione di assistenza.

I ruoli organizzazione assegnati nell'Organizzazione determinano l'accesso alle funzionalità di console di Cloud Services. I ruoli di servizio di cui si dispone all'interno dell'Organizzazione determinano i VMware Cloud services disponibili nell'organizzazione a cui è possibile accedere. È possibile disporre di ruoli diversi in più organizzazioni.

# Come utilizzare il catalogo di Cloud Services

5

Il catalogo di VMware Cloud Services rappresenta un modo semplice per visualizzare, sfogliare, cercare e filtrare i servizi che soddisfano criteri specifici.

Il catalogo dei servizi è la prima pagina che si apre quando si accede a console di Cloud Services. Ogni elemento del catalogo è rappresentato da una scheda separata che visualizza informazioni sul servizio. Se un servizio è disponibile nell'Organizzazione, è possibile richiedere l'accesso facendo clic sul collegamento nella scheda del servizio.

| Da... | È possibile... |
|---|---|
| Scheda **Servizi** > **Organizzazione** | ■ Nella sezione **I miei servizi** della pagina è possibile trovare tutti i servizi per i quali si è già ricevuta l'assegnazione di ruoli di servizio. Fare clic su una scheda di servizio per avviare un servizio.<br>■ La sezione **Altri servizi** mostra un elenco di tutti i servizi dell'Organizzazione per i quali non si è ricevuta l'assegnazione di ruoli di servizio.<br><br>Tutte le richieste di accesso devono essere approvate da un **Proprietario dell'Organizzazione**. Per informazioni sull'invio di una richiesta di accesso per i ruoli di servizio, vedere Come richiedere ruoli aggiuntivi. |
| Scheda **Servizi** > **Consigliato** | Consultare un elenco di consigli sui servizi in base alle sottoscrizioni ai servizi correnti. |
| Scheda **Servizi** > **Tutti** | Sfogliare o filtrare il catalogo di VMware Cloud Services completo. È possibile filtrare il catalogo dei servizi in base alla categoria e al modello di prezzo. |
| Qualsiasi pagina in **Servizi** | Utilizzare la casella **Cerca un servizio** nell'angolo superiore destro della pagina per trovare i servizi pertinenti per parola chiave. |

Leggi i seguenti argomenti:

# Azioni disponibili per il catalogo dei servizi

È possibile gestire l'accesso a VMware Cloud services direttamente dalle schede di servizio nel catalogo di VMware Cloud services. Le azioni che è possibile eseguire rispetto a un determinato servizio dipendono dal ruolo nell'Organizzazione e dal tipo di servizio a cui si desidera accedere. Sono disponibili diverse azioni per i servizi gratuiti, di prova e a pagamento.

## Azioni membro dell'organizzazione

| Se si dispone dell'accesso a... | e il servizio è... | l'azione che è possibile eseguire è... | il risultato di questa azione è... |
|---|---|---|---|
| al servizio | gratis, prova attiva o a pagamento | **Avvia servizio** | viene avviato il servizio in Cloud Services Console |
| | gratis, prova attiva o a pagamento con una o più istanze del servizio | **Avvia servizio** con una descrizione comando se è presente un'istanza del servizio | l'istanza del servizio selezionata viene avviata in Cloud Services Console |
| | | **Avvia servizio** con un menu a discesa se sono presenti più istanze per il servizio | |
| all'Organizzazione, ma non al servizio | gratis, prova attiva o a pagamento | **Richiedi ruolo** | viene richiesto di richiedere un ruolo per il servizio |
| nessun accesso al servizio e il servizio non è presente nell'Organizzazione | gratis, prova attiva o a pagamento | **Accesso** | viene richiesto di eseguire l'onboarding del servizio |
| | | **Ulteriori informazioni** | avvia la pagina dei dettagli del servizio |
| | prova scaduta | **Ulteriori informazioni** | apre la pagina con i dettagli del servizio o le informazioni sull'acquisto |

## Azioni proprietario dell'organizzazione

| Se si dispone dell'accesso a... | e il servizio è... | l'azione che è possibile eseguire è... | il risultato di questa azione è... |
|---|---|---|---|
| al servizio | gratis o a pagamento | **Avvia servizio** | viene avviato il servizio in Cloud Services Console |
| | prova attiva | **Avvia servizio** | viene avviato il servizio in Cloud Services Console |
| | | **Visualizza dettagli versione di prova** dall'icona con i puntini di accesso (***) | apre la pagina dei dettagli della versione di prova del servizio |
| | | **Servizio di acquisto** dall'icona con i puntini di accesso (***) | apre la pagina con le informazioni di acquisto |

| Se si dispone dell'accesso a... | e il servizio è... | l'azione che è possibile eseguire è... | il risultato di questa azione è... |
|---|---|---|---|
| all'Organizzazione, ma non al servizio | gratis, prova attiva o a pagamento | **Accesso** | viene richiesto di accedere al servizio modificando i ruoli |
| | | **Ulteriori informazioni** | avvia la pagina dei dettagli del servizio |
| non si dispone di accesso al servizio e il servizio non è presente nell'organizzazione | gratis, a pagamento o a pagamento con prova | **Accesso** | viene richiesto di eseguire l'onboarding del servizio |
| | prova scaduta<br>In base alla configurazione dell'Organizzazione, viene visualizzata una delle quattro azioni seguenti. | **Acquista servizio** | apre la pagina con le informazioni di acquisto |
| | | **Conferma metodo di pagamento** | apre la pagina **Conferma metodo di pagamento** in Cloud Services Console |
| | | **Aggiungi metodo di pagamento** | apre la pagina **Informazioni sul pagamento** in Cloud Services Console e richiede di aggiungere i dettagli del metodo di pagamento per la propria Organizzazione |

# Come richiedere ruoli aggiuntivi

Un utente **Membro dell'Organizzazione** può accedere ai VMware Cloud services disponibili nell'Organizzazione attraverso un invito da parte di un utente **Proprietario dell'Organizzazione** o inviando una richiesta self-service.

La richiesta self-service sostituisce la necessità di attendere un invito da parte di un **Proprietario dell'Organizzazione** e consente di specificare i servizi e i ruoli a cui si desidera accedere all'interno dell'Organizzazione, nonché il periodo di tempo per l'accesso richiesto.

**Nota** I **proprietari dell'Organizzazione** possono assegnare da soli ruoli aggiuntivi all'Organizzazione e al servizio. Per ulteriori informazioni, fare riferimento a Come gestire ruoli e autorizzazioni.

Per inviare una richiesta self-service, sfogliare il catalogo dei servizi per individuare il servizio per il quale si desidera richiedere ruoli aggiuntivi. È sufficiente fare clic sul collegamento **Richiedi accesso** nella scheda del servizio. Viene aperta una finestra pop-up dai cui menu a discesa è possibile selezionare un nuovo ruolo del servizio.

Tutte le richieste vengono inviate ai **proprietari dell'Organizzazione** che possono approvare, negare o modificare le richieste prima dell'approvazione. Al termine dell'elaborazione della richiesta si riceverà una notifica tramite e-mail.

## Come visualizzare le richieste self-service inviate?

È possibile visualizzare in qualsiasi momento le richieste di servizio in sospeso e passate nella sezione **Cronologia delle mie richieste** della pagina **Il mio account > I miei ruoli**.

## È possibile annullare una richiesta self-service creata?

È possibile annullare solo le richieste self-service con stato in sospeso. Aprire la pagina **I miei ruoli** e fare clic sul collegamento **Annulla** in corrispondenza della richiesta da eliminare.

## Perché nel riquadro del servizio non viene visualizzato il link **Richiedi accesso**?

L'opzione che consente di richiedere ruoli di servizio aggiuntivi può essere disattivata nelle Organizzazioni attivate per Identity Governance and Administration (IGA) con domini federati. In questo caso, è necessario un invito da parte di un **Proprietario dell'Organizzazione**.

# Come gestire l'account Cloud Services

6

Puoi gestire il tuo profilo utente dal tuo account VMware Cloud services. Puoi selezionare le preferenze relative alla lingua e al formato regionale, le impostazioni di sicurezza come la password e le impostazioni MFA, e generare e gestire i token API. È possibile anche visualizzare i ruoli di cui disponi nella tua Organizzazione.

Per accedere al proprio account, fare clic sul nome utente, quindi fare clic su **Il mio account**.

Leggi i seguenti argomenti:



## Come visualizzare il profilo utente

Il profilo utente è costituito dai dettagli forniti al momento della creazione dell'account cliente VMware. In base al profilo del cliente, potrebbe essere possibile modificare il profilo utente.

**Nota** Non è possibile modificare l'indirizzo e-mail con cui è stata effettuata la registrazione.

È possibile visualizzare il profilo utente in console di Cloud Services o accedendo all'account My VMware all'indirizzo https://customerconnect.vmware.com/.

Se l'account non è federato, è possibile modificare i dettagli del profilo in console di Cloud Services; le modifiche apportate verranno salvate nell'account VMware e viceversa.

Se l'account è federato, le opzioni di modifica sono limitate. Ad esempio, non è possibile modificare il nome del profilo e visualizzare solo i dettagli dell'ID VMware.

### Procedura

1 Nella barra degli strumenti di console di Cloud Services, fare clic sul nome utente e selezionare **Il mio account**.

2 Nella pagina **Profilo**, apportare le modifiche e fare clic su **Salva**.

## Come reimpostare la password

La password dei VMware Cloud services corrisponde a quella dell'ID VMware.

È possibile reimpostare l'ID VMware nella piattaforma VMware Cloud services o accedendo all'account di VMware Customer Connect su https://customerconnect.vmware.com/.

**Procedura**

1 Nella barra degli strumenti di console di Cloud Services, fare clic sul nome utente e scegliere **Il mio account > Sicurezza**.

2 Immettere le informazioni per modificare la password e fare clic su **Modifica password**.

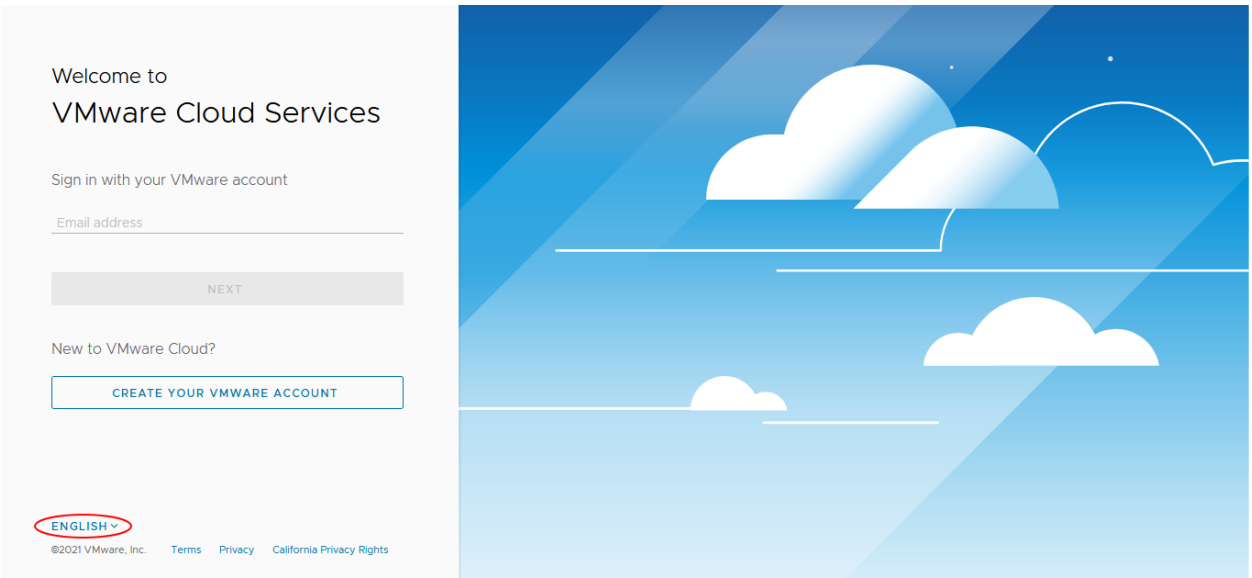
L'ID VMware viene reimpostato.

# Come modificare la lingua e il formato regionale

È possibile modificare la lingua di visualizzazione nella lingua preferita prima di eseguire l'onboarding dei servizi cloud oppure nelle impostazioni dell'account, dove è anche possibile impostare il formato regionale.

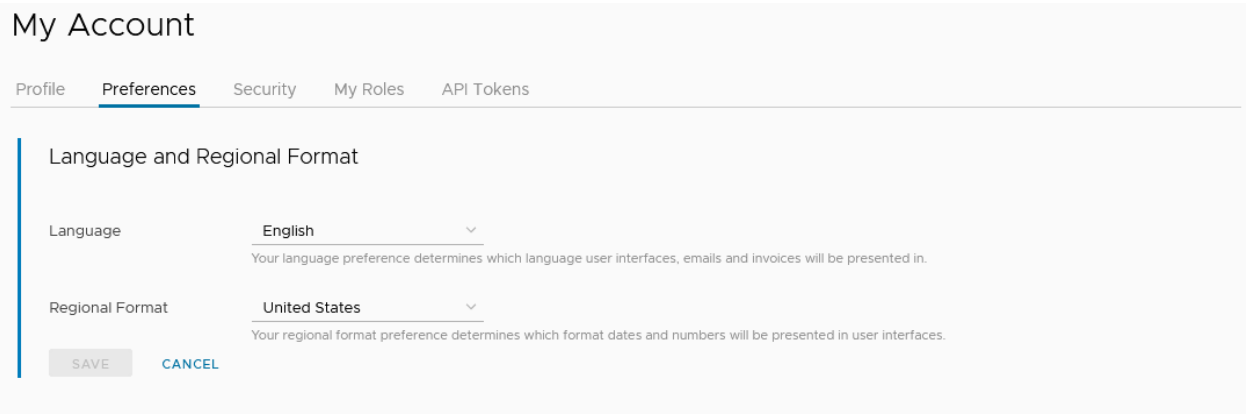
## Esperienza di onboarding nella lingua preferita

Se non è stato ancora eseguito l'onboarding VMware Cloud services, è possibile scegliere la lingua preferita prima di accedere. È supportato il formato regionale impostato nel browser.



## Modifica della lingua e del formato regionale

Per modificare la lingua e il formato regionale in qualsiasi momento dopo aver effettuato l'accesso, fare clic sul nome utente nella barra dei menu e selezionare **Il mio account > Preferenze**. Quindi fare clic su **Modifica**.




Se si cambia la lingua, è necessario sapere che non tutte le pagine vengono visualizzate nella lingua selezionata. Inoltre, alcuni moduli supportano solo i caratteri inglesi. Provvederemo a informare l'utente quando è supportato solo l'inglese.

## È possibile impostare un formato regionale diverso dalla lingua?

Se si imposta un formato regionale diverso dalla lingua preferita, in alcuni casi il formato regionale predefinito per la lingua selezionata potrebbe sostituire il formato regionale selezionato. Questo può verificarsi nella visualizzazione di e-mail, istruzioni e fatture. Ad esempio, se si sceglie l'inglese come lingua preferita e il giapponese come formato regionale, alcune comunicazioni potrebbero essere visualizzate nel formato regionale Stati Uniti. Di seguito è riportato un elenco delle lingue e del relativo formato regionale predefinito.

| Lingua | Formato regionale predefinito |
|---|---|
| Inglese | US |
| Cinese semplificato | CN |
| Cinese tradizionale | TW |
| Spagnolo | ES |
| Italiano | IT |
| Francese | FR |
| Giapponese | JP |
| Tedesco | DE |
| Coreano | KR |

# Come proteggere l'account con l'autenticazione multifattore

L'autenticazione multifattore (MFA) è un incremento della sicurezza che richiede la presentazione di due elementi di prova, ovvero le credenziali, al momento dell'accesso. Queste credenziali possono essere qualcosa di conosciuto dall'utente, come la password, e qualcosa di cui si è in possesso, come ad esempio un'applicazione che genera un codice d'accesso valido una sola volta. MFA aiuta a proteggere l'accesso a dati e applicazioni aggiungendo un ulteriore livello di sicurezza.

Probabilmente la MFA è già stata utilizzata in qualche modo. Ad esempio, se è stato effettuato l'accesso a un sito Web che invia un codice al dispositivo mobile per ottenere l'accesso al proprio account.

**Nota** Se l'account VMware Cloud Services è federato, la MFA viene gestita dal team di sicurezza aziendale.

Per proteggere l'account VMware Cloud Services con la MFA, scaricare un'applicazione di autenticazione sul proprio dispositivo mobile. Creare un dispositivo MFA virtuale. L'applicazione genera un codice di autenticazione di sei cifre compatibile con lo standard di password monouso basato sul tempo. Questo codice viene utilizzato insieme all'ID e alla password di VMware per accedere ai servizi cloud.

Quando si configura la MFA per il proprio account, si riceve una serie di 10 codici di ripristino. Salvare questi codici in un luogo sicuro. Saranno necessari per accedere se non si ha il dispositivo MFA a portata di mano o se è stato perso.

| Ecco come si procede | |
|---|---|
| Attivazione del dispositivo MFA. | 1 Fare clic sul proprio nome utente nel menu e selezionare **Il mio account > Sicurezza**.<br>2 Fare clic su **Attiva dispositivo MFA** e seguire le istruzioni per configurare il dispositivo.<br>3 MFA viene attivata automaticamente. Al successivo accesso, utilizzare l'ID e la password di VMware e un codice di autenticazione generato dall'app. |
| Per disattivare la MFA in modo da accedere solo con ID e password My VMware. | 1 Fare clic sul proprio nome utente nel menu e selezionare **Il mio account > Sicurezza**.<br>2 Fare clic sul tasto di alternanza **MFA è attivata**. |
| Disattivazione del dispositivo MFA. | 1 Fare clic sul proprio nome utente nel menu e selezionare **Il mio account > Sicurezza**.<br>2 Fare clic su **Disattiva dispositivo MFA**. |
| Rigenerare i codici di recupero | È possibile rigenerare un nuovo set di codici di recupero in qualsiasi momento accedendo a **Il mio account > Sicurezza**. |

## Quale applicazione di autenticazione a due fattori è possibile utilizzare?

VMware Cloud services supportano le seguenti applicazioni di autenticazione a due fattori.

È possibile scaricare l'applicazione di autenticazione per il proprio dispositivo facendo clic sul collegamento corrispondente di seguito riportato.

| Dispositivo | Applicazione di autenticazione |
| --- | --- |
| iOS | ■ Google Authenticator. Vedere https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8.<br>■ Duo Mobile. Vedere https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile. |
| Android | ■ Google Authenticator. Vedere https://support.google.com/accounts/answer/1066447?hl=en.<br>■ Duo Mobile. Vedere https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile. |
| Windows Phone | ■ Authenticator. Vedere https://www.microsoft.com/en-us/store/p/authenticator/9wzdncrfj3rj?rtc=1.<br>■ Duo Mobile. Vedere https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile. |
| Blackberry | Google Authenticator<br>Vedere https://support.google.com/accounts/answer/1066447. |

Per ulteriori informazioni sulle applicazioni MFA virtuali, vedere https://tools.ietf.org/html/rfc6238.

Quali azioni eseguire quando non è possibile accedere con MFA

Quando si attiva MFA in VMware Cloud services, si riceve un set di 10 codici di ripristino. Questi codici possono essere copiati, scaricati e persino stamparli, ma è necessario conservarli in un luogo sicuro.

## Come risolvere i problemi di MFA quando non è possibile accedere

Quando si attiva MFA in VMware Cloud services, si riceve un set di 10 codici di ripristino. Questi codici possono essere copiati, scaricati e persino stamparli, ma è necessario conservarli in un luogo sicuro.

Se si verificano problemi durante l'accesso a VMware Cloud services, è possibile utilizzare un codice di ripristino.

| Se... | Procedere così... |
| --- | --- |
| Non si ha accesso al proprio dispositivo MFA o il dispositivo è stato perso | Nella pagina di accesso di VMware Cloud Services, fare clic sul link **Risoluzione dei problemi MFA**. Quando richiesto, immettere una delle chiavi di recupero. |
| I codici di recupero sono andati persi | Contattare l'assistenza VMware chiamando un numero di telefono dell'assistenza o accedendo all'assistenza chat su VMware Customer Connect. |

# Come generare i token API

È possibile utilizzare token API per autenticarsi quando si effettuano connessioni API autorizzate. In precedenza denominato token di aggiornamento OAuth, un token API viene scambiato per un token di accesso e autorizza l'accesso per Organizzazione. È possibile generare token API dalla pagina dell'account in console di Cloud Services o tramite IVMware Cloud Services.

I token vengono generati utilizzando un algoritmo speciale che preleva caratteri alfanumerici. Ogni token è una combinazione univoca di 65 caratteri. Quando si genera un token, ne si determina la durata e gli ambiti:

- Il TTL (Time to Live) di un token può variare da alcuni minuti a diversi mesi oppure può non scadere mai. La durata predefinita è sei mesi.
- Gli ambiti forniscono un modo per implementare il controllo sulle aree dell'Organizzazione a cui un token può accedere, in particolare quale ruolo in un'Organizzazione, quali servizi e il livello di autorizzazioni.

### Prerequisiti

È bene garantire una posizione di archiviazione sicura e protetta per i token API.

### Procedura

1. Nella barra degli strumenti di console di Cloud Services, fare clic sul proprio nome utente e selezionare **Il mio account > Token API**.
2. Fare clic sul collegamento **Genera nuovo token API**.
3. Immettere un nome per il token.
4. Specificare la durata del token desiderata.

> **Nota** Un token che non ha scadenza può essere un rischio per la sicurezza se compromesso. In questo caso, è necessario revocare il token.

5 Definire gli ambiti per il token. La selezione deve essere basata sui ruoli supportati dall'account utente.

| Ambito | Descrizione |
| --- | --- |
| **Ruoli organizzazione** | I ruoli dell'Organizzazione determinano l'accesso di un utente alle risorse dell'Organizzazione.<br>■ Selezionare uno o più ruoli dell'Organizzazione per il token API. |
| **Ruoli servizio** | I ruoli di servizio sono creati in set di autorizzazioni predefiniti che concedono l'accesso a VMware Cloud services.<br>■ Utilizzare l'icona a forma di freccia accanto al nome di un servizio per espandere i ruoli disponibili per tale servizio, quindi selezionare uno o più ruoli di servizio per il token API. |
| **Autorizzazioni** | Alcuni servizi consentono di effettuare una selezione più granulare assegnando un set limitato di autorizzazioni disponibili per un ruolo di servizio.<br>■ Quando si seleziona un ruolo di servizio, le autorizzazioni disponibili vengono visualizzate nella parte destra della tabella. Selezionare le autorizzazioni del servizio pertinenti per il token API. |

Se necessario, è possibile selezionare **Tutti i ruoli** e fornire al token l'accesso a tutti i ruoli di Organizzazione e di servizio.

**Nota** Anche se al token si assegna l'accesso a **Tutti i ruoli**, esso disporrà solo di quei ruoli di accesso supportati dall'account utente. Per visualizzare i ruoli di Organizzazione e di servizio di cui si dispone, nella pagina **Il mio account** selezionare la scheda **I miei ruoli**.

6 (Facoltativo) Selezionare la casella di controllo **ID aperto** per recuperare un token conforme all'ID aperto con dettagli utente estesi.

7 (Facoltativo) Impostare una preferenza e-mail per ricevere un promemoria quando il token sta per scadere.

8 Fare clic su **Genera**.

9 Salvare le credenziali del token in un luogo sicuro in modo da poterle recuperare per utilizzarle in un secondo momento.

Per motivi di sicurezza, dopo aver generato il token nella pagina Token API viene visualizzato solo il nome del token e non le credenziali del token. Questo significa che non sarà più possibile riutilizzare il token copiando le credenziali da questa pagina.

10 Fare clic su **Continua**.

Oltre ai token API, è possibile utilizzare le app OAuth per autenticare le applicazioni. Per visualizzare quando utilizzare le app OAuth rispetto ai token API, vedere Differenza tra le app OAuth e i token API

## Esempio: Utilizzo di un token API per interagire con le API di VMware Cloud Services

È possibile utilizzare un token API per interagire con le nostre API scambiandolo per un token di autenticazione.

1 Generare un token API.

2 Eseguire `POST` in https://console.cloud.vmware.com/csp/gateway/am/api/auth/api-tokens/authorize.

3 Nell'intestazione, includere le seguenti richieste:

- accetta: `application/json`
- tipo di contenuto: `application/x-www-form-urlencoded`/

4 Nel corpo, includere la richiesta `refresh_token={token value}`.

5 Utilizzare il token di autenticazione nell'intestazione `csp-auth-token` nelle chiamate HTTP dello script.

## Come gestire i token API

In qualità di unico proprietario dei token API, è propria responsabilità archiviarli, eseguirne il backup e gestirli in modo sicuro.

Per visualizzare e gestire i token API, fare clic sul nome utente, quindi selezionare **Il mio account > Token API**.

- Per rigenerare un token, fare clic su **Rigenera**. In questo modo si sostituisce il token esistente con uno nuovo. Per continuare a chiamare le API, è necessario aggiornare il token nelle chiamate API.
- Per disattivare un token, fare clic su**Revoca**. In questo modo viene revocato il token API e il token di accesso associato.
- Per impedire l'accesso non autorizzato alle risorse dell'Organizzazione, si consiglia vivamente di conservare i token API generati in un luogo sicuro e protetto. VMware Cloud Services non verifica la presenza di una proof-of-possession, ma acquisisce gli eventi di controllo dell'utilizzo del token quando:
  - un utente genera un token API
  - un utente revoca uno o tutti i token personali
  - il tentativo di un utente di generare il token di accesso tramite l'aggiornamento del token API non riesce

  **Nota** Per visualizzare i registri degli eventi di controllo in VMware Cloud Services, è necessario disporre di un ruolo di **Proprietario dell'Organizzazione**.

- Per aggiungere un ulteriore livello di sicurezza alle API, è possibile impostare l'autenticazione multifattore per i token API. Per ulteriori informazioni, vedere Come proteggere i token API tramite l'autenticazione multifattore.
- Se il token dell'API è stato disattivato da un **Proprietario dell'Organizzazione** per aver violato qualsiasi criterio impostato nell'Organizzazione o per non aver eseguito l'adesione agli standard dell'Organizzazione, si riceverà una notifica tramite e-mail da VMware Cloud Services. Nella pagina **Il mio account > Token API**, i token disattivati sono contrassegnati con l'etichetta 

.

La seguente tabella riepiloga le attività di gestione self-service dei token API più comuni:

| Se si desidera... | Procedere così... |
|---|---|
| Estendere la validità di un token API scaduto. | È necessario rigenerare il token. |
| Rigenerare un token API valido. | È possibile rigenerare un token in qualsiasi momento. Se si rigenera un token, si revocano tutte le istanze del token precedente. Se è stato utilizzato il token, ad esempio in uno degli script, ricordarsi di sostituirlo con il token appena generato. |
| Sostituire un token API compromesso. | Se si ritiene che un token è stato compromesso, è possibile revocarlo per impedire accessi non autorizzati. È possibile generare un nuovo token per rinnovare l'autorizzazione. |
| Eliminazione di un token API ancora valido. | È possibile eliminare un token API valido revocandolo. |
| Ripristinare un token API perso. | I token persi non possono essere ripristinati. È necessario revocare il token perso e generarne uno nuovo. |
| Riattivare un token API disattivato da un **Proprietario dell'Organizzazione** | Se un token disattivato è ancora valido, è necessario contattare il **Proprietario dell'Organizzazione** e chiedere la riattivazione. |

## Come proteggere i token API tramite l'autenticazione multifattore

Se si utilizzano i token API per accedere alle API di VMware Cloud Services, è possibile aggiungere un ulteriore livello di sicurezza attivando l'Autenticazione multifattore (MFA) sui token API.

In questo modo, anche se il token API risulta compromesso, i dati e le applicazioni vengono protetti da accessi non autorizzati. Dopo aver attivato la MFA, qualsiasi token che si tenta di scambiare per un token di accesso alle API di VMware Cloud Services richiede l'autenticazione MFA.

Per proteggere le API di VMware Cloud Services con la MFA, scaricare un'applicazione di autenticazione sul proprio dispositivo mobile. Creare un dispositivo MFA virtuale. L'applicazione genera un codice di autenticazione di sei cifre compatibile con lo standard di password monouso basato sul tempo. Per accedere alle API di VMware Cloud Services, è necessario fornire un token di sei cifre generato dal dispositivo MFA registrato.

| Ecco come si procede | |
|---|---|
| Attivazione del dispositivo MFA. | 1 Fare clic sul proprio nome utente nel menu e selezionare **Il mio account > Token API > MFA**.<br>2 Fare clic su **Attiva dispositivo MFA** e seguire le istruzioni per configurare il dispositivo.<br>3 MFA viene attivata automaticamente. All'utilizzo successivo di un token API per ottenere il token di accesso sarà richiesto un codice di autenticazione generato dall'app. |
| Per disattivare la MFA. | 1 Fare clic sul proprio nome utente nel menu e selezionare **Il mio account > Token API > MFA**.<br>2 Fare clic sull'interruttore **MFA è attivata**.<br>**Importante** Se l'Organizzazione applica l'utilizzo della MFA su token API, non è possibile disattivare la MFA. Anche se si può generare token API, non sarà possibile scambiarli per i token di accesso a meno che non si fornisca un codice d'accesso di sei cifre dal dispositivo MFA registrato. |
| Disattivazione del dispositivo MFA. | 1 Fare clic sul proprio nome utente nel menu e selezionare **Il mio account > Token API > MFA**.<br>2 Fare clic su **Disattiva dispositivo MFA**. |

# Come gestire i ruoli in un'Organizzazione

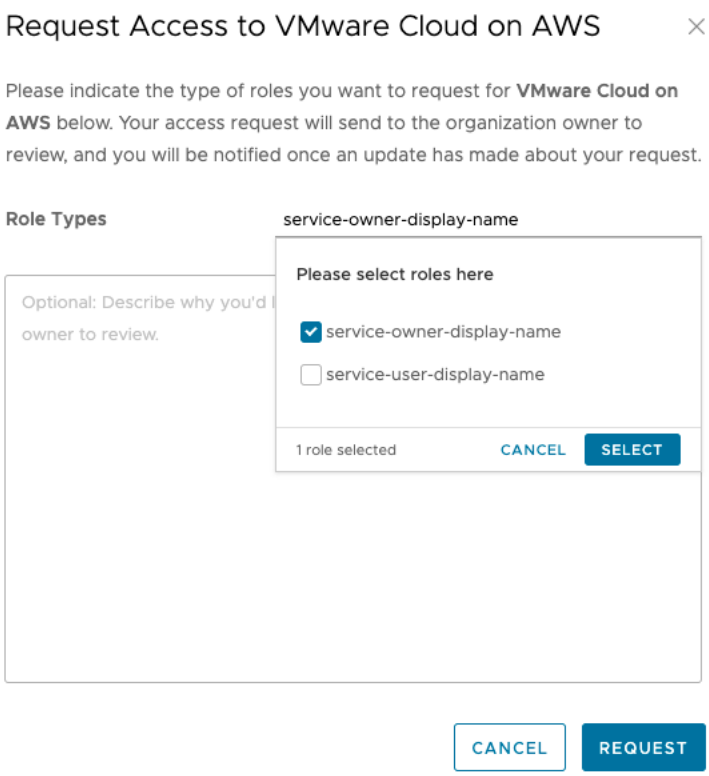
I ruoli vengono assegnati dagli utenti con il ruolo **Proprietario dell'Organizzazione**. In genere, si ricoprirà un ruolo nell'Organizzazione e un ruolo in uno o più servizi dell'Organizzazione. In qualità di utente **Membro dell'Organizzazione**, è possibile richiedere ruoli di servizio aggiuntivi per i servizi disponibili nell'Organizzazione ed eliminare i ruoli già assegnati. Per ottenere l'accesso al ruolo di servizio aggiuntivo, la richiesta deve essere approvata dal **Proprietario dell'Organizzazione**.

Per ulteriori informazioni sui ruoli dell'Organizzazione, vedere Come gestire ruoli e autorizzazioni.

Ecco come gestire i ruoli di servizio nell'Organizzazione:

- Per visualizzare i propri ruoli, verificare di quale accesso ai servizi si dispone e richiedere ruoli aggiuntivi, fare clic sul proprio nome utente e selezionare **Il mio account > I miei ruoli**.
- Per eliminare il ruolo di un servizio o un ruolo aggiuntivo dell'Organizzazione non più necessario, fare clic sul nome del servizio per espandere tutti i ruoli di cui si dispone per tale servizio. Dopo aver individuato il ruolo di servizio che si desidera rimuovere, fare clic su **Elimina ruolo**. Per essere applicata, la richiesta di eliminazione del ruolo deve essere approvata dal **Proprietario dell'Organizzazione**.
- Per visualizzare le richieste di ruolo precedenti, scorrere verso il basso fino alla sezione della pagina **Cronologia delle mie richieste**.

- Per richiedere ruoli di servizio aggiuntivi per i servizi già disponibili nell'Organizzazione, fare clic su **Richiedi ruoli** ed effettuare una selezione.




Se si è membri di un'Organizzazione attivata per l'Identity and Governance Administration (IGA), si dispone dell'opzione aggiuntiva per richiedere nuovi ruoli dell'Organizzazione. Per ulteriori informazioni, vedere Come richiedere ruoli nelle Organizzazioni attivate per la governance.

# Come richiedere ruoli nelle Organizzazioni attivate per la governance

I **proprietari dell'Organizzazione** attivati per Identity Governance and Administration possono consentire ai **Membri dell'Organizzazione** di inviare richieste di accesso self-service invece di concedere l'accesso tramite invito. Se questa opzione è disponibile nell'Organizzazione, è possibile richiedere ruoli aggiuntivi direttamente da console di Cloud Services.

Procedura

1 Accedere a VMware Cloud Services e andare alla pagina **Il mio account > I miei ruoli**.

2 Fare clic sul link **Aggiungi accesso al servizio**.

> **Nota** Se non viene visualizzato il link **Aggiungi accesso al servizio** significa che l'opzione delle richieste self-service è stata disattivata ed è possibile ottenere accessi aggiuntivi solo tramite un invito da parte del **Proprietario dell'Organizzazione**.

3 Selezionare i ruoli di Organizzazione e servizio aggiuntivi che si desidera richiedere.

4 Fare clic su **Invia**.

### Risultati

La richiesta viene creata e inviata per l'approvazione. Si riceverà una notifica quando un **Proprietario dell'Organizzazione** elaborerà la richiesta.

# Come gestire le Organizzazioni di Cloud Services 7

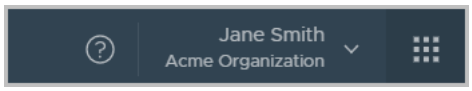
L'account VMware può essere associato a una o più Organizzazioni VMware Cloud services. VMware Cloud utilizza le Organizzazioni per fornire accesso controllato a uno o più servizi. Per accedere a un servizio cloud, è necessario appartenere a un'Organizzazione.

L'utente **Proprietario dell'Organizzazione** dispone dell'accesso a tutte le risorse dell'Organizzazione. È possibile aggiungere servizi cloud all'Organizzazione, quindi invitare gli utenti a partecipare. È possibile gestire i metodi di pagamento dell'Organizzazione e l'accesso degli utenti. Se si dispone di un utente ruolo di **Membro dell'Organizzazione** l'accesso alla risorsa dell'Organizzazione è limitato.

Per informazioni sui privilegi di ciascun ruolo all'interno dell'Organizzazione, vedere Come gestire ruoli e autorizzazioni.

## Organizzazione attiva

Quando si accede a VMware Cloud services, l'Organizzazione a cui è stato effettuato l'accesso viene visualizzata sotto il proprio nome utente nella barra dei menu della console di Cloud Services.




Se si appartiene a più di un'Organizzazione, è possibile passare dall'Organizzazione attiva a un'altra Organizzazione in qualsiasi momento. Puoi anche scegliere quale delle tue Organizzazioni viene visualizzata per impostazione predefinita quando effettui l'accesso.

## Visualizzazione dell'ID dell'organizzazione

Ogni Organizzazione ha un ID univoco. Potrebbe essere necessario utilizzare questo ID quando si interagisce con interfacce della riga di comando esterne come VMware Container Engine CLI. È possibile visualizzare l'ID dell'Organizzazione facendo clic sul proprio nome utente. Una versione abbreviata dell'ID viene visualizzata sotto il nome dell'Organizzazione. Per visualizzare l'ID completo dell'Organizzazione, fare clic sull'ID breve.

# Visualizzazione delle impostazioni dell'organizzazione

Puoi visualizzare il nome e l'ID dell'Organizzazione facendo clic sul tuo nome utente e selezionando **Visualizza Organizzazione**.

Se si è il **Proprietario dell'Organizzazione**, si può modificare il nome visualizzato dell'Organizzazione.

A seconda del proprio profilo cliente, è possibile anche visualizzare e modificare il paese e il CAP e aggiungere o modificare il tag utilizzato per le query alle API VMware.

Leggi i seguenti argomenti:

- Come accedere a un'altra Organizzazione
- Come specificare un'Organizzazione predefinita
- Come personalizzare l'intestazione di VMware Cloud Services

# Come accedere a un'altra Organizzazione

Se si appartiene a più di un'Organizzazione, è possibile passare dall'Organizzazione attiva a un'altra Organizzazione in qualsiasi momento.

Quando si accede ai servizi di VMware Cloud, viene visualizzata l'Organizzazione attiva. È possibile visualizzare il nome dell'Organizzazione attiva nel menu VMware Cloud Services, sotto il proprio nome utente.

### Procedura

1. Nel menu VMware Cloud Services, fare clic sulla freccia accanto al nome utente.
2. Dal menu, fare clic sulla freccia accanto al nome dell'Organizzazione.

   Viene visualizzato un elenco a discesa con i nomi delle Organizzazioni.
3. Selezionare l'Organizzazione che si desidera visualizzare.

# Come specificare un'Organizzazione predefinita

Se si appartiene a più di un'Organizzazione, è possibile scegliere quale delle Organizzazioni visualizzare per impostazione predefinita quando si esegue l'accesso.

Per impostazione predefinita, l'Organizzazione attiva è quella a cui si è stati invitati o quella che era visualizzata nel momento in cui ci si è disconnessi da VMware Cloud Services.

### Procedura

1. Nel menu VMware Cloud Services, fare clic sulla freccia accanto al nome utente.
2. Fare clic su **Imposta organizzazione predefinita**.

   Viene visualizzato l'elenco delle Organizzazioni.

3 Selezionare l'Organizzazione da visualizzare quando si esegue l'accesso.

# Come personalizzare l'intestazione di VMware Cloud Services

In qualità di utente **Proprietario dell'Organizzazione**, è possibile aggiungere un brand e personalizzare l'intestazione di VMware Cloud Services in modo che rifletta il brand della propria azienda.

L'intestazione personalizzata di VMware Cloud Services creata in questa attività è visibile solo per i **Membri dell'Organizzazione** che accedono a questa Organizzazione specifica.

### Prerequisiti

- È necessario disporre del ruolo di **Proprietario dell'Organizzazione**.
- È necessario conoscere le linee guida del branding aziendale.

### Procedura

1 Accedere a console di Cloud Services e passare a **Organizzazione > Dettagli**.

2 Nella sezione **Personalizzazione Organizzazione** della pagina dei dettagli dell'Organizzazione, fare clic su **Modifica**.

3 Nella casella di testo **Nome visualizzato intestazione**, inserire il nome che si desidera visualizzare nell'Organizzazione anziché VMware Cloud Services.

4 Per caricare il logo dell'Organizzazione per **Tema chiaro**, fare clic su **Sfoglia** e selezionare il file di immagine dalla macchina locale.

**Nota** Per le immagini del logo è possibile caricare solo i file `.svg`.

Il logo dell'intestazione per **Tema scuro** è impostato su **Uguale al tema chiaro** per impostazione predefinita. Per caricare un file di immagine diverso per **Tema scuro**, deselezionare la casella di controllo **Uguale al tema chiaro**, fare clic su **Sfoglia** e selezionare l'immagine dalla macchina locale.

La sezione **Anteprima** viene aggiornata per visualizzare le nuove modifiche apportate ai colori. È possibile ripristinare le modifiche apportate facendo clic su **Ripristina impostazioni predefinite**.

5 Per modificare la tavolozza dei colori per l'intestazione dell'Organizzazione per **Tema chiaro** e **Tema scuro**:

a Fare clic nei campi di testo **Colore sfondo intestazione** e **Colore testo intestazione**.

b Utilizzare lo strumento di selezione colore per definire il colore per ogni voce.

6 Fare clic su **Salva**.

La sezione **Anteprima** viene aggiornata per visualizzare il nuovo logo dell'intestazione.

7 Aggiornare la pagina del servizio per visualizzare le modifiche apportate.

# Conseguenze del download dei file binari del software per i servizi cloud

8

Alcuni VMware Cloud services richiedono l'uso di ulteriori file binari del software che vengono scaricati e installati separatamente dal servizio.

Per scaricare il software aggiuntivo, fare clic su **Scarica** nel menu console di Cloud Services. Questa opzione è disponibile per i seguenti ruoli nell'Organizzazione:

- **Proprietario dell'Organizzazione**;
- **Amministratore dell'Organizzazione** con ruolo di **Installatore software**.
- **Membro dell'Organizzazione** con ruolo di **Installatore software**.

La pagina **Download** è il punto di riferimento per ottenere i file binari del software necessari per tutti i servizi dell'Organizzazione per cui si dispone dell'accesso ai servizi e allo stesso tempo offre un software aggiuntivo da scaricare.

| Se... | Procedere così... |
|---|---|
| Se il link del menu **Download** non è disponibile | Richiedere il ruolo di **Proprietario dell'Organizzazione** o di **Installatore software** dell'Organizzazione.<br>A seconda dell'Organizzazione, è possibile eseguire questa operazione attraverso l'invito di un **Proprietario dell'Organizzazione** o l'invio di una richiesta self-service. Per ulteriori informazioni, vedere Come richiedere ruoli aggiuntivi. |
| Se è possibile aprire la pagina **Download**, ma non è disponibile il servizio per cui è necessario scaricare software aggiuntivo | Richiedere i ruoli per il servizio. Per ulteriori informazioni, vedere Come gestire i ruoli in un'Organizzazione.<br>**Nota** Se si dispone di ruoli di servizio assegnati nell'Organizzazione, ma non si vedono ancora file binari software da scaricare per quel servizio, significa che non ci sono file binari o pacchetti associati al servizio in VMware Cloud Services<br>. |
| Se si è membri di diverse Organizzazioni VMware Cloud Services | Passare all'Organizzazione in cui si dispone di ruoli di Organizzazione e servizio che consentono di accedere ai file binari del software che è necessario scaricare. Per ulteriori informazioni, vedere Come accedere a un'altra Organizzazione. |

Leggi i seguenti argomenti:

# Come scaricare software aggiuntivo per VMware Cloud Services

I file binari e i pacchetti software aggiuntivi da scaricare per i servizi possono essere accessibili dalla pagina **Download** in console di Cloud Services.

### Prerequisiti

Per scaricare file binari e pacchetti software aggiuntivi, è necessario:

- disporre di un ruolo di **Proprietario dell'Organizzazione** o dell'autorizzazione **Installatore software** se si è un **Amministratore dell'Organizzazione** o un **Membro dell'Organizzazione** nell'Organizzazione;
- avere ruoli di servizio assegnati per il servizio per il quale si desidera scaricare software aggiuntivo;
- che l'Organizzazione disponga di una sottoscrizione attiva per il servizio per cui si desidera scaricare un software aggiuntivo.

### Procedura

1. Accedere a console di Cloud Services.
2. Nel menu principale, fare clic su **Download**.

   Si apre la pagina **Esplora prodotti**. Mostra un elenco dei servizi a cui è possibile accedere e che allo stesso tempo dispongono di software aggiuntivo per il download.
3. Per visualizzare i file binari del software per un servizio, fare clic sul nome del servizio.

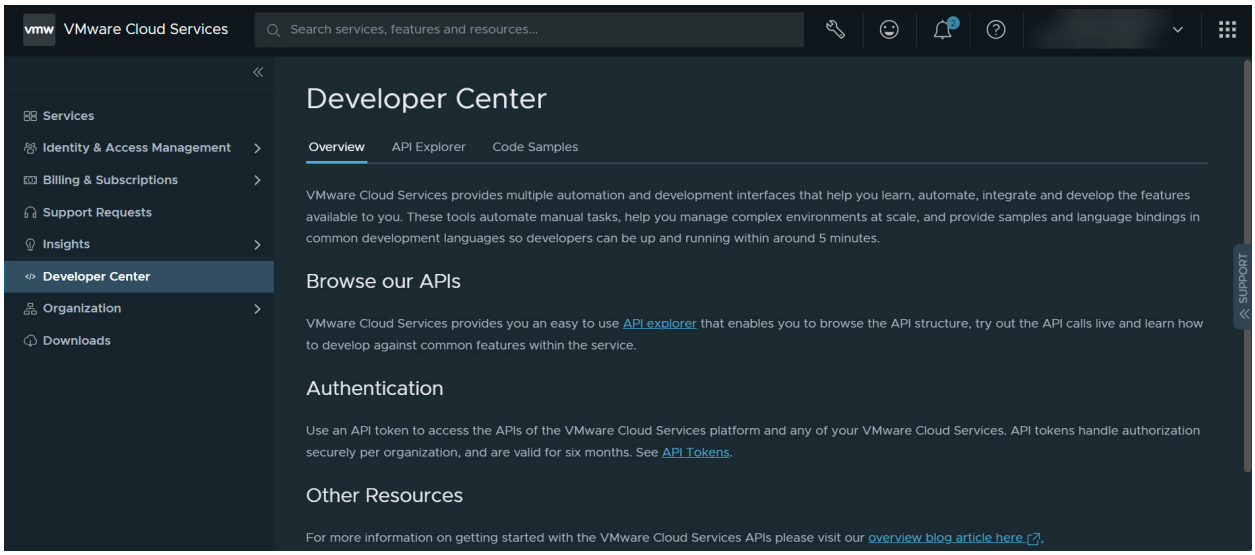
   Nel riquadro a destra di **Esplora prodotti** sono visualizzati i file binari di download associati al servizio selezionato.
4. Esplorare i download di software disponibili:
   a. Fare clic su **Ulteriori informazioni** per visualizzare i dettagli di un file binario software specifico.
   b. Fare clic su **Scarica** per scaricare il file binario del software nella macchina locale.

# Come si utilizza il Centro sviluppatori in VMware Cloud Services

9

Il **Centro sviluppatori** in VMware Cloud Services fornisce interfacce API che consentono di automatizzare, integrare e sviluppare le funzionalità disponibili in console di Cloud Services.

È possibile accedere a **Centro sviluppatori** dal menu principale in console di Cloud Services. Per utilizzare **Centro sviluppatori**, è necessario disporre del ruolo **Proprietario dell'Organizzazione**.




La pagina **Esplora API** nel **Centro sviluppatori** consente di interagire con le API disponibili di VMware Cloud Services. Per ulteriori informazioni, vedere Informazioni importanti su Esplora API.

Nella pagina **Esempi di codice** del **Centro sviluppatori**, è possibile sfogliare e scaricare gli esempi compilati dalla community. Utilizzare gli esempi per iniziare con le attività di automazione, gestione o integrazione.

Leggi i seguenti argomenti:

- Informazioni importanti su Esplora API
- Quali API sono disponibili nel Centro sviluppatori?
- Come provare un'API in Centro sviluppatori

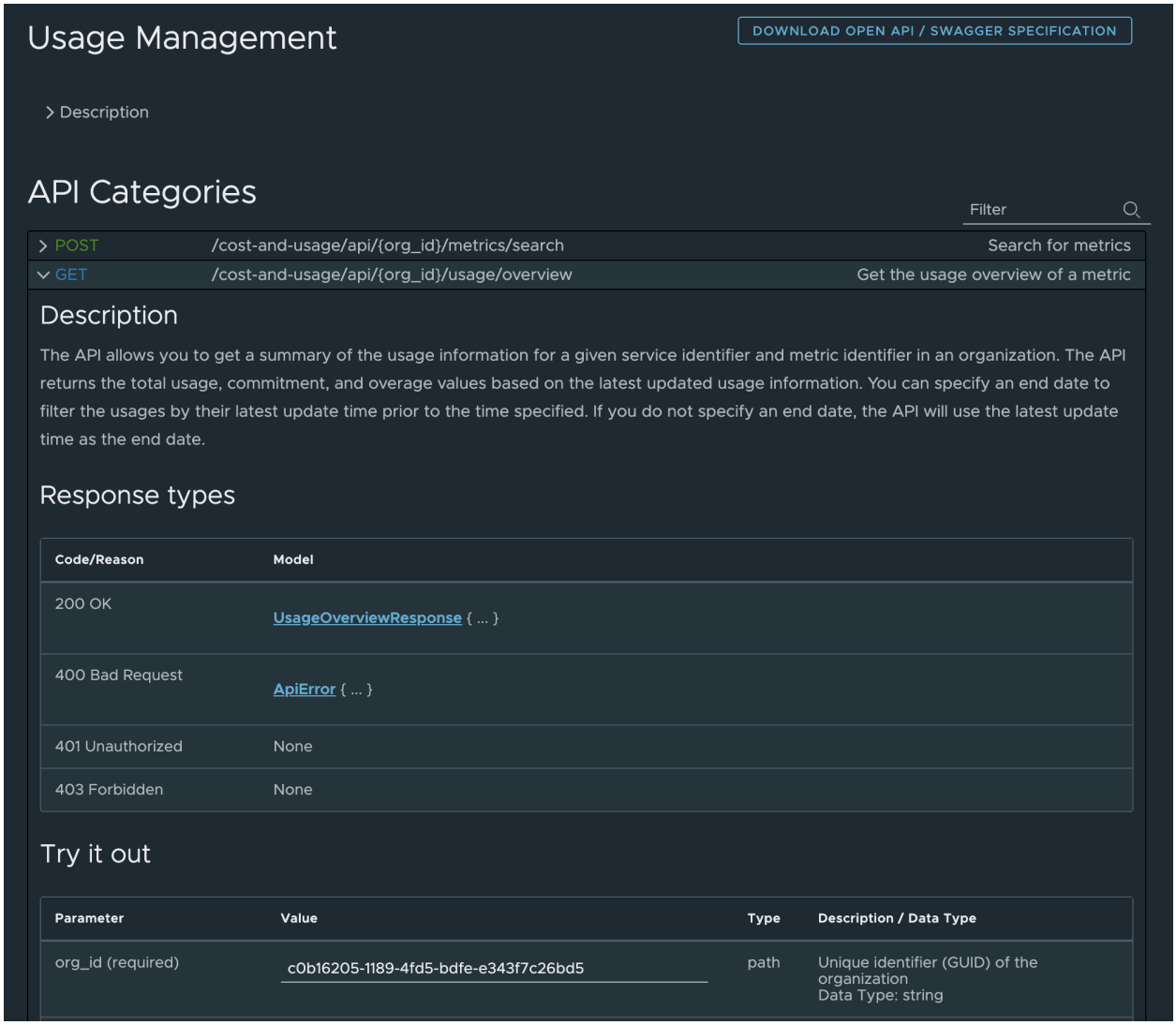
# Informazioni importanti su Esplora API

In qualità di **Proprietario dell'Organizzazione**, è possibile accedere a **Esplora API** in console di Cloud Services per individuare tutte le API di VMware Cloud services disponibili nell'Organizzazione.

È possibile:

- Richiamare un'API direttamente da console di Cloud Services.
- Sfogliare la struttura dell'API.
- Provare le chiamate API in tempo reale e scoprire come sviluppare le funzionalità più comuni all'interno del servizio.

Per iniziare a interagire con le API, accedere a console di Cloud Services e passare a **Centro sviluppatori > Esplora API**.



Come illustrato nella schermata precedente, la pagina **Esplora API** è suddivisa in diverse sezioni che consentono di selezionare le API disponibili, copiare le informazioni sull'ambiente e sul servizio per l'Organizzazione e interagire con le API selezionate.

**API disponibili**

La sezione **API disponibili** della pagina **Esplora API** consente di sfogliare le API nell'ambiente dell'Organizzazione. Fare clic su un collegamento qualsiasi dell'API sul lato sinistro della pagina per visualizzare:

- Informazioni su API specifiche nella rispettiva categoria.
- Elenco dei modelli di oggetti/strutture di dati che potrebbero essere restituiti come parte di qualsiasi API mostrata nella categoria selezionata. L'elenco include anche i dettagli di quello che è possibile trovare nella risposta a una chiamata API.

Per ulteriori informazioni sulle categorie di API, vedere Quali API sono disponibili nel Centro sviluppatori?.

**Ambiente**

La sezione **Ambiente** della pagina **Esplora API** consente di visualizzare e copiare i parametri comunemente richiesti in alcune API, ad esempio:

- **Nome Organizzazione**: nome dell'organizzazione a cui è stato effettuato l'accesso.
- **ID Organizzazione**: ID dell'organizzazione a cui è stato effettuato l'accesso.
- **Token di autenticazione**: combinato con il token di connessione, può essere utilizzato nell'intestazione di autenticazione della chiamata API.
- **Servizio**: quando si seleziona un servizio nel menu a discesa e si fa clic sull'icona Copia, viene copiato l'ID del servizio selezionato.

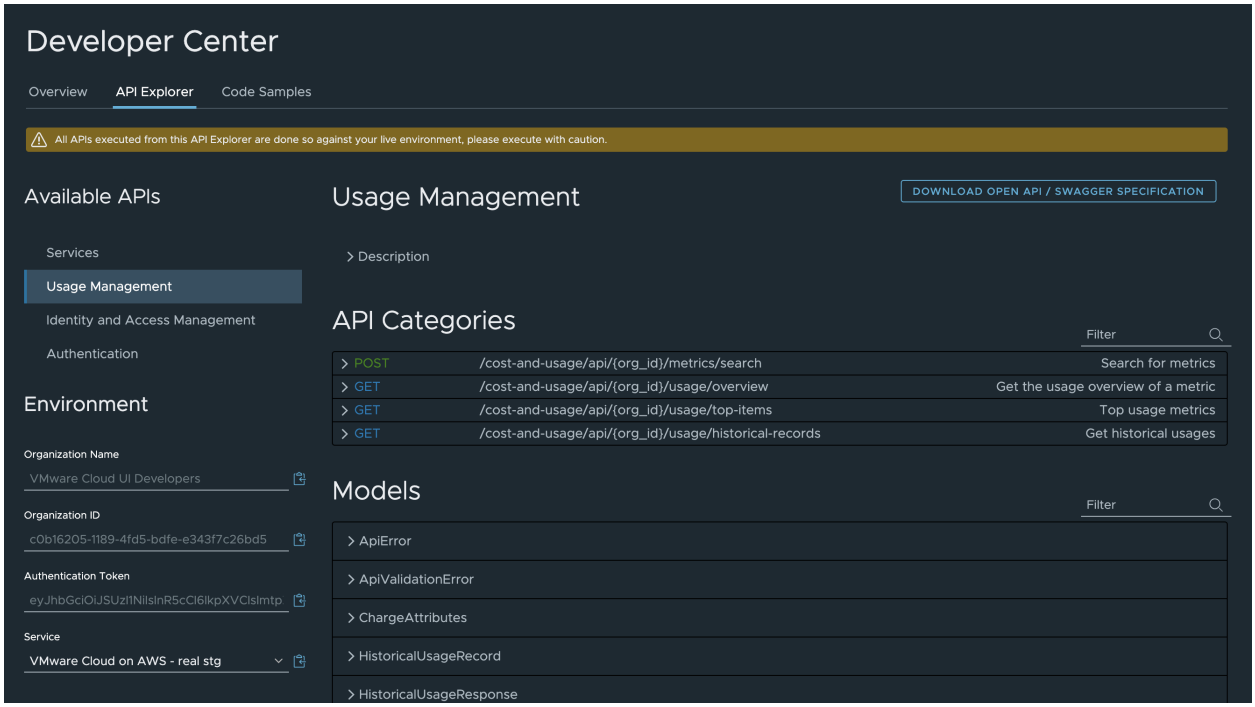
**Informazioni sul servizio**

La sezione **Informazioni sul servizio** viene visualizzata quando si seleziona un'API nell'elenco **API**. Consente di visualizzare e copiare l'URL di base da utilizzare quando le API vengono richiamate da una determinata categoria di API.

# Quali API sono disponibili nel Centro sviluppatori?

In qualità di utente del **Centro sviluppatori**, è possibile interagire con le API di VMware Cloud Services disponibili aprendo la pagina **Centro sviluppatori > Esplora API** in console di Cloud Services.

Le API elencate in questa pagina fungono da punto di autenticazione e gestione principale per le Organizzazioni e gli utenti dell'Organizzazione in VMware Cloud Services. Ogni collegamento nel menu **API disponibili** rappresenta una categoria o un gruppo di API specifici.




| Categoria API | Descrizione |
|---|---|
| **Servizi** | Contiene l'elenco delle API di tutti i servizi dell'organizzazione con i relativi nomi visualizzati e icone. |
| **Gestione utilizzo** | Questo gruppo di API consente di trovare i dati sull'utilizzo corrente e cronologico nell'Organizzazione, inclusa la ricerca in base al tipo e alla regione.<br>È possibile trovare la documentazione dettagliata dell'API Gestione utilizzo nel Developer Portal all'indirizzo https://developer.vmware.com/apis/cost-and-usage-management/latest/. |
| **Gestione accessi e identità** | È possibile utilizzare questo gruppo di API per gestire utenti e gruppi nell'Organizzazione.<br>È possibile trovare la documentazione dettagliata dell'API Gestione accessi e identità nel Developer Portal all'indirizzo https://developer.vmware.com/apis/csp/csp-iam/latest/. |
| **Autenticazione** | È possibile utilizzare le API di questo gruppo quando si desidera automatizzare i processi che interagiscono con console di Cloud Services. Prima di connettersi ad altre API, è necessario eseguire l'autenticazione con la console di Cloud Services. A tale scopo, creare prima un token API. Per i dettagli, vedere Come generare i token API. |

# Come provare un'API in Centro sviluppatori

È possibile provare qualsiasi API disponibile nell'Organizzazione direttamente nella pagina **Esplora API** in console di Cloud Services.

### Prerequisiti

È necessario disporre del ruolo di **Proprietario dell'Organizzazione** all'interno dell'Organizzazione.

### Procedura

1 Accedere all'Organizzazione in console di Cloud Services.

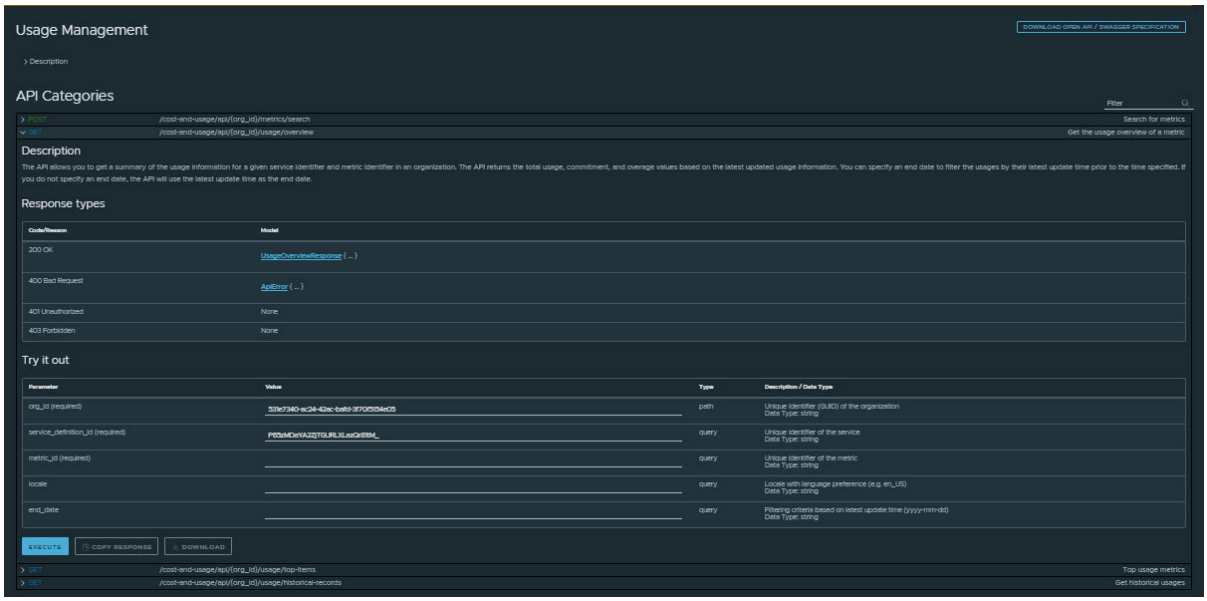
2 Passare a **Centro sviluppatori > Esplora API**.

3 Nel menu **API disponibili** nella pagina **Esplora API**, selezionare una categoria di API.

La pagina viene aggiornata per visualizzare tutte le API disponibili nella categoria selezionata.

4 Utilizzare l'icona a forma di freccia per espandere il contenuto di un'API.

5 Scorrere verso il basso fino alla sezione **Prova**.




6 Per creare una chiamata API, compilare le proprietà obbligatorie.

Se possibile, le proprietà vengono precompilate in base ai dettagli dell'ambiente mostrati sul lato destro della pagina.

Quando si creano o si utilizzano integrazioni API o chiamate server in locale, è possibile utilizzare frammenti di esempi delle specifiche dell'API. Un modo semplice per farlo consiste nel fare clic sul pulsante **Scarica le specifiche Open API/Swagger** disponibile nella parte superiore e inferiore della pagina di **Esplora API**. Il file delle specifiche contiene chiamate di esempio e le risposte previste.

7 Fare clic su **Esegui**.

**Nota** Tutte le chiamate API effettuate da **Esplora API** vengono eseguite nell'ambiente in tempo reale. Prestare sempre attenzione quando si utilizza la funzionalità **Prova**.

**Risultati**

Quando si esegue la chiamata API, la pagina viene aggiornata per visualizzare la risposta sotto la sezione **Prova** della pagina **Esplora API**. È possibile interagire con la risposta del modello, visualizzare il payload in formato di testo, copiare o scaricare la risposta.

## Esempio:

In questo esempio, verrà utilizzata un'API della categoria Gestione accessi e identità per ottenere informazioni sull'utente **Utente principale**, ovvero l'utente attualmente connesso all'organizzazione.

1 Aprire **Esplora API**.

2 Nell'elenco **API disponibili**, selezionare **Gestione accessi e identità**.

3 Nell'elenco di **Categorie API** visualizzato, fare clic su **Utente principale**.

4 Fare clic su `GET /am/api/loggedin/user`.

5 Fare clic su **Esegui**.

La risposta alla chiamata API creata viene visualizzata nella sezione **Risposta** della pagina, che restituisce le informazioni utente utilizzate per accedere all'Organizzazione.

# Gestione identità e accessi

10

In qualità di utente **Proprietario dell'Organizzazione**, si controlla l'accesso dei gruppi e degli utenti all'Organizzazione e alle risorse.

Leggi i seguenti argomenti:

- Come gestire ruoli e autorizzazioni
- Come gestire gli utenti nell'Organizzazione
- Come utilizzare gruppi
- Come impostare i criteri di autenticazione nell'Organizzazione
- Che cos'è la federazione aziendale e come funziona con VMware Cloud Services?
- Che cos'è la governance e l'amministrazione delle identità, e come funzionano con VMware Cloud Services?
- Come eseguire l'autenticazione delle applicazioni con OAuth 2.0
- Come funziona il controllo dei registri eventi in VMware Cloud Services
- Come creare una notifica di pre-accesso NIST in VMware Cloud Services
- Come utilizzare il dashboard dei dettagli
- Elementi coinvolti nell'utilizzo dei progetti nella console di Cloud Services

## Come gestire ruoli e autorizzazioni

In qualità di utente **Proprietario dell'Organizzazione**, è possibile concedere l'accesso in base al ruolo a utenti VMware Cloud Services quando li si invita a partecipare all'Organizzazione.

È possibile visualizzare e gestire i ruoli utente nell'Organizzazione dal menu **Gestione accessi e identità > Utenti attivi** in console di Cloud Services.

### Ruoli e permessi dell'organizzazione

L'accesso alle risorse di un'Organizzazione è determinato dal ruolo assegnato a ciascun utente nell'Organizzazione. Per ogni utente possono essere assegnati uno o più dei seguenti ruoli in un'Organizzazione:

- **Proprietario dell'Organizzazione**

- **Membro dell'Organizzazione**
- **Amministratore dell'Organizzazione**

Per informazioni sui permessi di ciascun ruolo dell'Organizzazione, fare riferimento a Quali ruoli dell'Organizzazione sono disponibili in VMware Cloud Services?.

**Ruoli e permessi del servizio**

VMware Cloud services include un set predefinito di ruoli di servizio che possono essere assegnati agli utenti dell'Organizzazione. Gli utenti **Proprietario dell'Organizzazione** concedono agli altri utenti dell'Organizzazione l'accesso ai servizi cloud in base ai ruoli forniti da ciascun servizio cloud. Per ulteriori informazioni sui ruoli di servizio integrati, fare riferimento alla documentazione del servizio VMware Cloud pertinente.

# Quali ruoli dell'Organizzazione sono disponibili in VMware Cloud Services?

Gli utenti di VMware Cloud Services possono avere uno dei seguenti ruoli in qualsiasi Organizzazione: **Membro dell'Organizzazione**, **Amministratore dell'Organizzazione** o **Proprietario dell'Organizzazione**.

## Ruoli e permessi dell'organizzazione

Il livello di autorizzazioni per ogni Organizzazione varia:

- Il ruolo **Proprietario Organizzazione** dispone dell'accesso amministrativo completo a tutte le risorse dell'Organizzazione. Gli utenti **Proprietario Organizzazione** possono anche assegnare automaticamente ruoli agli stessi.
- Il ruolo di **Amministratore dell'Organizzazione** dispone di accesso amministrativo completo. Gli utenti con il ruolo **Amministratore dell'Organizzazione** possono assegnare ruoli dei servizi a qualsiasi ruolo dell'Organizzazione, ma possono gestire solo utenti, gruppi e app OAuth che dispongono di ruoli con autorizzazioni amministrative identiche o inferiori.

  Ad esempio, un utente con il ruolo **Amministratore dell'Organizzazione** può concedere o gestire l'accesso per altri utenti e gruppi che hanno il ruolo **Membro dell'Organizzazione** o **Amministratore dell'Organizzazione** nell'Organizzazione, ma non può gestire utenti, gruppi o risorse a cui è assegnato il ruolo **Proprietario dell'Organizzazione**.
- Il ruolo **Membro dell'Organizzazione** dispone dell'accesso in sola lettura alle risorse dell'Organizzazione.

Ecco cosa occorre sapere sulle autorizzazioni dei tre ruoli dell'Organizzazione in VMware Cloud Services. Se a un utente vengono assegnati ruoli in conflitto tra loro, viene applicato il ruolo che dispone di autorizzazioni maggiori.

| Autorizzazione | Proprietario dell'organizzazione | Amministratore dell'Organizzazione | Membro dell'organizzazione |
|---|---|---|---|
| Appartenere a una o più Organizzazioni | ☑ | ☑ | ☑ |
| Accedere a una delle altre Organizzazioni | ☑ | ☑ | ☑ |
| Specificare l'Organizzazione che viene visualizzata quando si esegue l'accesso. | ☑ | ☑ | ☑ |
| Visualizzare e modificare le impostazioni dell'Organizzazione. | ☑ | ☑ Solo visualizzazione. | ☑ Solo visualizzazione. |
| Aggiungi/rimuovi utenti nell'Organizzazione | ☑ | ☑ Solo gli utenti che dispongono del ruolo **Membro dell'Organizzazione** o **Amministratore dell'Organizzazione**. | |
| Gestire accesso e ruoli a livello di servizio degli utenti dell'Organizzazione. | ☑ | ☑ | |
| Gestire e visualizzare metodi di pagamento e fatturazione. | ☑ | ☑ Quando la casella di controllo **Fatturazione in sola lettura** è selezionata, questo ruolo fornisce l'accesso in sola lettura alle informazioni relative alla fatturazione e l'opzione per generare i report su utilizzo e consumi. | ☑ Quando la casella di controllo **Fatturazione in sola lettura** è selezionata, questo ruolo fornisce l'accesso in sola lettura alle informazioni relative alla fatturazione e l'opzione per generare i report su utilizzo e consumi. |
| Inviare e gestire ticket di supporto. | ☑ | ☑ Quando la casella di controllo **Assistenza utente** è selezionata. | ☑ Quando la casella di controllo **Assistenza utente** è selezionata. |
| Eseguire query alle API del servizio cloud sull'utilizzo e i dati dei clienti.<br>Questa autorizzazione è disponibile solo per profili cliente specifici. | ☑ | ☑ Quando la casella di controllo **Provider di servizi gestiti** è selezionata. | ☑ Quando la casella di controllo **Provider di servizi gestiti** è selezionata. |
| Creare e gestire le app OAuth per autorizzare le app di terze parti ad accedere alle risorse protette. | ☑ | ☑ Solo per le app OAuth create dagli utenti dell'Organizzazione. | ☑ Quando la casella di controllo **Sviluppatore** è selezionata. |

| Autorizzazione | Proprietario dell'organizzazione | Amministratore dell'Organizzazione | Membro dell'organizzazione |
|---|---|---|---|
| Accedere a tutti i dati di controllo per l'Organizzazione nell'istanza di servizio vRealize Log Insight Cloud associata per l'Organizzazione. | ☑ | ☑ Quando la casella di controllo **Revisori del registro di accesso** è selezionata. | ☑ Quando la casella di controllo **Revisori del registro di accesso** è selezionata. |
| Accedere ai link per il download di file binari e pacchetti software aggiuntivi per i servizi cloud. | ☑ | ☑ Quando la casella di controllo **Installatore software** è selezionata. | ☑ Quando la casella di controllo **Installatore software** è selezionata. |
| Creare, modificare e gestire l'accesso ai progetti e alle relative risorse. | ☑ | ☑ Quando la casella di controllo **Amministratore del progetto** è selezionata. | ☑ Quando la casella di controllo **Amministratore del progetto** è selezionata. |

# Come gestire gli utenti nell'Organizzazione

Un utente **Proprietario dell'Organizzazione** gestisce gli accessi utente e stabilisce le autorizzazioni a livello di servizio e di Organizzazione per utenti e gruppi nell'Organizzazione.

È possibile utilizzare il menu **Gestione identità e accessi** in console di Cloud Services per invitare gli utenti dell'Organizzazione, assegnare ruoli a livello di Organizzazione e di servizio, modificare i ruoli utente o rimuovere utenti dall'Organizzazione.

**Nota** L'applicazione delle modifiche ai ruoli utente può richiedere fino a 30 minuti nell'Organizzazione.

Quando inviti utenti nelle tue Organizzazioni, assegni due tipi di accesso basato sui ruoli:

- Consente di accedere a uno o più servizi cloud dell'Organizzazione. Puoi concedere agli utenti l'accesso al servizio assegnando loro uno o più ruoli forniti dal servizio. Per ulteriori informazioni, fare riferimento alla documentazione del servizio cloud VMware pertinente.
- Accesso all'Organizzazione basato sui ruoli. Come utente **Proprietario dell'Organizzazione** con accesso completo o come utente **Membro dell'Organizzazione** con accesso in sola lettura.

L'assegnazione delle autorizzazioni di accesso ai gruppi è più efficiente rispetto all'assegnazione delle stesse autorizzazioni ai singoli utenti uno alla volta. Il **proprietario dell'Organizzazione** stabilisce gli utenti che compongono i tuoi gruppi e quali ruoli e autorizzazioni assegnare loro.

## Come aggiungere utenti all'Organizzazione

In qualità di **Proprietario dell'Organizzazione**, è possibile invitare gli utenti nell'Organizzazione e garantire loro l'accesso ai servizi associati. È inoltre possibile tenere traccia degli inviti inviati.

Gli inviti hanno una validità di sette giorni. Se è stato inviato un invito per errore, è possibile revocarlo.

Gli utenti invitati possono ricoprire diversi ruoli:

- Un ruolo all'interno dell'Organizzazione (**Proprietario dell'Organizzazione** o **Membro dell'Organizzazione**). Per visualizzare le autorizzazioni assegnate a ciascuno di questi ruoli, vedere Quali ruoli dell'Organizzazione sono disponibili in VMware Cloud Services?.
- Un ruolo nel servizio cloud a cui si sta invitando l'utente. Ogni servizio cloud ha i propri ruoli specifici. Per ulteriori informazioni, fare riferimento alla documentazione pertinente di VMware Cloud services.
- In base al profilo del cliente, è inoltre possibile visualizzare il ruolo Provider di servizi gestiti che consente agli utenti di eseguire query nelle API del servizio cloud per l'utilizzo e i dati del cliente. Se si assegna questo ruolo agli utenti di un'Organizzazione tenant, questi potranno accedere a tutti i dati all'interno dell'Organizzazione.

Procedura

1. Nella barra degli strumenti di console di Cloud Services, fare clic sull'icona della **VMware Cloud Services** e selezionare **Gestione identità e accessi > Utenti attivi**.
2. Fare clic su **Aggiungi utenti**.
3. Nella pagina **Aggiungi nuovi utenti**, immettere le informazioni seguenti:
   a. Nella casella di testo **Utenti** immettere l'indirizzo e-mail dell'utente che si desidera aggiungere all'Organizzazione.

      È possibile aggiungere più di un utente alla volta separando gli indirizzi e-mail con una virgola o immettendo ciascun indirizzo e-mail in una riga separata.

   b. Nella sezione **Assegna ruoli Organizzazione**, assegnare il ruolo che l'utente avrà nell'Organizzazione.

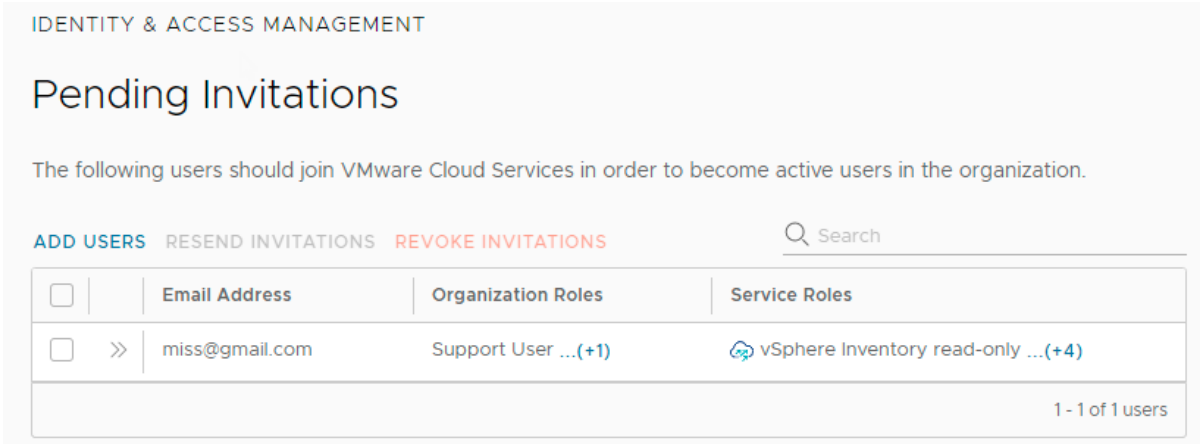
      Il ruolo del **Proprietario dell'Organizzazione** dispone dell'accesso amministrativo completo. Se si seleziona il ruolo di **Membro dell'Organizzazione** per il nuovo utente, si consiglia di aggiungere un accesso aggiuntivo selezionando uno o più ruoli nella sezione **Ruoli aggiuntivi**.

   c. Per assegnare i ruoli di servizio utente nell'Organizzazione, fare clic su **Aggiungi accesso al servizio** e utilizzare i menu a discesa per effettuare una selezione.

   d. Fare di nuovo clic su **Aggiungi accesso al servizio**, per consentire all'utente di accedere a un altro servizio.

4 Fare clic su **Aggiungi** per inviare un invito all'utente.

Gli inviti inviati sono validi per sette giorni. È possibile visualizzare lo stato dell'invito nella scheda **Gestione identità e accessi > Inviti in sospeso**




5 Se è stato inviato un invito per errore, è possibile revocarlo. Selezionare la casella di controllo accanto all'invito e fare clic su **Revoca inviti**.

Il link di attivazione nell'e-mail viene revocato e la persona a cui è stata inviata l'email non potrà accedere al servizio.

## Come rimuovere gli utenti dall'Organizzazione

Il **Proprietario dell'Organizzazione**, può rimuovere utenti dall'Organizzazione. Gli utenti che sono stati rimossi non potranno accedere all'Organizzazione e ai relativi servizi.

Procedura

1 Aprire console di Cloud Services e selezionare **Gestione identità e accessi > Utenti attivi**.

2 Selezionare uno o più utenti e fare clic su **Rimuovi utenti**.

3 Fare clic su **Rimuovi** per rimuovere definitivamente l'utente dall'Organizzazione.

## Come modificare i ruoli utente

Quando gli utenti si uniscono all'Organizzazione, ricevono l'accesso ai ruoli dell'Organizzazione e del servizio concesso direttamente da un **Proprietario dell'Organizzazione** o lo acquisiscono in quanto membri di gruppi. In qualità di **Proprietario dell'Organizzazione**, è possibile visualizzare e modificare i ruoli utente di console di Cloud Services.

Ecco cosa è necessario sapere sulla modifica dei ruoli degli utenti.

- Gli utenti possono avere una combinazione di ruoli: i ruoli assegnati a loro direttamente e i ruoli acquisiti da un gruppo. Ad esempio, l'assegnazione diretta del ruolo di utente di assistenza e alcuni ruoli acquisiti dal gruppo, come sviluppatore e amministratore di VMware Cloud on AWS.

- Quando a un utente vengono assegnati ruoli in conflitto tra loro, questo riceve il ruolo che dispone di autorizzazioni maggiori. Ad esempio, se a un utente viene assegnato un ruolo di sola lettura e un ruolo di amministratore, riceve il ruolo di amministratore.

Procedura

1. Nella barra degli strumenti di console di Cloud Services, fare clic sull'icona della **VMware Cloud Services** e selezionare **Gestione identità e accessi > Utenti attivi**.
2. Fare clic sull'icona delle due frecce ( » ) accanto al nome di un utente per visualizzare i relativi ruoli e se fanno parte dei gruppi.

   Le modifiche apportate al ruolo dell'utente potrebbero sovrascrivere i ruoli assegnati al gruppo.
3. Selezionare la casella di controllo accanto a un utente e fare clic su **Modifica ruoli**.
4. Modificare i ruoli dell'Organizzazione e i ruoli di servizio dell'utente in base alle necessità.
5. Fare clic su **Salva**.

# Come utilizzare gruppi

L'assegnazione di ruoli ai gruppi è più efficiente rispetto all'assegnazione delle stesse autorizzazioni a singoli utenti una alla volta. In qualità di utente **Proprietario dell'Organizzazione**, è possibile creare gruppi e determinare i membri che costituiscono i gruppi e i ruoli a essi assegnati.

È inoltre possibile modificare i gruppi dopo che sono stati creati o aggiunti. Mano a mano che l'Organizzazione cresce o si modifica, i membri vengono aggiunti o rimossi dai gruppi.

In VMware Cloud services sono disponibili due tipi di gruppi: i gruppi personalizzati e i gruppi aziendali. I gruppi personalizzati possono essere condivisi con altre Organizzazioni. I gruppi aziendali possono essere nidificati all'interno di gruppi personalizzati.

### Gruppi personalizzati

È possibile creare gruppi personalizzati immettendo un nome e una descrizione, aggiungendo membri e quindi assegnando ruoli per l'Organizzazione e le relative risorse. Ad esempio, è possibile creare un gruppo personalizzato e assegnargli un ruolo di **membro dell'Organizzazione** e un ruolo di supporto, nonché l'accesso in sola lettura a servizi specifici dell'Organizzazione. I gruppi personalizzati possono anche includere gruppi aziendali.

Per i gruppi personalizzati, è possibile modificare il nome e la descrizione, aggiungere o rimuovere membri e modificare l'assegnazione di ruolo del gruppo.

### Gruppi condivisi

Quando si crea un gruppo personalizzato, è possibile decidere se renderlo condiviso o meno. Il **Proprietario dell'Organizzazione** può associare il gruppo condiviso ad altre Organizzazioni in modo da consentire l'assegnazione di ruoli ai membri del gruppo condiviso nelle Organizzazioni associate e l'accesso ai servizi senza richiedere l'invito da parte dei **proprietari dell'Organizzazione**.

I ruoli dei servizi assegnati ai gruppi condivisi sono specifici dell'Organizzazione. I **proprietari dell'Organizzazione** associate importano il gruppo condiviso e assegnano ruoli al gruppo all'interno delle proprie Organizzazioni. Per importare un gruppo condiviso, i **proprietari dell'Organizzazione** devono conoscere il nome o l'ID del gruppo.

Solo il **Proprietario dell'Organizzazione** di origine, ovvero l'Organizzazione in cui è stato creato il gruppo condiviso, può modificare i membri del gruppo o eliminarlo. La rimozione di un gruppo condiviso da un'Organizzazione associata non lo elimina, quindi il gruppo può essere aggiunto nuovamente in un secondo momento. Al seguente link è possibile vedere come Come gestire gruppi condivisi.

### Gruppi aziendali

I gruppi aziendali sono gruppi sincronizzati dal dominio aziendale. Dopo aver federato il dominio aziendale con VMware Cloud services, è possibile utilizzare i gruppi aziendali nell'Organizzazione. Al seguente link è possibile vedere come Come assegnare ruoli ai gruppi aziendali.

Per i gruppi aziendali è possibile modificare solo l'assegnazione del ruolo del gruppo. Non è possibile aggiungere o rimuovere membri da gruppi aziendali in VMware Cloud services, ma è possibile assegnare loro ruoli per l'Organizzazione e le relative risorse e aggiungerli ai gruppi personalizzati.

### Gruppi nidificati

L'aggiunta di un gruppo a un altro gruppo è denominata nidificazione. Ecco cosa è necessario sapere sui gruppi nidificati:

- È possibile nidificare un gruppo aziendale in un gruppo personalizzato.
- I gruppi nidificati possono contenere una combinazione di ruoli: ruoli assegnati direttamente al gruppo aziendale e ruoli assegnati tramite il gruppo personalizzato.
- È possibile modificare i ruoli di un gruppo aziendale nidificato o aggiungere ruoli aggiuntivi, ma non è possibile rimuovere i ruoli ereditati dal gruppo personalizzato.
- Non è possibile nidificare un gruppo personalizzato in un altro gruppo personalizzato.

In qualità di **Proprietario dell'Organizzazione**, è inoltre possibile modificare i gruppi dopo che sono stati creati o aggiunti. Per i gruppi personalizzati, è possibile modificare il nome e la descrizione, aggiungere o rimuovere membri e modificare l'assegnazione di ruolo del gruppo. Per i gruppi aziendali è possibile modificare solo l'assegnazione del ruolo del gruppo.

In qualità di **Proprietario dell'Organizzazione**, è possibile creare gruppi, gestirli e, mano a mano che l'Organizzazione cresce e si modifica, aggiungere o rimuovere membri dai gruppi.

**Nota** Quando si apportano modifiche ai gruppi possono essere necessari fino a 30 minuti affinché le modifiche abbiano effetto nell'Organizzazione.

## Come creare un nuovo gruppo

In qualità di utente **Proprietario dell'Organizzazione**, è possibile creare nuovi gruppi nell'Organizzazione e assegnare i ruoli di Organizzazione e di servizio del gruppo. Questi gruppi sono denominati gruppi personalizzati.

Per informazioni sulle autorizzazioni assegnate a ogni ruolo dell'Organizzazione, vedere Come gestire ruoli e autorizzazioni. Per informazioni sulle autorizzazioni assegnate con i ruoli di servizio, vedere la documentazione per il servizio.

Procedura

1 Nella console di Cloud Services, selezionare **Gestione identità e accessi > Gruppi**.

2 Fare clic su **Aggiungi gruppi**.

3 Selezionare **Crea un nuovo gruppo** e fare clic su **Continua**.

4 Immettere un nome e una descrizione per il gruppo.

5 Se si desidera condividere il gruppo con altre Organizzazioni, fare clic su **Aggiungi Organizzazioni**.

   a Selezionare le Organizzazioni con cui si desidera condividere il gruppo: immettere l'ID dell'Organizzazione per ogni Organizzazione o effettuare una selezione dall'elenco delle Organizzazioni visualizzato nella finestra a comparsa.

   b Fai clic su **Aggiungi**.

   **Nota** Quando si crea un gruppo personalizzato condiviso, i **proprietari dell'Organizzazione** delle Organizzazioni associate possono assegnare ruoli al gruppo nella loro Organizzazione.

6 Fare clic su **Aggiungi membri** per aggiungere membri al gruppo, quindi fare clic su **Aggiungi**.

   I membri possono essere gruppi aziendali e utenti. È possibile scegliere di ignorare questo passaggio e aggiungere membri dopo aver creato il gruppo.

7 Assegnare al gruppo l'accesso all'Organizzazione selezionando un ruolo dell'Organizzazione.

8 Assegnare al gruppo l'accesso ai servizi facendo clic su **Aggiungi accesso al servizio** e selezionando un servizio e i ruoli che si desidera assegnare al gruppo per questo servizio.

9 Per aggiungere l'accesso a un servizio aggiuntivo, fare clic su **Aggiungi accesso al servizio**.

10 Fare clic su **Crea**.

   Il gruppo viene aggiunto all'elenco di gruppi nella pagina **Gestione identità e accessi**.

# Come assegnare ruoli ai gruppi aziendali

Se il dominio è federato con VMware Cloud services, è possibile selezionare i gruppi dal dominio di origine aziendale e assegnare loro ruoli nell'Organizzazione. Questi gruppi sono denominati gruppi aziendali.

I gruppi aziendali sono gruppi sincronizzati dal dominio aziendale. È possibile assegnare ruoli a più di un gruppo aziendale alla volta e visualizzare i membri in un gruppo selezionato.

I membri del gruppo assegnato possono ricoprire diversi ruoli:

- Ruolo Organizzazione: un ruolo all'interno dell'Organizzazione (**Proprietario dell'Organizzazione** o **Membro dell'Organizzazione**). Per visualizzare i privilegi assegnati a ciascuno di questi ruoli, vedere Come gestire ruoli e autorizzazioni.
- Ruolo di servizio: un ruolo all'interno di uno o più VMware Cloud services. Ogni servizio cloud ha i propri ruoli specifici. Per ulteriori informazioni, fare riferimento alla documentazione pertinente del servizio VMware Cloud.
- In base al profilo del cliente, è inoltre possibile visualizzare il ruolo Provider di servizi gestiti che consente agli utenti di eseguire query nelle API del servizio cloud per l'utilizzo e i dati del cliente. Se si assegna questo ruolo ai membri di un'Organizzazione tenant, questi potranno accedere a tutti i dati all'interno dell'Organizzazione.

Procedura

1. Dal menu principale di console di Cloud Services, selezionare **Gestione identità e accessi > Gruppi**.
2. Fare clic su **Seleziona gruppi dal dominio di origine**, quindi su **Continua**.
3. Cercare i gruppi aziendali a cui si desidera assegnare i ruoli.
4. Assegnare al gruppo un ruolo dell'Organizzazione.

   Fare riferimento al link precedente per visualizzare le autorizzazioni di ciascun ruolo.
5. Selezionare un servizio, quindi assegnare al gruppo uno o più ruoli nel servizio.

   Quando si seleziona un servizio, viene visualizzato il ruolo predefinito del servizio. Fare clic sul ruolo per selezionarne uno diverso.
6. Per concedere al gruppo l'accesso a un altro servizio, fare clic su **Aggiungi accesso al servizio** e assegnare un ruolo.
7. Fai clic su **Aggiungi**.

   Per inviare un'e-mail agli utenti con il ruolo di **Membro dell'Organizzazione** selezionare la casella di controllo. Agli utenti con ruoli di **Proprietario dell'Organizzazione** e utente di supporto viene inviata automaticamente un'e-mail.

# Come gestire gruppi condivisi

Quando il **Proprietario dell'Organizzazione** crea un gruppo personalizzato e lo associa ad altre Organizzazioni, il gruppo diventa condiviso. I **proprietari dell'Organizzazione** di destinazione ricevono un'e-mail dal **Proprietario dell'Organizzazione** di origine contenente l'invito a importare il gruppo condiviso e assegnare ruoli del servizio.

Il **Proprietario dell'Organizzazione** che riceve l'invito a importare un gruppo condiviso creato in un'altra Organizzazione assegna ruoli di servizio per il gruppo condiviso durante l'importazione nell'Organizzazione.

Puoi distinguere i gruppi condivisi importati dai gruppi condivisi creati nella tua Organizzazione in base alla loro etichetta: 

.

Gli utenti del gruppo condiviso importato possono accedere ai servizi dell'Organizzazione in base ai ruoli che sono stati assegnati al gruppo. In questo modo è possibile accedere ai servizi tra più Organizzazioni a livello di gruppo e non è più necessario inviare inviti individuali a ciascun utente.

**Importante** I gruppi condivisi importati da altre Organizzazioni non possono essere modificati. È possibile modificare i ruoli assegnati al gruppo condiviso o rimuovere il gruppo dall'Organizzazione.

### Prerequisiti

È necessario conoscere il nome o l'ID dell'Organizzazione di origine che ha creato il gruppo condiviso che si desidera aggiungere.

### Procedura

1. Nella console di Cloud Services, selezionare **Gestione identità e accessi > Gruppi**.
2. Fare clic su **Aggiungi Gruppi**.
3. Selezionare **Importa gruppi da altre organizzazioni** quindi fare clic su **Continua**.
4. Nel menu a discesa, selezionare l'Organizzazione di origine che ha creato il gruppo condiviso.
5. Selezionare il gruppo condiviso che si desidera importare.
6. Selezionare un ruolo dell'Organizzazione per assegnare l'accesso al gruppo selezionato alla propria Organizzazione.
7. Fare clic su **Aggiungi accesso al servizio** per assegnare ruoli di servizio al gruppo selezionato:
   a. Utilizzare il menu a discesa per selezionare il servizio della propria Organizzazione a cui si desidera che il gruppo condiviso acceda.
   b. Fare clic sulla casella dei ruoli e selezionare i ruoli di servizio da assegnare al gruppo condiviso.
   c. Definire il periodo di tempo per l'accesso. È possibile scegliere una data di fine o fornire un accesso senza scadenza.

8 Per aggiungere l'accesso a un servizio aggiuntivo, fare clic su **Aggiungi accesso al servizio** e ripetere i passaggi da 7.a a 7.c.

9 Lasciare l'opzione **Invia e-mail a tutti gli utenti invitati per informarli dell'assegnazione di questo ruolo** selezionata se si desidera che tutti gli utenti del gruppo condiviso ricevano gli inviti per accedere al servizio.

10 Fare clic su **Importa**.

**Risultati**

Il gruppo condiviso viene aggiunto alla propria Organizzazione come gruppo remoto personalizzato.

# Come impostare i criteri di autenticazione nell'Organizzazione

In qualità di utente **Proprietario dell'Organizzazione** è possibile impostare criteri di autenticazione per l'accesso degli utenti all'Organizzazione di VMware Cloud services, ad esempio l'autenticazione multifattore, le preferenze di autenticazione IP e l'accesso degli utenti a livello di dominio.

È possibile creare e gestire le impostazioni dei criteri di autenticazione per l'Organizzazione dalla pagina **Organizzazione > Criterio di autenticazione** in console di Cloud Services.

**Importante** L'applicazione di un nuovo criterio o di una modifica può richiedere fino a 30 minuti.

Per l'Organizzazione sono configurati diversi criteri di autenticazione, l'accesso di ogni utente viene convalidato in sequenza rispetto a tutti i criteri. Se un criterio viene violato, all'utente non sarà consentito accedere all'Organizzazione.

## Come configurare l'autenticazione multifattore

Quando viene attivata l'autenticazione multifattore (MFA), a tutti gli utenti dell'Organizzazione verrà richiesto di fornire un codice di autenticazione a sei cifre oltre alle credenziali di accesso. Per fornire il codice, devono registrare un dispositivo MFA in VMware Cloud Services. Agli utenti dell'Organizzazione che non forniscono un codice MFA valido verrà negato l'accesso all'Organizzazione.

Se si è **proprietari dell'Organizzazione** di un dominio federato, non si controlla la MFA per la propria Organizzazione. La MFA per i domini federati è configurata da un **Amministratore aziendale** sul fornitore di identità utilizzato dall'azienda. Questa procedura si applica solo ai domini non federati.

**Prerequisiti**

- Si deve disporre del ruolo di **Proprietario dell'Organizzazione** all'interno dell'Organizzazione.

- È necessario aver registrato un dispositivo MFA in VMware Cloud Services in modo da non bloccare l'Organizzazione dopo aver applicato la MFA. Per istruzioni dettagliate, fare riferimento a Come proteggere l'account con l'autenticazione multifattore.

Procedura

1. Accedere a console di Cloud Services e fare clic su **Organizzazione > Criterio di autenticazione**.
2. Nella sezione **Autenticazione multifattore**, fare clic sull'interruttore in modo che il colore del pulsante diventi verde.

Risultati

Ora la MFA è attiva e tutti gli utenti dell'Organizzazione dovranno registrare un dispositivo MFA e fornire un token MFA al momento dell'accesso.

**Nota** L'applicazione del criterio nell'Organizzazione può richiedere fino a 30 minuti.

## Come definire le preferenze di autenticazione IP

In qualità di **Proprietario dell'Organizzazione**, è possibile gestire l'accesso alla propria Organizzazione definendo gli indirizzi IP o intervalli IP per bloccare o consentire l'accesso degli utenti da IP specifici.

A tale scopo, è necessario applicare una preferenza di autenticazione per bloccare o consentire l'accesso degli utenti da un intervallo IP o da un IP specifico. Se la preferenza di autenticazione è definita per un intervallo IP, è possibile impostare eccezioni per IP specifici all'interno dell'intervallo. Ad esempio, se si applica l'autenticazione di blocco a un intervallo IP, è possibile impostare un'eccezione per uno o più IP all'interno di tale intervallo a cui sarà consentito l'accesso a VMware Cloud services.

**Nota** L'indirizzo IP immesso deve seguire la notazione CIDR per gli indirizzi IP IPv4 e IPv6.

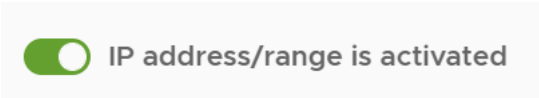
È possibile definire due opzioni di preferenza di autenticazione:

- **Blocca IP**: gli accessi degli utenti all'Organizzazione da intervalli o indirizzi IP specifici sono bloccati.
- **Consenti IP**: gli accessi degli utenti all'Organizzazione da intervalli o indirizzi IP specifici sono consentiti.

Nell'Organizzazione può essere attivata una sola preferenza. È possibile passare da una preferenza all'altra, ma non è possibile attivarle entrambe contemporaneamente.

Per impostare o modificare una preferenza di autenticazione IP nell'Organizzazione, accedere a console di Cloud Services e passare a **Organizzazione > Criterio di autenticazione > Indirizzo/intervallo IP**.

**Nota** L'applicazione delle impostazioni dei criteri nell'Organizzazione può richiedere fino a 30 minuti.

| Per | Procedere così |
| --- | --- |
| Impostare una preferenza di autenticazione IP per l'Organizzazione | 1 Se si imposta una preferenza di autenticazione IP per la prima volta, selezionare un'opzione e fare clic su **Attiva**.<br><br>Viene visualizzata la pagina delle impostazioni del criterio, che indica che l'indirizzo o l'intervallo IP sono stati attivati nell'Organizzazione.<br><br>  <br><br><br>2 Fare clic su **Aggiungi** e digitare un indirizzo o un intervallo IP.<br>3 Fare nuovamente clic su **Aggiungi**.<br><br>L'indirizzo o l'intervallo immesso viene aggiunto all'elenco di indirizzi e intervalli bloccati o consentiti specificati per l'Organizzazione. |
| Aggiungere un'eccezione alla preferenza di autenticazione | È possibile definire regole di eccezione per gli indirizzi IP di un intervallo di IP già specificato nell'elenco di IP consentiti o bloccati.<br>1 Nella sezione **Eccezione** della pagina **Indirizzo/ intervallo IP**, fare clic su **Aggiungi un'eccezione**.<br>2 Nella finestra popup che viene visualizzata, digitare gli indirizzi IP che si desidera aggiungere come eccezioni al criterio di autenticazione nell'Organizzazione.<br><br>Se è stata attivata la preferenza **Consenti IP**, verrà negato l'accesso agli utenti che accedono a VMware Cloud services dagli IP presenti nell'elenco delle eccezioni. Al contrario, se è stata attivata la preferenza **Blocca IP**, verrà consentito l'accesso agli utenti che accedono a VMware Cloud services dagli IP presenti nell'elenco delle eccezioni. |

| Per | Procedere così |
| --- | --- |
| Modificare gli indirizzi IP, intervalli o eccezioni per le preferenze di autenticazione | Dopo aver attivato un criterio di autenticazione IP, è possibile aggiungere IP, intervalli IP ed eccezioni aggiuntive. È inoltre possibile modificare o rimuovere IP e intervalli esistenti dal criterio.<br>■ Per apportare una modifica, selezionare innanzitutto l'indirizzo IP o l'intervallo dall'elenco, quindi procedere con l'azione appropriata. |
| Modificare la preferenza di autenticazione IP | Se si desidera passare dalla preferenza di autenticazione nell'Organizzazione **Blocca IP** a **Consenti IP** o viceversa, è necessario rimuovere gli indirizzi e gli intervalli IP specificati per la preferenza di autenticazione attuale.<br>1 Nella pagina **Indirizzo/intervallo IP**, selezionare tutti gli indirizzi e intervalli IP attualmente definiti.<br>2 Fare clic su **Rimuovi**.<br>3 Fare clic sul link **Modifica** accanto all'opzione Preferenza di autenticazione IP dell'utente.<br>4 Nella finestra popup che viene visualizzata, selezionare la nuova opzione, quindi fare clic su **Salva**.<br>5 Per definire nuovi indirizzi o intervalli IP per l'impostazione del criterio appena selezionato, fare clic su **Aggiungi**. |

### Per errore ho bloccato il mio indirizzo IP e desidero sbloccarlo

Se, per errore, il proprio indirizzo IP è stato aggiunto all'elenco **Blocca IP** dell'Organizzazione, è necessario inviare un ticket di assistenza per poterlo sbloccare. Dal momento che non si può accedere all'Organizzazione e utilizzare il **Centro di assistenza** di console di Cloud Services, è possibile procedere contattando telefonicamente l'assistenza VMware.

### Il blocco dell'indirizzo IP di un utente nell'Organizzazione impedisce loro di accedere ad altre Organizzazioni di cui sono membri?

Se un utente appartiene a più Organizzazioni e il criterio basato su IP viene applicato in una di queste Organizzazioni, non gli è consentito l'accesso in quella particolare Organizzazione. Ha quindi la possibilità di passare a un'Organizzazione diversa al momento dell'accesso.

## Come gestire l'accesso degli utenti a livello di dominio

In qualità di utente **Proprietario dell'Organizzazione**, è possibile determinare i domini a cui è consentito accedere all'Organizzazione VMware Cloud Services.

Quando viene attivato il criterio di autenticazione Dominio di origine, solo gli utenti dei domini specificati possono accedere all'Organizzazione. L'accesso da tutti gli altri domini viene bloccato anche se i gruppi e gli utenti vengono aggiunti o invitati nell'Organizzazione.

#### Procedura

1 Accedere a console di Cloud Services e passare a **Organizzazione > Criterio di autenticazione > Dominio di origine**.

2 Per attivare il criterio, fare clic sul dispositivo di scorrimento e modificarne la posizione in modo da mostrare che i domini di origine sono bloccati.


3 Immettere il nome dominio a cui si sta consentendo l'accesso all'Organizzazione.

4 Per aggiungere altri domini e sottodomini all'elenco di domini consentiti, fare clic sul link **Aggiungi domini**.

5 Fare clic su **Salva**.

**Risultati**

Dominio di origine è ora attivato per i domini e i sottodomini specificati. Solo i membri dell'Organizzazione che accedono dai domini consentiti possono accedere all'Organizzazione. L'accesso degli utenti da un dominio diverso è bloccato.

**Nota** L'applicazione del criterio nell'Organizzazione può richiedere fino a 30 minuti.

Se l'utente o un altro **Proprietario dell'Organizzazione** blocca accidentalmente a se stesso l'accesso all'Organizzazione senza includere il proprio dominio nell'elenco dei domini di origine a cui è consentito accedere all'Organizzazione, aprire un ticket di assistenza.

# Che cos'è la federazione aziendale e come funziona con VMware Cloud Services?

Le aziende che utilizzano VMware Cloud services possono configurare la federazione con più domini aziendali. Con la federazione dei domini aziendali, è possibile attivare il Single Sign-On per gli utenti della propria azienda. La federazione aziendale con VMware Cloud services viene configurata tramite un workflow self-service e supporta l'integrazione con i provider di identità basati su SAML 2.0.

L'adozione di un accesso con identità federata per gli utenti e le Organizzazioni di VMware Cloud services dell'azienda consente di ottenere i seguenti vantaggi:

- Tutti gli utenti dell'azienda accedono a VMware Cloud services utilizzando il proprio account aziendale.
- I **proprietari dell'Organizzazione** possono controllare l'autenticazione in Organizzazioni e servizi assegnando ruoli di Organizzazione e servizio ai gruppi sincronizzati dalla directory aziendale.
- Il team della sicurezza può configurare e applicare criteri di protezione e accesso a livello aziendale per VMware Cloud services, inclusa l'autenticazione multifattore.

I **proprietari dell'Organizzazione** di un dominio non federato possono avviare il workflow di federazione self-service per l'intero dominio aziendale. Dopo aver completato la configurazione, la federazione aziendale diventa disponibile per tutti gli utenti del dominio aziendale e si applica a tutti i servizi di tutte le Organizzazioni.

**Avvertimento** L'azienda deve essere proprietaria dei domini che si desidera includere nella federazione per l'accesso con VMware Cloud services ed è necessario verificare la proprietà durante il primo passaggio del workflow self-service. Non è possibile eseguire la federazione dei domini che appartengono a un provider di servizi.

Per istruzioni dettagliate sulla configurazione della federazione aziendale tramite il workflow di federazione self-service, fare riferimento alla guida Configurazione della Federazione aziendale con VMware Cloud Services.

## Differenza tra autenticazione federata e autenticazione non federata

Se il dominio aziendale non è federato, l'accesso a VMware Cloud services viene autenticato tramite l'account ID VMware. Se è la prima volta che si utilizzano VMware Cloud services, visitare my.vmware.com per creare un ID VMware.

Se il dominio aziendale è federato, l'accesso a VMware Cloud services viene autenticato tramite l'account aziendale. Viene utilizzato un tenant di Workspace ONE Access ospitato come Identity Broker per configurare la federazione con il provider di identità. Il tenant ospitato viene configurato per la convalida con il provider di identità aziendale e Active Directory. È possibile gestire l'accesso di utenti e gruppi a VMware Cloud services configurando Workspace ONE Access Connector per sincronizzare utenti e gruppi dall'Active Directory aziendale. Per la sincronizzazione viene configurato solo un sottoinsieme degli attributi dei profili utente necessari, come `username`, `firstname`, `lastname` e indirizzo e-mail. È possibile aggiungere ulteriori attributi in un secondo momento.

**Nota** Le password degli utenti non vengono mai sincronizzate né memorizzate nella cache.

.

## È possibile annullare la federazione per il dominio aziendale?

Se si decide di annullare la configurazione della federazione o annullare la federazione di uno qualsiasi dei domini aziendali federati inizialmente configurati, è necessario generare un ticket di supporto.

## Elementi coinvolti nella configurazione della federazione aziendale per il dominio aziendale

La configurazione della federazione aziendale per il dominio aziendale è un processo self-service che coinvolge più passaggi, utenti e ruoli.

Ecco chi e cosa è coinvolto nella federazione del dominio aziendale con VMware Cloud services.

### Proprietario dell'Organizzazione

Gli utenti **Proprietario dell'Organizzazione** dei domini non federati possono avviare la configurazione della federazione da console di Cloud Services. Qualsiasi **Proprietario dell'Organizzazione** può avviare il processo di federazione self-service e assegnare uno o più utenti **Amministratore aziendale** per completare la configurazione.

I **proprietari dell'Organizzazione** che dispongono di ruoli di amministratore di sistema nella propria azienda e hanno una conoscenza sufficiente dei servizi Directory aziendali e della configurazione del fornitore di identità, possono agire come **Amministratori aziendali** per la configurazione della federazione.

### Amministratore aziendale

L'**Amministratore aziendale** è un amministratore di sistema che appartiene al team di sicurezza centrale dell'azienda e gestisce i servizi Directory e i fornitori di identità. In qualità di persona designata per la configurazione della federazione aziendale per il dominio aziendale, l'**Amministratore aziendale** completa i passaggi di configurazione e convalida del processo di configurazione self-service. La configurazione della federazione aziendale potrebbe includere i rappresentanti di diversi team di sicurezza. L'**Amministratore aziendale** designato può invitare altri amministratori ad aiutare con la configurazione.

### L'organizzazione della Federazione aziendale

Quando un **Proprietario dell'Organizzazione** avvia il workflow di federazione self-service per il proprio dominio aziendale invitando uno o più **Amministratori aziendali**, un'Organizzazione di federazione speciale diventa disponibile per la configurazione. Tutti gli utenti coinvolti nel processo di federazione self-service ricevono una notifica tramite e-mail con un collegamento per accedere a tale organizzazione di federazione. Lo scopo di questa organizzazione è configurare la federazione aziendale per il dominio aziendale e modificare la configurazione iniziale.

### Collegamento degli account aziendali agli ID VMware

Per poter accedere ai servizi della loro organizzazione, gli utenti esistenti di VMware Cloud services i cui account sono federati devono collegare i loro account aziendali ai rispettivi ID account VMware. I nuovi utenti che eseguono l'onboarding in VMware Cloud services dopo che la configurazione della federazione per i loro domini è stata attivata non devono creare un ID VMware, a meno che non abbiano bisogno di visualizzare le informazioni di fatturazione o di archiviare i ticket di supporto.

VMware Cloud services

### Tenant VMware Workspace ONE Access

La configurazione della gestione delle identità federate richiede che il cliente configuri e gestisca un tenant VMware Workspace ONE Access. Il tenant viene creato come parte del processo di federazione self-service. Il tenant Workspace ONE Access funge da broker di

identità (fornitore di servizi) per il fornitore di identità e non è coinvolto nell'autenticazione utente effettiva.

**Workflow di configurazione della federazione self-service**

La configurazione della federazione self-service prevede più passaggi che possono essere eseguiti in vari momenti da diversi **Amministratori aziendali**. Il workflow riprende dall'ultima posizione. Gli **Amministratori aziendali** coinvolti nella configurazione devono disporre di account VMware Cloud services con un ID VMware. Tutti i passaggi della configurazione della federazione vengono completati tramite il workflow **Configura la federazione Enterprise** in tale organizzazione di federazione.

## Perché è necessario collegare l'ID My VMware?

Se si è **proprietari dell'Organizzazione** o un **Utente di supporto** con un account federato, è comunque necessario disporre di un ID VMware collegato all'account aziendale in modo da accedere alle informazioni di fatturazione e all'assistenza clienti.

### Perché non è possibile visualizzare tutti i servizi cloud personali?

È necessario collegare l'account ID VMware all'account federato in modo da poter accedere a tutti i servizi dall'account ID VMware. Se sono presenti token, questi verranno trasferiti automaticamente.

### Come si collega l'account dei servizi cloud personali?

Collegare l'account facendo clic su **Il mio account > Profilo** nella console di Cloud Services.

Se al momento della creazione dell'ID VMware è stato utilizzato l'indirizzo e-mail aziendale, fare clic sul pulsante **Collega ID VMware** nel banner del console di Cloud Services. Se si chiude il banner prima di collegare il proprio account, è possibile collegarsi all'account in un secondo momento facendo clic su **Il mio account > Profilo** nella console di Cloud Services.

È possibile visualizzare i dettagli dell'account collegato nella pagina Profilo.

### In che modo questo influisce sui proprietari o gli utenti dell'Organizzazione con ruoli di supporto?

Se si è **proprietari dell'Organizzazione** o si ricopre un ruolo di **Utente di supporto**, è necessario collegare l'account ID VMware per continuare ad accedere alle informazioni di fatturazione e all'assistenza clienti. Dopo aver collegato l'account, si riceverà un numero cliente. Successivamente, quando si crea una nuova Organizzazione, si collega l'account ID VMware durante la configurazione dell'Organizzazione.

### Dove è possibile visualizzare il numero cliente?

In qualità di **Proprietario dell'Organizzazione** o di **Utente di supporto**, è necessario un numero cliente. Dopo aver collegato l'account, il numero cliente viene visualizzato sotto il proprio nome nel menu **Impostazioni utente/organizzazione**.


Nella pagina Profilo è inoltre possibile visualizzare il numero cliente e altri dettagli dell'account collegato.

### Che cosa accade ai client OAuth personali?

I client OAuth vengono utilizzati per integrare applicazioni di terze parti con VMware Cloud services.

Nei casi in cui il nome utente dell'account federato è uguale all'ID VMware, ad esempio joe@acme.com, tutti i client OAuth creati durante l'accesso con l'ID VMware vengono trasferiti nell'account federato quando si collega l'ID di VMware.

Se il nome utente dell'ID VMware non corrisponde all'account federato, ad esempio joe@gmail.com e joe@acme.com, i client non vengono trasferiti nell'account federato ed è necessario creare nuovi client.

Per ulteriori informazioni sulla creazione dei clienti OAuth, vedere Come eseguire l'autenticazione delle applicazioni con OAuth 2.0.

## Perché è necessario collegare il provider di identità aziendale?

Se il dominio è federato, è possibile utilizzare le funzionalità avanzate di Amministrazione identità e governance (IGA) per eseguire facilmente l'onboarding di chi non è utente dell'Organizzazione in VMware Cloud services.

Un modo per attivare l'IGA consiste nel chiedere a un **Amministratore aziendale** di apportare la modifica nel dashboard dell'Organizzazione della Federazione aziendale. Un altro modo consiste nel collegare l'Organizzazione al fornitore di identità. Solo i **proprietari dell'Organizzazione** dei domini federati possono collegare le Organizzazioni al proprio fornitore di identità.

1 Accedere a console di Cloud Services e fare clic su **Organizzazione > Dettagli**.

2 Nella sezione **Domini collegati a fornitore di identità**, fare clic su **Collega fornitore di identità**.

   L'IdP e i domini associati all'Organizzazione vengono visualizzati in una finestra popup.

3 Fare clic su **Collega**, quindi su **Continua**.

Per ulteriori informazioni sulle funzionalità IGA, vedere Che cos'è la governance e l'amministrazione delle identità, e come funzionano con VMware Cloud Services?.

# Che cos'è la governance e l'amministrazione delle identità, e come funzionano con VMware Cloud Services?

Identity Governance and Administration (IGA) è un servizio che consente alla propria azienda di ottenere dati per l'audit trail e la certificazione e aiuta gli utenti **proprietari dell'Organizzazione** a gestire richieste di accesso self-service, approvazioni, violazioni e token API in tempo reale.

Il servizio IGA include due tipologie di funzionalità: base e avanzate. È disponibile solo per le Organizzazioni con domini federati.

- Per iniziare a utilizzare le funzionalità IGA di base, il **Proprietario dell'Organizzazione** deve attivare il servizio IGA facendo clic sul link **Inizia** nella pagina **Gestione identità e accessi > Governance**.
- Per iniziare a utilizzare le funzionalità IGA avanzate, vedere Come attivare la governance e l'amministrazione avanzate delle identità nell'Organizzazione.

L'utilizzo del servizio IGA in un'Organizzazione consente agli utenti VMware Cloud Services di eseguire le operazioni seguenti:

| In qualità di | con IGA base | con IGA avanzato |
|---|---|---|
| Utente **Proprietario dell'Organizzazione** | ■ Accedere al dashboard Governance e amministrazione delle identità dalla pagina **Gestione identità e accessi > Governance** nella console di Cloud Services.<br>■ Attivare o disattivare la possibilità dei **Membri dell'Organizzazione** di inviare richieste self-service per ruoli aggiuntivi.<br>■ Gestire l'accesso ai servizi nell'Organizzazione tramite la gestione delle richieste dei ruoli di servizio e dell'Organizzazione in arrivo.<br>■ Monitorare le violazioni e rispondere immediatamente alle minacce. | ■ Onboarding di un servizio in qualsiasi Organizzazione attivata per la governance e collegata al proprio fornitore di identità aziendale. |
| **Membro dell'Organizzazione** | ■ Se attivato nell'Organizzazione, inviare le richieste di accesso self-service per ruoli di Organizzazione e di servizio aggiuntivi. Vedere Come richiedere ruoli nelle Organizzazioni attivate per la governance. | ■ Eseguire l'onboarding autonomamente in qualsiasi Organizzazione attivata dalla governance collegata al fornitore di identità aziendale. Vedere Come eseguire l'onboarding in qualità di utente con un account federato. |

## Come attivare la governance e l'amministrazione avanzate delle identità nell'Organizzazione

Se il dominio è federato, è possibile attivare ulteriori funzionalità IGA (Identity Governance and Administration) avanzate per tutte le Organizzazioni nel dominio federato.

L'attivazione delle funzionalità IGA avanzate nell'Organizzazione richiede quanto segue:

- Un **Proprietario dell'Organizzazione** del dominio federato deve collegare il fornitore di identità aziendale a VMware Cloud Services. Vedere Perché è necessario collegare il provider di identità aziendale?.
- Un **Amministratore aziendale** deve attivare le funzionalità avanzate Governance e amministrazione delle identità per alcune o tutte le Organizzazioni VMware Cloud services collegate al loro fornitore di identità aziendale. Per ulteriori informazioni, vedere Attivazione delle funzionalità avanzate Governance e amministrazione delle identità per i domini federati.

Per ulteriori informazioni sulla federazione aziendale, vedere Che cos'è la federazione aziendale e come funziona con VMware Cloud Services?.

Quando le funzionalità avanzate Governance e amministrazione delle identità sono attivate, gli utenti esterni all'Organizzazione possono richiedere l'accesso ai ruoli di Organizzazione e servizio nelle Organizzazioni collegate durante l'onboarding. Per ulteriori informazioni su questa funzionalità, vedere Come eseguire l'onboarding in qualità di utente con un account federato.

## Come gestire le richieste self-service per i ruoli aggiuntivi

In qualità di utente **Proprietario dell'Organizzazione** con attivazione all'Identity Governance and Administration (IGA) è possibile gestire le richieste dei ruoli dell'Organizzazione e servizio tramite la pagina **Governance > Richieste** nella console di Cloud Services.

L'opzione che consente di inviare richieste self-service è disponibile per gli utenti **Membri dell'Organizzazione** solo se questa opzione è attivata nell'Organizzazione.

| **Se la richiesta di ruoli aggiuntivi è attivata, gli utenti Membri dell'Organizzazione richiedono l'accesso...** | **Se la richiesta di ruoli aggiuntivi non è attivata...** |
|---|---|
| facendo clic sul collegamento **Richiedi accesso** in un riquadro del servizio nel catalogo di Cloud Services. | non è possibile fare clic sul collegamento **Richiedi accesso** nel riquadro del servizio. |
| facendo clic sul collegamento **Richiedi ruoli** nella pagina **Il mio account > I miei ruoli**. | Il collegamento **Richiedi ruoli** non viene visualizzato nella pagina **Il mio account > I miei ruoli**. |

### Come attivare o disattivare le richieste self-service

Per attivare o disattivare le richieste self-service per i ruoli aggiuntivi nell'Organizzazione, eseguire le operazioni seguenti:

1 Passare a **Governance > Richieste** e fare clic su **Impostazioni**.

2 Fare clic sul dispositivo di scorrimento **Richiesta di ruoli aggiuntivi** per attivare o disattivare l'impostazione.

3 Fare clic su **Salva**.

### Come si gestiscono le richieste in sospeso?

Tutte le richieste di accesso ai ruoli dell'Organizzazione e del servizio effettuate sono elencate nella sezione **Richieste in sospeso**. In **Richieste passate** è visualizzata la cronologia di tutte le richieste create nell'Organizzazione.

Per approvare o negare le richieste, selezionare una o più voci nell'elenco **Richieste in sospeso** e fare clic sul relativo pulsante. Gli utenti che richiedono l'accesso al ruolo ricevono una notifica e-mail quando la richiesta viene approvata o rifiutata.

### È possibile modificare le richieste di accesso prima di approvarle?

In qualità di **Proprietario dell'Organizzazione**, puoi modificare il periodo di tempo per l'accesso al ruolo di servizio richiesto da un **Membro dell'Organizzazione**. Puoi visualizzare il periodo di tempo della richiesta originaria facendo clic sul link **ID richiesta**. Per modificare il periodo di tempo richiesto, fare clic su **Approva**, quindi selezionare **Approva con modifica**. Modificare l'impostazione e inviare la modifica apportata.

**Nota** L'opzione **Approva con modifica** è disponibile solo per le richieste di accesso al ruolo del servizio e non è applicabile per i ruoli dell'Organizzazione.

I **proprietari dell'Organizzazione** non possono modificare l'accesso al servizio o al ruolo originariamente richiesto dal **Membro dell'Organizzazione**. Se si desidera fornire istruzioni al richiedente sul livello appropriato di accesso che si è disposti ad approvare, è possibile includere un messaggio nell'e-mail di notifica di mancata approvazione della richiesta. Il richiedente riceve l'e-mail di notifica e può inviare una nuova richiesta di accesso con i ruoli di Organizzazione e servizio appropriati.

## Come monitorare le violazioni dei criteri nell'Organizzazione

In qualità di **Proprietario dell'Organizzazione** attivata per Identity Governance and Administration (IGA), è possibile monitorare le violazioni di accesso per gli accessi degli utenti e gli accessi con app OAuth e token API nell'Organizzazione. È possibile definire e modificare i criteri per l'attivazione delle violazioni.

È possibile configurare criteri di violazione per gli accessi nell'Organizzazione attivata alla IGA attivando vari trigger per le app OAuth e i token API, ad es. token API inattivi, proprietari OAuth inattivi, ambiti di servizio ampi, URL non sicuri o non approvati per le app OAuth.

**Nota** Se il criterio di autenticazione del Dominio di origine è attivato, le violazioni dell'accesso dell'utente vengono acquisite per tutti i tentativi di accesso provenienti da domini non consentiti dall'impostazione del criterio.

**Procedura**

1 Accedi a console di Cloud Services con il tuo account aziendale.

2 Vai a **Gestione accessi e identità > Governance > Violazioni**.

3 Fare clic su **Impostazioni**.

4 Nella pagina **Impostazioni di violazione** che viene visualizzata, modifica le impostazioni per le app OAuth e i token API secondo necessità.

5 Fare clic su **Salva**.

Risultati

Il dashboard **Violazioni** verrà aggiornato e includerà le violazioni stabilite dalle nuove impostazioni.

Le informazioni sui dashboard vengono aggiornate quotidianamente.

## Come intervenire contro le violazioni dei criteri nell'Organizzazione

L'utente **Proprietario dell'Organizzazione** con Identity Governance and Administration (IGA) attivata che monitora le violazioni può agire in risposta alle violazioni individuate nell'Organizzazione. È possibile accedere all'elenco completo delle violazioni accedendo a **Gestione identità e accessi > Governance > Violazioni**.

Le violazioni acquisite nell'Organizzazione sono raggruppate in base al tipo di metodo di autenticazione utilizzato per accedere ai VMware Cloud Services che hanno attivato la violazione. Fare clic sulla scheda corrispondente per visualizzare l'elenco completo e le possibili azioni da eseguire per rispondere a una violazione.

- Nella scheda **App OAuth** sono visualizzati il nome dell'app che ha attivato la violazione, la sua gravità, la descrizione e l'indirizzo e-mail dell'utente dell'Organizzazione che ha creato l'app OAuth.
- Nella scheda **Token API** sono visualizzati il nome del token API che ha attivato la violazione, la sua gravità, la descrizione e l'indirizzo e-mail dell'utente dell'Organizzazione che ha creato il token API.
- Nella scheda **Accesso utente** sono visualizzati l'indirizzo e-mail dell'utente dell'Organizzazione il cui tentativo di accesso ha attivato la violazione, la sua gravità, la data in cui si è verificata la violazione e il dominio di origine da cui è stata generata. Una violazione dell'accesso dell'utente viene acquisita per i tentativi di accesso da qualsiasi dominio non consentito dal criterio di autenticazione del Dominio di origine. Per ulteriori informazioni, vedere Come gestire l'accesso degli utenti a livello di dominio.

Nella tabella seguente sono descritte le azioni che è possibile eseguire in risposta alle violazioni nella propria Organizzazione.

| Obiettivo | Operazione da eseguire |
| --- | --- |
| Cambiare la visibilità di una violazione | Questa azione modifica lo stato di visibilità di una violazione da `Attiva` a `Nascosta`. La violazione non viene eliminata e può essere ripristinata.<br>1 Individuare la violazione che si desidera nascondere e cliccare sulla doppia freccia corrispondente ( » ) per espanderne i relativi dettagli.<br>2 Selezionare la casella di controllo accanto alla violazione attiva da nascondere.<br>3 Fare clic su **Nascondi**.<br>La violazione non sarà più visualizzata nella sezione dei dettagli. |
| Visualizzare una violazione che è stata nascosta | Questa azione visualizza violazioni con stato `Nascosto`.<br>■ Espandere la sezione dei dettagli di una violazione e attivare l'interruttore **Mostra tutti**. Vengono visualizzate tutte le violazioni che sono state nascoste. |
| Rimuovere un'app OAuth dall'Organizzazione | Questa azione rimuove l'app OAuth e ne impedisce l'accesso all'Organizzazione. L'app OAuth non viene eliminata. Non verranno segnalate ulteriori violazioni da questa app. L'azione di rimozione non può essere annullata dalla pagina **Violazioni** – per monitorare le violazioni da questa app OAuth, è necessario aggiungerla di nuovo all'Organizzazione.<br>1 Nella pagina **Violazioni**, aprire la scheda **App OAuth**.<br>2 Individuare l'app che si desidera rimuovere.<br>3 Selezionare la casella di controllo accanto al nome.<br>4 Fare clic su **Rimuovi**. |
| Modificare il livello di gravità di una violazione | In base alle esigenze dell'Organizzazione, è possibile definire la gravità di qualsiasi criterio di violazione.<br>1 Sulla pagina **Violazioni** , fare clic su **Impostazioni**.<br>2 Utilizzare il menu a discesa **Gravità** per modificare l'impostazione relativa a ciascun criterio di violazione da modificare.<br>3 Fare clic su **Salva**. |

## Come gestire i token API nell'Organizzazione

In qualità di utente **Proprietario dell'Organizzazione** con Identity Governance and Administration (IGA) attivata, è possibile monitorare i token API creati nell'Organizzazione e impostare vincoli per il Time to live (TTL) inattivo e massimo per tutti i token che vengono creati.

Per accedere al dashboard **Token API**, aprire console di Cloud Services e passare a **Gestione identità e accessi > Governance > Token API**. Il dashboard che si apre fornisce un elenco di tutti i token API creati dagli utenti dell'Organizzazione.

Per ogni token API, è possibile visualizzare dettagli come il nome del token, il nome dell'utente dell'Organizzazione che ha creato il token API, le date di creazione e scadenza, la data dell'ultimo utilizzo del token e gli ambiti del token, ossia i ruoli dell'Organizzazione assegnati al token.

Nell'elenco del dashboard **Token API** viene visualizzata un'icona di avviso (⚠) se i criteri TTL per l'Organizzazione sono stati violati. I criteri TTL impostati per l'Organizzazione vengono applicati a tutti i nuovi token API creati dagli utenti dell'Organizzazione. Se si modifica un criterio TTL, viene visualizzata un'icona di avviso accanto a tutti i token API creati in precedenza che violano la nuova impostazione.

Esistono due impostazioni dei criteri TTL che è possibile attivare e disattivare o modificare:

- **Token TTL inattivo**.

  Questa impostazione definisce il tempo di inattività consentito per un token API prima che violi il criterio.

- **TTL token max**.

  Questa impostazione definisce il TTL massimo consentito per qualsiasi token API creato nell'Organizzazione. Gli utenti dell'Organizzazione non potranno generare token API con un TTL del token massimo superiore a quello definito da questa impostazione.

## Cosa è possibile fare se un token API viola qualsiasi criterio o linea guida nell'Organizzazione

Se un token API viola un criterio TTL nell'Organizzazione o sembra in qualche modo sospetto, è possibile disattivare il token dal dashboard **Token API**. In questo modo non può essere utilizzato per accedere alle risorse nell'Organizzazione.

1 Nel dashboard **Token API**, selezionare il token API che si desidera disattivare.

2 Fare clic sul link **Disattiva**.

  Lo stato del token API diventa Attivato a Disattivato. Il Proprietario del token API riceve una notifica tramite e-mail da VMware Cloud Services che un token che è stato utilizzato per accedere all'Organizzazione è stato disattivato da un **Proprietario dell'Organizzazione**.

  Per riattivare un token API disattivato, selezionare il token API nel dashboard, quindi fare clic sul link **Attiva**. Il proprietario del token API riceve una notifica e-mail che conferma la riattivazione.

### Come modificare i criteri TTL per i token API nell'Organizzazione

Per modificare i criteri TTL dei token API, eseguire le operazioni seguenti:

1 Sul dashboard **Token API**, fare clic su **Impostazioni**.

| Operazione da eseguire | Procedere così... |
|---|---|
| Attivare o disattivare un criterio. | Utilizzare il dispositivo di scorrimento **Stato criterio**. |
| Modificare un'impostazione TTL | Immettere un nuovo valore nella rispettiva sezione delle impostazioni TTL e selezionare un'unità di tempo nell'elenco a discesa. L'unità di tempo può essere in minuti, ore o giorni. |

2 Fare clic su **Salva**.

La convalida dei token esistenti rispetto ai criteri avviene una volta ogni 24 ore. Ciò significa che potrebbe essere necessario un po' di tempo prima che l'elenco delle violazioni del dashboard **Token API** venga aggiornato in seguito alla modifica apportata.

## Come assegnare i ruoli predefiniti nell'Organizzazione

In qualità di **Proprietario dell'Organizzazione** con Identity and Access Governance (IGA) attivata, è possibile assegnare ruoli di Organizzazione e di servizio predefiniti agli utenti dell'Organizzazione impostando un criterio.

I ruoli predefiniti concessi tramite tale criterio si applicano a tutti gli utenti che accedono all'Organizzazione da un dominio federato specificato e non possono essere modificati a livello di utente. Per modificare i permessi dei ruoli predefiniti, è necessario modificare il criterio.

**Importante** Esiste un problema noto per cui un **Proprietario dell'Organizzazione** non può visualizzare gli utenti dell'Organizzazione a cui sono stati assegnati ruoli predefiniti in base al criterio e che non dispongono di altri ruoli nell'Organizzazione. Questi utenti non verranno visualizzati nell'elenco **Utenti attivi** in console di Cloud Services, a meno che non richiedano ruoli aggiuntivi e le richieste non vengano approvate. Quando gli utenti con ruoli predefiniti ottengono ruoli aggiuntivi nell'Organizzazione, vengono visualizzati nell'elenco **Utenti attivi** e il **Proprietario dell'Organizzazione** può concedere loro ruoli aggiuntivi.

#### Prerequisiti

- Il fornitore di identità aziendale è collegato a VMware Cloud Services.
- Le funzionalità IGA avanzate sono attivate nell'Organizzazione.
- Si dispone del ruolo di **Proprietario dell'Organizzazione** all'interno dell'Organizzazione.

#### Procedura

1 Accedi a console di Cloud Services con il tuo account aziendale.

2 Andare in **Gestione accessi e identità > Governance > Richieste**.

3 Fare clic su **Impostazioni**.

4 Nella sezione **Concedi ruoli predefiniti** della pagina, fare clic sul link **Aggiungi criterio di dominio**.

5 Immettere un nome e una descrizione per il nuovo criterio.

6 Selezionare il dominio a cui si desidera applicare il criterio.

7 Selezionare i ruoli di Organizzazione e servizio che si desidera assegnare automaticamente a tutti gli utenti che accedono all'Organizzazione dal dominio specificato.

8 Fare clic su **Salva**.

**Risultati**

I ruoli specificati diventano disponibili per tutti gli utenti del dominio specificato al loro accesso a VMware Cloud Services.

# Come eseguire l'autenticazione delle applicazioni con OAuth 2.0

VMware console di Cloud Services utilizza OAuth 2.0 in modo da poter concedere alle applicazioni un accesso delegato sicuro alle risorse protette all'interno dell'Organizzazione. VMware Cloud Services supporta l'accesso alle applicazioni Web in cui gli utenti dell'app autorizzano l'accesso e le interazioni da server a server in cui i token di accesso vengono emessi direttamente nell'app.

## Che cos'è OAuth 2.0

OAuth 2.0 è un protocollo di autorizzazione che consente di concedere alle app un accesso sicuro alle risorse. Il client è autorizzato tramite un token di accesso. Il token di accesso ha un ambito che definisce a quali risorse può accedere il token. Per informazioni su OAuth 2.0, vedere la specifica OAuth all'indirizzo https://tools.ietf.org/html/rfc6749#page-8 oppure guardare questo post del blog intitolato OAuth 2.0 Simplified all'indirizzo https://aaronparecki.com/oauth-2-simplified/.

## Come funziona OAuth 2.0 con VMware Cloud Services

VMware Cloud services copre diversi casi d'uso per l'autorizzazione delle app sfruttando diversi tipi di concessione, come `client credentials`, `authorization code` e `public client` con `authorization code`. In base ai propri obiettivi, scegliere di creare uno dei tre tipi di app OAuth che corrispondono ad ciascun tipo di concessione, rispettivamente dal Server all'app del server, all'app Web e all'app nativa/mobile.

Si supponga di essere **Proprietario dell'Organizzazione** con accesso a VMware Cloud on AWS. È stata sviluppata un'app che aiuta a scambiare azioni. L'app viene chiamata `Trading 1.0`. Si desidera eseguire l'app nelle macchine virtuali gestite da un vCenter Server, ma prima di tutto è necessario autorizzare l'app con le API di VMware Cloud on AWS.

1 Viene creata un'app OAuth 2.0 nella console di Cloud Services. Questa azione può essere un modo per registrare l'app `Trading 1.0`. Per avviare la creazione dell'app, fare clic su **Crea App** nel menu **Organizzazione > App OAuth** e seguire una serie di passaggi. Al termine del processo, vengono emesse le credenziali del client sotto forma di ID dell'app e segreto dell'app utilizzati per identificare il client con le API. Incollare queste credenziali nello script.

2 L'app è stata creata nell'Organizzazione, ma non le è ancora stato concesso l'accesso. È possibile concedere l'accesso aggiungendola all'Organizzazione. In questo modo l'app può accedere ai servizi e alle risorse dell'Organizzazione definite durante la creazione dell'app. Questo passaggio è necessario solo per le app del tipo da server a server. Non è applicabile alle app Web e native/mobili.

3 Quando si esegue l'app client `Trading 1.0`, viene richiesto un token di accesso dal server di autorizzazione. Se autorizzato, il server di autorizzazione invia un token di accesso alle API di e al client viene concesso l'accesso.

## Chi può creare e gestire le app OAuth

In qualità di utente **Proprietario dell'Organizzazione** o di **Membro di un'Organizzazione** con il ruolo di **Sviluppatore**, si ha la possibilità di creare e gestire le app OAuth.

È inoltre possibile gestire le app OAuth create o aggiunte da altri **proprietari dell'Organizzazione** all'interno dell'Organizzazione.

## È possibile rigenerare un segreto dell'app?

Sì, in qualità di **Proprietario dell'Organizzazione**, si ha la possibilità rigenerare il segreto app di un'app OAuth nell'Organizzazione. Questo è utile se il **Proprietario dell'Organizzazione** che ha creato l'app OAuth non è più nell'azienda ma si desidera continuare a eseguire l'app.

## È possibile utilizzare un'autenticazione token API anziché un'app OAuth?

Sì, se un'API impone che un utente sia l'entità autenticata nel processo di autorizzazione, è necessario utilizzare un token API. Per visualizzare quando utilizzare le app OAuth rispetto ai token API, vedere Differenza tra le app OAuth e i token API

## Come gestire le app OAuth 2.0

In qualità di utente **Proprietario dell'Organizzazione**, è possibile creare, visualizzare e modificare i dettagli delle app OAuth 2.0 nell'Organizzazione.

È inoltre possibile:

- gestire le app OAuth create o aggiunte da altri utenti **proprietari di Organizzazione** all'interno dell'Organizzazione;
- concedere l'accesso alle app create in qualsiasi Organizzazione in cui si disponga del ruolo di **Proprietario dell'Organizzazione**.

| Operazione da eseguire | Procedere così... |
| --- | --- |
| Visualizzare le app OAuth che hanno accesso all'Organizzazione. | Fare clic su **Gestione identità e accessi > App OAuth**.<br>Qui è possibile visualizzare le app create in altre Organizzazioni con accesso alla propria Organizzazione. |
| Aggiungere un'app OAuth creata in un'altra Organizzazione. | 1 Fare clic su **Gestione identità e accessi > App OAuth**.<br>2 Fare clic su **Aggiungi app**.<br>3 Per identificare l'app OAuth che si desidera aggiungere, selezionare una delle seguenti opzioni:<br>■ **Immettere l'ID app**<br>■ **Cerca per organizzazione**<br>4 Fare clic su **Continua**.<br>5 Se si è scelto di identificare l'app OAuth utilizzando il relativo ID, viene richiesto di immettere l'ID dell'app OAuth.<br>6 Se si è scelto di identificare l'app OAuth tramite l'organizzazione in cui è stata creata, viene innanzitutto richiesto di selezionare il nome dell'organizzazione nel menu a discesa e quindi di selezionare l'app OAuth nell'elenco di app OAuth disponibili in tale organizzazione.<br>Il menu a discesa **Organizzazione** mostra solo le Organizzazioni in cui si dispone dell'accesso come **Proprietario dell'Organizzazione**.<br>7 Rivedere i dettagli dell'app e fare clic su **Aggiungi**. |
| Rimuovere un'app OAuth creata in un'altra Organizzazione che ha accesso all'Organizzazione. | 1 Fare clic su **Gestione identità e accessi > App OAuth**.<br>2 Nell'elenco di app OAuth visualizzato, selezionare l'app a cui si desidera impedire l'accesso all'Organizzazione.<br>3 Fare clic su **Rimuovi**. |

| Operazione da eseguire | Procedere così... |
| --- | --- |
| Per visualizzare le app create nell'Organizzazione. | Fare clic su **Organizzazione > App OAuth**.<br>Qui è possibile visualizzare tutte le app create nell'Organizzazione.<br>■ Modificare un'app. Se si modifica l'ambito di un'app, le modifiche non vengono incluse nelle istanze dell'app che si trovano in altre Organizzazioni. Per aggiornare l'ambito, gli utenti **proprietari dell'Organizzazione** devono rimuovere l'app dalla propria Organizzazione e aggiungerla di nuovo oppure modificare l'app in modo che rifletta l'ambito aggiornato.<br>■ Rimuovere un'app dall'Organizzazione.<br>■ Aggiungere un'app creata nell'Organizzazione ma che non abbia ancora ricevuto l'accesso all'Organizzazione.<br>■ Creare un'app. |
| Per creare una nuova app OAuth nell'Organizzazione. | 1 Fare clic su **Organizzazione > App OAuth**.<br>2 Selezionare il tipo di app che si desidera aggiungere:<br>■ Per l'app da server a server, vedere Come utilizzare OAuth 2.0 per le app da server a server<br>■ Per l'app Web, vedere Come utilizzare OAuth 2.0 per le app Web<br>■ Per l'app nativa/mobile, vedere Come utilizzare OAuth 2.0 per le app native e mobili |
| Per gestire le app OAuth create nell'Organizzazione. | Fare clic su **Organizzazione > App OAuth** e selezionare l'app che si desidera gestire:<br>■ Per modificare l'app OAuth, fare clic su **Modifica**.<br>**Nota** Se si modifica l'ambito di un'app, le modifiche non vengono incluse nelle istanze dell'app che si trovano in altre Organizzazioni. Per aggiornare l'ambito, gli utenti **proprietari dell'Organizzazione** devono rimuovere l'app dalla propria Organizzazione e aggiungerla di nuovo oppure modificare l'app in modo che rifletta l'ambito aggiornato.<br>■ Per rimuovere un'app, fare clic su **Elimina**.<br>**Nota** Questa azione non può essere annullata. Tutte le applicazioni che utilizzano queste credenziali client non saranno più in grado di accedere a risorse protette e le credenziali verranno invalidate.<br>■ Per aggiungere un'app da server a server creata nell'Organizzazione ma a cui non è ancora stato concesso l'accesso all'Organizzazione, fare clic su **Aggiungi all'Organizzazione**. |

## Come utilizzare OAuth 2.0 per le app da server a server

Se l'applicazione richiede l'accesso diretto a un altro server senza l'autorizzazione dell'utente, è possibile creare una `Server to server app`. Questa opzione si basa sul tipo di concessione

delle `client credentials` OAuth 2.0. Durante questo flusso, l'app utilizza le credenziali OAuth per recuperare un token di accesso.

L'ambito ha un'importanza speciale nelle app da server a server. Gli ambiti forniscono un modo per implementare il controllo su quali aree di un'Organizzazione possono accedere al client, in modo specifico a quale ruolo in un'Organizzazione e a quali servizi e livello di autorizzazioni. L'utente **Proprietario dell'Organizzazione** può aggiungere l'app da server a server a qualsiasi Organizzazione. Pertanto, anche se è possibile specificare un'ampia gamma di accesso per l'app su molti servizi cloud, l'accesso viene infine determinato dai servizi contenuti in un'Organizzazione. Quando si aggiunge un'app OAuth a un'Organizzazione che non include i servizi inclusi nell'ambito dell'app, viene visualizzata una notifica.

Prerequisiti

- Si dispone delle autorizzazioni necessarie per aggiungere e gestire le app OAuth in questa Organizzazione. Vedere Quali ruoli dell'Organizzazione sono disponibili in VMware Cloud Services?.

Procedura

1. Accedere a console di Cloud Services.
2. Fare clic su **Organizzazione > App OAuth** e quindi su **Crea nuova app OAuth**.
3. Selezionare **App da server a server**.
4. Registrare il client immettendo un nome e una descrizione.
5. Impostare il valore **TTL token di accesso** per la nuova app OAuth.

   Il TTL (Time To Live) del token di accesso definisce il periodo di tempo in cui il token è valido.

   - Il TTL del token di accesso predefinito è 30 minuti;
   - il TTL massimo del token di accesso che è possibile impostare è 300 minuti (cinque ore);
   - il TTL minimo del token di accesso che è possibile impostare è 1 minuto.
6. Definire gli ambiti.

   Gli ambiti forniscono un modo per implementare il controllo su quali aree di un'Organizzazione possono accedere al client, in modo specifico a quale ruolo in un'Organizzazione e a quali servizi e livello di autorizzazioni.
7. Fare clic su **Crea** per generare le credenziali del client.
8. Nella finestra a comparsa **App OAuth creata**, copiare le credenziali o scaricare un file JSON e fare clic su **Continua**.

   L'utente è responsabile dell'archiviazione delle credenziali in un luogo sicuro.
9. (Facoltativo) Aggiungere l'app all'Organizzazione attiva.

   È possibile ignorare questo passaggio e aggiungere l'app a questa Organizzazione e ad altre Organizzazioni in un secondo momento. Vedere Come gestire le app OAuth 2.0.

### Operazioni successive

Incollare le credenziali nello script.

## Come utilizzare OAuth 2.0 per le app Web

Se l'applicazione è un'app Web regolare che viene eseguita su un server e richiede l'autorizzazione dell'utente, viene creata una `Web app`. Questa opzione si basa sul tipo di concessione delle `authorization code` OAuth 2.0. Durante questo flusso, gli utenti autorizzano l'applicazione prima di accedere a tutte le risorse e l'app recupera un token di accesso e, facoltativamente, un token di aggiornamento.

### Prerequisiti

- Si dispone delle autorizzazioni necessarie per aggiungere e gestire le app OAuth in questa Organizzazione. Vedere Quali ruoli dell'Organizzazione sono disponibili in VMware Cloud Services?.

### Procedura

1. Accedere a console di Cloud Services.
2. Fare clic su **Organizzazione > App OAuth** e quindi su **Crea nuova app OAuth**.
3. Selezionare **App Web** e fare clic su **Continua**.
4. Registrare l'app immettendo i relativi dettagli:
   a. Digitare un nome e una descrizione per la nuova app OAuth.
   b. Inserire almeno un URI di reindirizzamento.

      Dopo che un utente ha autorizzato il client, il server di autorizzazione reindirizza l'utente al client all'URI specificato con un token di accesso. È consigliabile aggiungere più di un URI. Utilizzare il formato http://acme.com.
   c. Specificare un intervallo di tempo per il token di accesso.

      L'impostazione TTL (Time to Live) del token di accesso predefinito è 30 minuti. Il valore massimo che è possibile impostare è 300 minuti (cinque ore). Il valore minimo che è possibile impostare è 1 minuto.
   d. Se si desidera che il token di accesso autorizzi le richieste in modo continuativo, selezionare **Emetti un token di aggiornamento** e impostare il valore **Aggiorna TTL token**.

      Il valore predefinito di Aggiorna TTL token è 30 minuti. Il valore massimo che è possibile impostare è 300 minuti (cinque ore). Il valore minimo che è possibile impostare è 1 minuto.
5. Definire gli ambiti.

   Gli ambiti forniscono un modo per implementare il controllo sulle aree dell'Organizzazione a cui il client può accedere, in particolare i determinati servizi e il livello di autorizzazione.

6 Selezionare la casella di controllo **Apri ID** per ottenere informazioni sugli utenti che autorizzano l'app.

7 Fare clic su **Crea** per generare le credenziali del client.

8 Copiare le credenziali o scaricare un file JSON contenente le proprie credenziali. L'utente è responsabile dell'archiviazione delle credenziali in un luogo sicuro.

9 Fare clic su **Continua**.

#### Operazioni successive

Incollare le credenziali nello script.

## Come utilizzare OAuth 2.0 per le app native e mobili

I client pubblici come le app native e mobili non possono mantenere la riservatezza di un segreto client. Quando si utilizza OAuth 2.0 per le app native e mobili, viene generato un ID app e viene utilizzata la chiave pubblica per lo scambio di codice (PKCE) per fornire una verifica aggiuntiva.

PKCE è una tecnica per proteggere i client pubblici che non utilizzano un segreto client. Per ulteriori informazioni sull'utilizzo di PKCE con le app mobili, vedere questo blog.

#### Prerequisiti

- Si dispone delle autorizzazioni necessarie per aggiungere e gestire le app OAuth in questa Organizzazione. Vedere Quali ruoli dell'Organizzazione sono disponibili in VMware Cloud Services?.

#### Procedura

1 Fare clic sul nome utente e selezionare **Visualizza organizzazione > App OAuth**, quindi fare clic su **Crea nuova app OAuth**.

2 Selezionare **App nativa/mobile** e fare clic su **Continua**.

3 Registrare l'app immettendo i relativi dettagli:

   a Digitare un nome e una descrizione per la nuova app OAuth.

   b Inserire almeno un URI di reindirizzamento.

      Dopo che un utente ha autorizzato il client, il server di autorizzazione reindirizza l'utente al client all'URI specificato con un token di accesso. È consigliabile aggiungere più di un URI. Utilizzare il formato http://acme.com.

c Specificare un intervallo di tempo per il token di accesso.

L'impostazione TTL (Time to Live) del token di accesso predefinito è 30 minuti. Il valore massimo che è possibile impostare è 300 minuti (cinque ore). Il valore minimo che è possibile impostare è 1 minuto.

d Se si desidera che il token di accesso autorizzi le richieste in modo continuativo, selezionare **Emetti un token di aggiornamento** e impostare il valore **Aggiorna TTL token**.

Il valore predefinito di Aggiorna TTL token è 30 minuti. Il valore massimo che è possibile impostare è 300 minuti (cinque ore). Il valore minimo che è possibile impostare è 1 minuto.

4 Definire gli ambiti.

Gli ambiti forniscono un modo per implementare il controllo sulle aree dell'Organizzazione a cui il client può accedere, in particolare i determinati servizi e il livello di autorizzazione.

5 Selezionare la casella di controllo **Apri ID** per ottenere informazioni sugli utenti che autorizzano l'app.

6 Fare clic su **Crea** per generare le credenziali del client.

7 Copiare l'ID dell'app o scaricare un file JSON che contenga l'ID dell'app. L'utente è responsabile dell'archiviazione di queste credenziali in un luogo sicuro.

8 Fare clic su **Continua**.

#### Operazioni successive

Incollare le credenziali nello script.

## Differenza tra le app OAuth e i token API

È possibile utilizzare sia le app OAuth sia i token API per interagire con le API di VMware Cloud Services.

I token API vengono emessi dagli utenti in un'Organizzazione e sono associati all'account dell'utente e all'Organizzazione da cui hanno generato il token API. Una volta create da un utente in un'Organizzazione, le app OAuth agiscono come entità nelle interazioni da server a server e possono essere utilizzate in più Organizzazioni. Solo gli utenti che hanno creato i token API possono gestirli. Il Proprietario dell'app OAuth è l'Organizzazione in cui è stata creata e l'app può essere gestita da utenti che sono **proprietari dell'Organizzazione** o **Membri dell'Organizzazione** con un ruolo **Sviluppatore**.

È possibile utilizzare sia le app OAuth sia i token API per automatizzare i processi che interagiscono con le API di VMware Cloud Services. La differenza è che i token API incorporano l'account utente nel token di accesso mentre le app OAuth eseguono l'autorizzazione senza un account utente. Quando si seleziona l'utilizzo di un token API o di un'app OAuth per effettuare una chiamata API, è necessario considerare i requisiti specifici del servizio API coinvolto nell'interazione. Alcune API richiedono che un account utente sia l'entità autenticata, mentre altre non lo richiedono. Ad esempio, se si chiama un'API per recuperare le informazioni di fatturazione e sottoscrizione per l'Organizzazione in VMware Cloud Services, è possibile utilizzare un'app

OAuth del tipo da server a server o un token API per effettuare chiamate al servizio API perché non richiede autenticazione tramite le credenziali dell'utente e accetta anche credenziali client. Se gli utenti di un'Organizzazione utilizzano un'API per aggiornare la propria password, l'API richiede che un utente agisca come entità di autenticazione.

**Importante** Prima di utilizzare le app OAuth del tipo da server a server per le chiamate automatizzate ai servizi cloud, devi innanzitutto consultare la documentazione dell'API pertinente.

# Come funziona il controllo dei registri eventi in VMware Cloud Services

Utilizzando un'istanza associata di VMware Aria Operations for Logs, è possibile monitorare gli eventi attivati dagli utenti dell'Organizzazione come risultato di attività con accessi utente, gestione degli utenti, token API, applicazioni OAuth e fatturazione.

VMware Aria Operations for Logs è un servizio di VMware Cloud ed è necessaria una sottoscrizione a pagamento o di prova per utilizzarlo. Per informazioni sulle diverse opzioni di sottoscrizione, vedere Sottoscrizione e fatturazione di VMware Aria Operations for Logs (SaaS) .

Utilizzando il servizio VMware Aria Operations for Logs, è possibile ottenere un'ampia gamma di funzionalità di controllo come il filtro dei registri, l'archiviazione e l'inoltro. È possibile accedere ai dati di controllo dell'Organizzazione avviando il servizio VMware Aria Operations for Logs nella console di Cloud Services. In questo modo si apre il dashboard **Controllo di eventi per VMware Cloud Services** in cui viene visualizzata una panoramica visiva degli eventi nell'Organizzazione. Se il dashboard non è attivato per impostazione predefinita, selezionarlo per la visualizzazione dalla scheda **Dashboard pacchetto di contenuti** della pagina **Dashboard**.

Per ulteriori informazioni sull'utilizzo di VMware Aria Operations for Logs, fare riferimento a Utilizzo di VMware Aria Operations for Logs (SaaS).

**Nota** Se l'Organizzazione non dispone di una sottoscrizione al servizio VMware Aria Operations for Logs e si desidera comunque visualizzare gli eventi del registro di VMware Cloud services per il periodo presente o passato, come soluzione alternativa è possibile ottenere un report di controllo Capitolo 12 Come ricevere assistenza. Il report viene ricevuto per il periodo di tempo specificato in un file CSV codificato via e-mail entro 48 ore dalla creazione della richiesta di assistenza.

## Chi può visualizzare i dati di controllo in VMware Aria Operations for Logs

Tutti gli utenti dell'Organizzazione con un ruolo di servizio **Utente di VMware Aria Operations for Logs** o **Amministratore di VMware Aria Operations for Logs** possono accedere a tutti i dati di controllo dell'Organizzazione nell'istanza del servizio VMware Aria Operations for Logs associata.

# Quali eventi di controllo vengono acquisiti da VMware Cloud Services?

I registri degli eventi forniscono informazioni sulle azioni dell'utente, come il nome dell'evento, l'utente che ha attivato l'evento, nonché l'ora e la posizione. In qualità di utente **Proprietario dell'Organizzazione**, è possibile rivedere gli eventi di controllo dell'Organizzazione utilizzando un'istanza di VMware Aria Operations for Logs associata.

VMware Cloud services acquisisce una serie di eventi di controllo relativi alle attività degli utenti in console di Cloud Services con gestione degli accessi e degli account, fatturazione e sottoscrizione. Se viene utilizzata l'automazione per gestire alcune risorse nell'Organizzazione, alcuni eventi possono essere attivati da un chiamante anziché da un utente.

## Ricerca e filtro degli eventi di controllo di VMware Cloud Services

È possibile cercare e filtrare gli eventi del registro per l'Organizzazione in due modi: utilizzando query salvate dal pacchetto di contenuti di **Eventi di controllo per VMware Cloud Services** e creando query personalizzate.

È possibile accedere ai pacchetti di contenuti dal menu **Pacchetti di contenuti** dell'istanza di vRealize Log Insight Cloud. Per ulteriori informazioni, vedere Utilizzo dei pacchetti di contenuti.

È possibile cercare e filtrare gli eventi dei registri nella pagina **Esplorazione di registri** del servizio vRealize Log Insight Cloud utilizzando query personalizzate per gli eventi di controllo di VMware Cloud Services. Per visualizzare solo gli eventi di controllo per VMware Cloud Services, come criterio di ricerca selezionare **log_type**, quindi **Contiene** e immettere **`csp-audit`**. Per cercare eventi specifici, creare una query che contenga il tipo di evento.

## Eventi di controllo per VMware Cloud Services

Tabella 10-1. Gestione dell'account

| Nome evento di controllo | Tipo di evento | Descrizione |
|---|---|---|
| UserLogin | csp__user_login | Accesso utente riuscito. |
| UserLogout | csp__user_logout | Logout utente riuscito. |
| GenerateApiToken | csp__generate_api_token | L'utente ha generato un token API personale. |
| RevokeApiToken | csp__revoke_api_token | L'utente ha revocato un token API personale. |
| RevokeAllApiTokens | csp__revoke_all_api_tokens | L'utente ha revocato tutti i token API personali. |
| RefreshTokenExchangeFailed | csp__refresh_token_exchange_failed | L'utente ha eseguito un tentativo non riuscito di generare il token di accesso tramite l'aggiornamento del token API. |
| FirstLogin | csp__first_login | All'utente sono stati assegnati i ruoli dall'invito al primo accesso. |

Tabella 10-1. Gestione dell'account (continua)

| Nome evento di controllo | Tipo di evento | Descrizione |
|---|---|---|
| LinkAccount | csp__link_account | L'utente ha collegato il proprio account federato aziendale all'account ID VMware. Questa azione ha permesso all'utente di accedere a VMware Cloud Services con le proprie credenziali aziendali. |
| UnlinkAccount | csp__unlink_account | L'utente ha modificato l'account collegato al relativo ID VMware. |
| CreateOrgOAuthApp | csp__create_org_o_auth_app | Il chiamante ha creato un'app OAuth in un'Organizzazione. |
| UpdateOrgOAuthApp | csp__update_org_o_auth_app | Il chiamante ha aggiornato un'app OAuth in un'Organizzazione. |
| DeleteOrgOAuthApp | csp__delete_org_o_auth_app | Il chiamante ha eliminato un'app OAuth in un'Organizzazione. |
| OrgOAuthAppNewSecretRotation | csp__org_o_auth_app_new_secret_rotation | Il chiamante ha ruotato il segreto di un'app OAuth in un'Organizzazione. |
| ActivateMfa | csp__activate_mfa | L'utente con ID VMware ha attivato un dispositivo MFA. |
| DeactivateMfa | csp__deactivate_mfa | L'utente con ID VMware ha disattivato un dispositivo MFA. |
| TurnOnMfa | csp__turn_on_mfa | L'utente con ID VMware ha attivato l'autenticazione multifattore per il proprio account. |
| TurnOffMfa | csp__turn_off_mfa | L'utente con ID VMware ha disattivato l'autenticazione multifattore per il proprio account. |
| RegenerateMfaRecoveryCodes | csp__regenerate_mfa_recovery_codes | L'utente con ID VMware ha rigenerato un nuovo set di codici di ripristino per l'autenticazione multifattore. |
| UpdateMfaAttributes | csp__update_mfa_attributes | L'utente con ID VMware ha aggiornato le impostazioni MFA per il proprio account. |
| GenerateNewMfaActivationSecret | csp__generate_new_mfa_activation_secret | L'utente con ID VMware ha generato un nuovo segreto di attivazione per la configurazione di MFA per il proprio account. |
| InvitationSentAck | csp__invitation_sent_act | Notifica interna creata quando un invito viene inviato a un utente. |
| CreateMspInvitation | csp__create_msp_invitation | È stato inviato tramite e-mail un invito per l'onboarding di una nuova Organizzazione di provider a un nuovo provider di servizi. |

Tabella 10-1. Gestione dell'account (continua)

| Nome evento di controllo | Tipo di evento | Descrizione |
|---|---|---|
| UpdateMspInvitation | csp__update_msp_invitation | È stato inviato tramite e-mail un invito aggiornato per l'onboarding di una nuova Organizzazione di provider a un nuovo provider di servizi. |
| DeleteMspInvitation | csp__delete_msp_invitation | L'invito tramite e-mail per l'onboarding di una nuova Organizzazione di provider inviata a un nuovo provider di servizi è stato revocato. |

Tabella 10-2. Gestione dell'organizzazione

| Nome evento di controllo | Tipo di evento | Descrizione |
|---|---|---|
| CreateOrganization | csp__create_org | L'utente ha creato una nuova Organizzazione. |
| UpdateOrganization | csp__update_org | L'utente ha aggiornato un'Organizzazione esistente. |
| DeleteOrganization | csp__delete_org | L'utente ha eliminato un'Organizzazione esistente. |
| InviteExistingUserToOrganization | csp__invite_existing_user_to_org | L'utente esistente è stato aggiunto a un'Organizzazione. |
| RemoveUserFromOrganization | csp__remove_user_from_org | L'utente esistente è stato rimosso da un'Organizzazione. |
| UpdateUserRolesOnOrganization | csp__update_user_roles_on_org | I ruoli di un utente esistente sono stati aggiornati. |
| InviteNonExistingUserToOrganization | csp__invite_non_existing_user_to_org | L'invito tramite e-mail è stato inviato a un nuovo utente. |
| RevokeUserInvitations | csp__revoke_user_invitations | Gli inviti inviati agli utenti tramite e-mail sono stati revocati. |
| RemoveClientFromOrganization | csp__remove_client_from_org | L'utente ha rimosso un'app OAuth assegnata a un'Organizzazione. L'azione non ha eliminato l'app OAuth. |
| AssignRolesToClientOnOrganization | csp__assign_roles_to_client_on_org | Ruoli di servizio/Organizzazione assegnati dal chiamante a un client di un'Organizzazione. L'azione indica una prima assegnazione a un client a cui non sono stati assegnati ruoli prima. |

Tabella 10-2. Gestione dell'organizzazione (continua)

| Nome evento di controllo | Tipo di evento | Descrizione |
|---|---|---|
| UpdateClientRolesOnOrganization | csp__update_client_roles_on_org | Ruoli di servizio/Organizzazione aggiornati dal chiamante a un client in un'Organizzazione. |
| UpdateUserDefaultOrganization | csp__update_user_default_org | L'utente ha aggiornato l'Organizzazione predefinita visualizzata per il proprio account. Questa azione si applica solo agli utenti che sono membri di più di un'Organizzazione. |

Tabella 10-3. Gruppi

| Nome evento di controllo | Tipo di evento | Descrizione |
|---|---|---|
| RemoveGroupFromOrganization | csp__remove_group_from_org | L'utente ha rimosso un gruppo esistente da un'Organizzazione. |
| AssignRolesToGroupOnOrganization | csp__assign_roles_to_group_on_org | L'utente ha assegnato ruoli di Organizzazione e servizio a un gruppo appena creato in un'Organizzazione. |
| UpdateGroupRolesOnOrganization | csp__update_group_roles_on_org | L'utente ha aggiornato le assegnazioni dei ruoli di un gruppo esistente in un'Organizzazione. |
| CustomGroupAddClients | csp__custom_group_add_clients | L'utente ha aggiunto nuovi membri a un gruppo personalizzato in un'Organizzazione. |
| CustomGroupRemoveClients | csp__custom_group_remove_clients | L'utente ha rimosso i membri esistenti da un gruppo personalizzato in un'Organizzazione. |

Tabella 10-4. Fatturazione e sottoscrizioni

| Nome evento di controllo | Tipo di evento | Descrizione |
|---|---|---|
| CreateSubscription | csp__create_subscription | L'utente ha creato una sottoscrizione per un servizio nuovo o esistente. |
| AddOrgPaymentMethod | csp__add_org_payment_method | L'utente ha aggiunto un nuovo metodo di pagamento alla propria Organizzazione. |
| RemoveOrgPaymentMethod | csp__remove_org_payment_method | L'utente ha rimosso un metodo di pagamento dalla propria Organizzazione. |
| UpdateOrgDefaultPaymentMethod | csp__update_org_default_payment_method | L'utente ha aggiornato il metodo di pagamento predefinito di un'Organizzazione. |

Tabella 10-4. Fatturazione e sottoscrizioni (continua)

| Nome evento di controllo | Tipo di evento | Descrizione |
|---|---|---|
| AddDetailsToOrg | csp__add_details_to_org | L'utente ha aggiunto un indirizzo aziendale e/o altri dettagli di fatturazione e sottoscrizione a un'Organizzazione. |
| UpdateOrgAddress | csp__update_org_address | L'utente ha aggiornato l'indirizzo dell'azienda nei dettagli di fatturazione e sottoscrizione per la propria Organizzazione. |
| UpdateOrgCommerceData | csp__update_org_commerce_data | L'utente ha aggiornato i dettagli di fatturazione e sottoscrizione per la propria Organizzazione (valuta, data di fatturazione annuale e così via) |
| UpdateOrgTaxId | csp__updated_org_tax_id | L'utente ha aggiornato l'ID fiscale nei dettagli di fatturazione e sottoscrizione per la propria Organizzazione. |
| UpdateOrgPoReferenceNumber | csp__update_org_po_reference_number | L'utente ha impostato un nuovo numero di riferimento del PO dell'Organizzazione. |
| IncomingOrder | csp__incoming_order | Il chiamante ha creato un ordine per la sottoscrizione di un servizio. |

Tabella 10-5. Identity Governance and Administration

| Nome evento di controllo | Tipo di evento | Descrizione |
|---|---|---|
| ApproveDenyEntitlementRequest | csp__iga_entitlements_requests_approval | Una richiesta di permesso è stata approvata o negata dal **Proprietario dell'Organizzazione**. |
| CreateEntitlementRequest | csp__iga_register_entitlements_request | L'utente ha creato una richiesta di permesso. |
| CreateEntitlementRequestForNonOrgMember | csp__iga_register_entitlements_request_non_org_member | Un nuovo utente non dell'Organizzazione ha creato una richiesta di permesso. |
| CancelEntitlementRequest | csp__iga_delete_entitlement_request | L'utente ha annullato una richiesta di permesso. |
| CancelEntitlementRequestForNonOrg | csp__iga_delete_entitlement_request_non_org_member | Un nuovo utente non dell'Organizzazione ha annullato una richiesta di permesso già inviata dallo stesso utente. |

Tabella 10-5. Identity Governance and Administration (continua)

| Nome evento di controllo | Tipo di evento | Descrizione |
|---|---|---|
| EnablingGovernance | csp__iga_status_change | Identity Governance and Administration è stata attivata per l'Organizzazione. |
| UpdateGovernancePolicies | csp__iga_update_governance_policies_request | L'utente ha aggiornato i criteri di Identity Governance and Administration |

# Come creare una notifica di pre-accesso NIST in VMware Cloud Services

Per soddisfare i requisiti di controllo di NIST 800- 53 AC-8, è necessario essere in grado di mostrare una notifica di pre-accesso agli utenti **Membri dell'Organizzazione** che accedono all'Organizzazione.

La notifica NIST viene applicata al dominio da cui gli utenti accedono a VMware Cloud Services indipendentemente dall'Organizzazione a cui appartengono. Quando gli utenti accedono a un'Organizzazione da un dominio per cui è stata creata una notifica NIST, visualizzano una finestra di dialogo che chiede loro di leggere e accettare i termini della notifica prima di procedere alla pagina di immissione della password.

In qualità di **Proprietario dell'Organizzazione**, è possibile richiedere un messaggio di notifica di NIST 800- 53 AC-8 personalizzato aprendo una richiesta di assistenza in VMware Customer Connect. Nella richiesta di assistenza includere le seguenti informazioni:

- il dominio aziendale per cui si desidera applicare la notifica NIST;
- il testo che si desidera visualizzare nella finestra di dialogo della notifica NIST;
- le versioni localizzate del testo in tutte le lingue necessarie;
- il nome dell'Organizzazione di VMware Cloud Services.

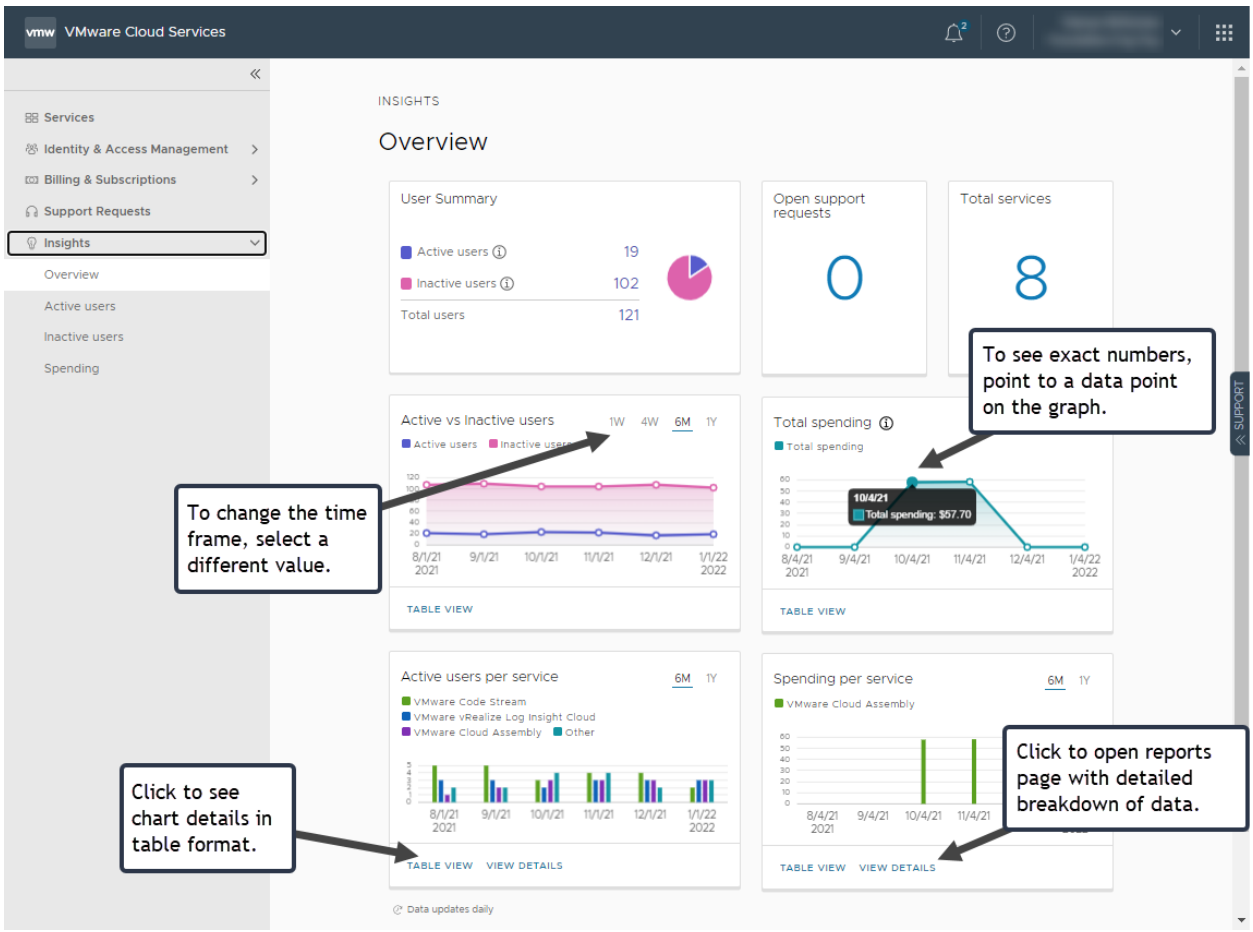
La notifica NIST viene implementata manualmente dall'assistenza tecnica di VMware dopo la verifica dello stato di **Proprietario dell'Organizzazione** e del dominio.

# Come utilizzare il dashboard dei dettagli

L'utente **Proprietario dell'Organizzazione** può visualizzare il modo in cui i servizi dell'Organizzazione vengono utilizzati nel tempo attraverso il dashboard **Dettagli** nella console di Cloud Services.

Per accedere al dashboard **Dettagli**, selezionare **Dettagli > Panoramica**.

Nel dashboard **Dettagli** viene visualizzato uno snapshot visivo del livello di attività degli utenti dell'Organizzazione in un periodo di tempo predefinito. È possibile ottenere informazioni sul numero totale di utenti attivi e inattivi nell'Organizzazione, sugli utenti attivi e inattivi per servizio, sui costi totali per tutti i servizi e sulla ripartizione dei costi per ciascun servizio.




I dati del dashboard **Dettagli** sono aggiornati giornalmente.

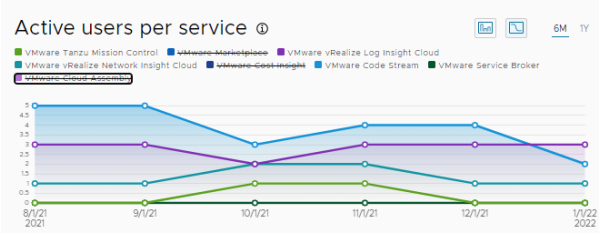
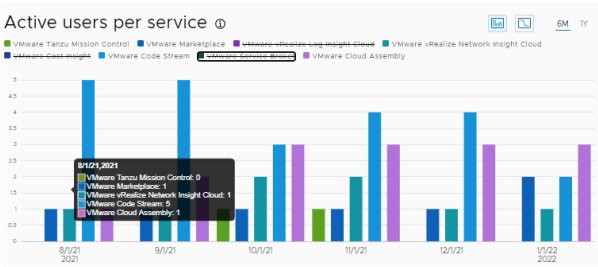
## Ulteriori utilizzi del dashboard Dettagli dati

In qualità di utente **Proprietario dell'Organizzazione**, è possibile ottenere un'analisi dettagliata dei dati relativi ai servizi, all'utilizzo e ai costi accedendo ai dashboard **Utenti attivi**, **Utenti inattivi** e **Costi**. È possibile filtrare i dati per visualizzare i sottoinsiemi delle informazioni visualizzate in ciascuna scheda.

### Il dashboard Utenti attivi

Il dashboard **Utenti attivi** visualizza informazioni su tutti gli utenti attivi per servizio nell'Organizzazione. Gli utenti attivi sono gli utenti che hanno effettuato l'accesso a VMware Cloud services almeno una volta in un periodo di 60 giorni.

| Operazione da eseguire | Procedere così... |
|---|---|
| Alternare fra la vista grafico e diagramma dei dati | Fare clic sull'icona del grafico ( ) o del diagramma ( ) nell'angolo in alto a destra del dashboard. |
| Per modificare il periodo di tempo per il report dei dati | Selezionare un periodo di tempo diverso facendo clic sulla rispettiva icona nell'angolo in alto a destra del dashboard. È possibile scegliere tra sei mesi e un anno. |

| Operazione da eseguire | Procedere così... |
| --- | --- |
| Per filtrare gli utenti attivi per servizi specifici | Fare clic sui nomi dei servizi che si desidera escludere dalla visualizzazione.<br>  <br><br>I nomi dei servizi esclusi appaiono barrati. Per includere di nuovo un servizio nella visualizzazione dei dati, fare clic sul relativo nome. |
| Visualizzare una ripartizione degli utenti attivi per servizio in un mese specifico | Puntare a un punto dati nel grafico o diagramma.<br>  <br> |
| Mostrare dettagli del diagramma in una vista tabella | Fare clic sul link **Mostra dettagli in una vista tabella**. |
| Visualizzare i dettagli dell'utente attivo | La tabella sotto il diagramma dati fornisce dettagli su tutti gli utenti attivi nell'Organizzazione, ad esempio nome, indirizzo email e giorni dall'ultimo accesso.<br>Scorrere le pagine della tabella facendo clic sulle icone avanti e indietro. |

## Il dashboard degli Utenti inattivi

Il dashboard **Utenti inattivi** include informazioni su tutti gli utenti inattivi per servizio nell'Organizzazione. Gli utenti inattivi sono gli utenti che non hanno effettuato l'accesso a VMware Cloud services negli ultimi 60 giorni.

| Operazione da eseguire | Procedere così... |
| --- | --- |
| Alternare fra la vista grafico e diagramma dei dati | Fare clic sull'icona del grafico ( ) o del diagramma ( ) nell'angolo in alto a destra del dashboard. |
| Per modificare il periodo di tempo per il report dei dati | Selezionare un periodo di tempo diverso facendo clic sulla rispettiva icona nell'angolo in alto a destra del dashboard. È possibile scegliere tra sei mesi e un anno. |
| Per filtrare gli utenti inattivi per servizio | Fare clic sui nomi dei servizi che si desidera escludere dalla visualizzazione. |
| Per visualizzare una ripartizione degli utenti inattivi per servizio in un mese specifico | Puntare a un punto dati nel grafico o diagramma. |

| Operazione da eseguire | Procedere così... |
| --- | --- |
| Mostrare dettagli del diagramma in una vista tabella | Fare clic sul link **Mostra dettagli in una vista tabella**. |
| Visualizzare i dettagli dell'utente inattivo | La tabella sotto il diagramma dei dati fornisce dettagli sugli utenti inattivi nell'Organizzazione, come il nome, l'indirizzo email, i giorni trascorsi dall'ultimo accesso e la data dell'ultima azione.<br>Scorrere le pagine della tabella facendo clic sulle icone avanti e indietro. |
| Rimuovere un utente inattivo dall'Organizzazione | Selezionare la casella di controllo accanto al nome dell'utente e fare clic su **Rimuovi dall'organizzazione**. |

### Dashboard Costo per servizio

Questo dashboard mostra la spesa mensile per servizio nell'Organizzazione in un determinato periodo di tempo. Il valore di costo visualizzato è riportato nella valuta predefinita dell'Organizzazione.

| Operazione da eseguire | Procedere così... |
| --- | --- |
| Alternare fra la vista grafico e diagramma dei dati | Fare clic sull'icona del grafico (  ) o del diagramma (  ) nell'angolo in alto a destra del dashboard. |
| Per modificare il periodo di tempo per il report dei dati | Selezionare un periodo di tempo diverso facendo clic sulla rispettiva icona nell'angolo in alto a destra del dashboard. È possibile scegliere tra sei mesi e un anno. |
| Per filtrare i servizi di cui viene visualizzato il costo | Fare clic sui nomi dei servizi che si desidera escludere dalla visualizzazione. |
| Per visualizzare la ripartizione dei costi dei servizi in un mese specifico | Puntare a un punto dati nel grafico o diagramma. |
| Mostrare dettagli del diagramma in una vista tabella | Fare clic sul link **Mostra dettagli in una vista tabella**. |

## Elementi coinvolti nell'utilizzo dei progetti nella console di Cloud Services

VMware Cloud Services utilizza Progetti per raggruppare le risorse di un'organizzazione in bucket distinti e assegnare l'accesso di utenti e gruppi alle risorse in ciascun bucket. In questo modo, i **Proprietari dell'Organizzazione** possono organizzare, mappare e monitorare in modo logico l'utilizzo delle risorse dei servizi cloud.

Quando si fa riferimento al termine "risorse" in VMware Cloud Services, è possibile pensare a queste come segmenti predefiniti, misurabili e logici di un servizio specifico. Organizzando le risorse dei servizi in Progetti, gli utenti **Proprietari dell'Organizzazione** possono misurare e monitorare l'utilizzo dei servizi cloud nella propria azienda tra reparti o centri di costo.

**Importante** Solo alcuni VMware Cloud services sono stati abilitati per utilizzare la funzionalità Progetti in console di Cloud Services. Per scoprire se un servizio in uso può utilizzare Progetti per raggruppare le risorse, consultare la documentazione di tale servizio o contattare l'assistenza VMware.

Si supponga di avere due progetti nell'organizzazione, Progetto 1 e Progetto 2, e tre servizi, ovvero Servizio A, Servizio B e Servizio C.

- Il Servizio A e il servizio B sono abilitati per il Progetto 1.
- Il Servizio B e il servizio C sono abilitati per il Progetto 2.

Il raggruppamento di risorse dei servizi abilitati consente di utilizzare le risorse del Servizio B in entrambi i progetti, mentre le risorse del servizio A e del Servizio C vengono utilizzate in un progetto ciascuno.

## Come creare un progetto nella console di Cloud Services

Per configurare e gestire i Progetti, è necessario disporre di un ruolo **Proprietario dell'Organizzazione** o **Amministratore del progetto** nell'Organizzazione. È possibile configurare un nuovo progetto da **Gestione identità e accessi > Progetti** in console di Cloud Services.

Nella configurazione di un nuovo progetto sono coinvolti tre passaggi:

1 Definire un nome per il nuovo progetto.

   Il nuovo progetto rimarrà vuoto finché non verranno abilitati i servizi che si intende utilizzare con tale progetto.

2 Visualizzare i servizi e le risorse abilitati per il progetto.

   Un servizio è abilitato per il progetto se elencato nella sezione **Servizi abilitati** e le risorse sono elencate nella tabella **Risorse**.

3 Assegnare l'accesso di utenti e/o gruppi al nuovo progetto.

## Come eliminare un progetto dall'Organizzazione

È possibile eliminare un progetto solo se vengono soddisfatte queste due condizioni:

- Al progetto non sono associati servizi e risorse abilitati.
- Gli utenti e/o i gruppi non dispongono delle autorizzazioni di accesso assegnate per il progetto.

# Fatturazione e sottoscrizioni

11

Gli utenti VMware Cloud Services con ruolo di **Proprietario dell'Organizzazione** possono visualizzare i dettagli di fatturazione e della sottoscrizione e gestire i metodi di pagamento per la propria Organizzazione. Gli utenti **Membro dell'Organizzazione** con un ruolo aggiuntivo **Fatturazione in sola lettura** possono visualizzare i dettagli di fatturazione e sottoscrizione per la propria Organizzazione senza la possibilità di gestire i metodi di pagamento.

Ogni Organizzazione in VMware Cloud Services è associata a un account di fatturazione.

È possibile utilizzare VMware Cloud services su richiesta o acquistando sottoscrizioni per un periodo di 1 o 3 anni. L'ordine di acquisto descrive la capacità, le date di inizio e di fine dei termini e il prezzo negoziato degli impegni inclusi nella sottoscrizione. VMware Cloud Services fattura in base alle condizioni indicate nell'ordine di acquisto.

L'utente riceve la fattura o il resoconto mensile delle attività per tutti i costi sostenuti dai servizi dell'Organizzazione acquistati tramite VMware.

Se l'Organizzazione ha acquistato servizi da più venditori, la pagina **Fatturazione e sottoscrizioni** mostra le informazioni di tutti i venditori. Tuttavia, le informazioni relative ai costi sostenuti e agli addebiti dei servizi acquistati tramite venditori non VMware non sono disponibili tramite la console di Cloud Services. Contattare i venditori per ottenere tali informazioni.

Leggi i seguenti argomenti:

- Guida introduttiva alla fatturazione e alle sottoscrizioni di VMware Cloud Services
- Come gestire i metodi di pagamento per l'Organizzazione
- Come utilizzare le sottoscrizioni e gli impegni di VMware Cloud Services
- Come funziona il dashboard Gestione utilizzo
- Come visualizzare estratti conto e fatture

## Guida introduttiva alla fatturazione e alle sottoscrizioni di VMware Cloud Services

Quando si acquistano sottoscrizioni VMware Cloud Services per la prima volta, si riceve un'e-mail con un link che apre il workflow di onboarding di VMware Cloud Services.

In qualità di utente iniziale e **Proprietario dell'Organizzazione**, è possibile specificare l'indirizzo e il metodo di pagamento predefinito quando si configura l'Organizzazione. VMware Cloud Services fattura ciascuna Organizzazione in base ai dettagli di fatturazione configurati durante l'onboarding:

- L'**Indirizzo** dell'azienda determina l'unità di vendita, le opzioni relative alla valuta, la tassazione e i metodi di pagamento disponibili per l'Organizzazione.

  Ad esempio, gli indirizzi statunitensi vengono addebitati in dollari USA e sono soggetti a imposte sulle vendite, mentre gli indirizzi britannici vengono addebitati in sterline britanniche e sono soggetti all'IVA. Inoltre, ogni Organizzazione registrata nell'Unione Europea ha la possibilità di immettere un ID imposta.
- La **Valuta con cui pagare** nell'Organizzazione è determinata dall'unità di vendita, che deriva dal paese in cui si trova l'indirizzo dell'azienda. Ogni Organizzazione può avere una valuta predefinita e valute di eccezione preapprovate in base all'indirizzo dell'Organizzazione. Unità di vendita diverse possono essere associate a una o più valute. Per ulteriori informazioni, vedere Come viene stabilita la valuta di pagamento.
- Il **Metodo di pagamento predefinito** può consistere in fondi prepagati VMware, carta di credito o Pagamento con fattura (PBI). I metodi di pagamento predefiniti disponibili per l'Organizzazione durante l'onboarding variano in base all'account di fatturazione.

  Ad esempio, alcuni utenti possono selezionare solo un PBI come metodo di pagamento, mentre altri possono selezionare i fondi VMware e le carte di credito.

### Prerequisiti

- Si sta effettuando l'onboarding di un servizio cloud a pagamento in una nuova Organizzazione in VMware Cloud Services.

### Procedura

1. Nel passaggio **Creazione di un'Organizzazione** del workflow di onboarding del servizio, specificare i dettagli di fatturazione per l'Organizzazione:
   a. Immettere un nome per l'organizzazione.
   b. Specificare l'indirizzo dell'azienda.

   **Importante** L'indirizzo aziendale fornito in questo passaggio deve superare un controllo di convalida dell'indirizzo ed essere conforme alle regole di convalida. Per ulteriori informazioni, vedere Informazioni importanti sulla convalida dell'indirizzo.

c Se sono disponibili diverse opzioni di valuta, selezionare la valuta in cui verranno emesse le fatture per l'Organizzazione.

d Selezionare il metodo di pagamento predefinito.

**Nota** Dopo l'onboarding di un servizio in un'Organizzazione, in qualsiasi momento gli utenti **proprietari dell'Organizzazione** possono Come modificare il metodo di pagamento predefinito dell'Organizzazione utilizzato per saldare le fatture in qualsiasi momento. La valuta di fatturazione dell'Organizzazione non può essere modificata in console di Cloud Services. Per passare a una valuta diversa, è necessario aprire un ticket di supporto.

2 Fare clic su **Completato**.

**Risultati**

L'account di fatturazione dell'Organizzazione è ora stato creato. Ora è possibile ottenere informazioni di fatturazione, gestire metodi di pagamento e sottoscrizioni ai servizi dal menu **Fatturazione e sottoscrizioni** in console di Cloud Services.

## Informazioni importanti sulla convalida dell'indirizzo

VMware Cloud Services applica i criteri di convalida all'indirizzo aziendale fornito per l'Organizzazione.

In qualità di **Proprietario dell'Organizzazione**, è possibile immettere un indirizzo aziendale quando si configura l'Organizzazione durante l'onboarding del servizio o quando si aggiungono nuovi servizi o sottoscrizioni a un'Organizzazione esistente. Per superare la convalida, l'indirizzo di un'Organizzazione deve contenere informazioni corrette su indirizzo, CAP, città, stato o provincia (se applicabile) e paese. Il controllo di convalida viene eseguito automaticamente quando:

- È possibile immettere o aggiornare l'indirizzo dell'azienda durante l'onboarding del servizio o della sottoscrizione.
- È possibile aggiornare l'indirizzo dell'azienda dalla pagina **Organizzazione > Dettagli**.

La tabella seguente fornisce dettagli sui possibili risultati del controllo di convalida e sulle azioni che è possibile eseguire, se necessario.

| Se... | In questo caso... |
| --- | --- |
| La convalida dell'indirizzo dell'Organizzazione è riuscita. | Procedere con il passaggio successivo del workflow di onboarding del servizio/sottoscrizione. |
| L'indirizzo dell'organizzazione non è conforme alle regole di convalida. Viene suggerito l'indirizzo conforme. | Viene aperta la finestra a comparsa **Modifica o seleziona un indirizzo** che mostra l'indirizzo originale e un indirizzo suggerito conforme alle regole di convalida.<br>■ Se si seleziona l'indirizzo suggerito, si procede con il passaggio successivo del workflow.<br>■ Se si decide di mantenere l'indirizzo originale, è necessario riconoscere che non è conforme alle regole di convalida e fornire il consenso per autorizzare VMware ad apportare tutte le modifiche necessarie all'indirizzo in modo che diventi conforme. A tale scopo, selezionare la rispettiva casella di controllo nella finestra a comparsa **Modifica o seleziona un indirizzo**.<br>■ Per modificare l'indirizzo originale fornito per l'Organizzazione, fare clic sul pulsante **Modifica indirizzo**. In questo modo, si torna alla pagina Profilo dell'organizzazione in cui è possibile apportare le modifiche necessarie. |
| Impossibile convalidare l'indirizzo dell'organizzazione. Non viene suggerito un indirizzo conforme. | Quando la convalida dell'indirizzo non riesce e non viene suggerito un indirizzo alternativo, viene aperta una finestra a comparsa che richiede di eseguire una delle seguenti operazioni:<br>■ Modificare l'indirizzo.<br>■ Fornire il consenso per autorizzare VMware ad apportare tutte le modifiche necessarie all'indirizzo dell'Organizzazione in modo che sia conforme alle regole di convalida selezionando la rispettiva casella di controllo. Solo dopo aver accettato il consenso sarà possibile procedere con l'onboarding del servizio/sottoscrizione. |
| Indirizzo dell'Organizzazione aggiornato da VMware dopo il consenso fornito dal **Proprietario dell'organizzazione**. | Quando si accede come **Proprietario dell'organizzazione** in VMware Cloud Services, viene aperta una finestra a comparsa che mostra l'indirizzo aggiornato.<br>■ Se si accetta il nuovo indirizzo convalidato, quest'ultimo sostituirà l'indirizzo dell'Organizzazione esistente. Tutti gli utenti con ruolo di **Proprietario dell'organizzazione** riceveranno una notifica sulla modifica all'interno dell'app.<br>■ Se si ignora il nuovo indirizzo convalidato, ogni volta che si apre il workflow del servizio/sottoscrizione di onboarding, verrà richiesto di modificare l'indirizzo in modo che sia conforme alle regole di convalida. |

# Come utilizzare le pagine di Fatturazione e sottoscrizione in VMware Cloud Services

La sezione **Fatturazione e sottoscrizioni** in console di Cloud Services ha alcune pagine di base che consentono di visualizzare l'attività dell'Organizzazione e di gestire i metodi di pagamento utilizzati per i servizi e le sottoscrizioni.

| | |
|---|---|
| **Panoramica** | La pagina **Panoramica** mostra i costi e gli addebiti correnti accumulati nell'ultimo mese per tutti i servizi dell'Organizzazione. Se le sottoscrizioni sono state acquistate tramite più fornitori, è possibile accedere ai dettagli di ciascun venditore da questa pagina.<br>Per ulteriori informazioni, vedere Come recuperare le informazioni di fatturazione per l'Organizzazione |
| **Gestione dei metodi di pagamento** | La pagina **Gestisci metodi di pagamento** consente di aggiungere nuovi metodi di pagamento all'Organizzazione e di modificare il metodo di pagamento predefinito.<br>Per ulteriori informazioni, vedere Come gestire i metodi di pagamento per l'Organizzazione |
| **Sottoscrizioni** | Nella pagina **Sottoscrizioni** vengono visualizzati i dettagli di tutte le sottoscrizioni VMware Cloud Services acquistate nell'Organizzazione.<br>Per ulteriori informazioni, vedere Come utilizzare le sottoscrizioni e gli impegni di VMware Cloud Services |
| **Crediti promozionali** | La pagina **Crediti promozionali** mostra i crediti promozionali disponibili che è possibile applicare e riscattare in relazione ai costi mensili dell'Organizzazione.<br>Per ulteriori informazioni, vedere Pagamento con i crediti promozionali |
| **Fatture ed estratti conto** | La pagina **Fatture ed estratti conto** consente di visualizzare e scaricare le note delle attività e le fatture per l'Organizzazione.<br>Per ulteriori informazioni, vedere Come visualizzare estratti conto e fatture |

# Come recuperare le informazioni di fatturazione per l'Organizzazione

Le informazioni di fatturazione relative all'Organizzazione possono essere visualizzate dalla pagina **Panoramica** nel menu **Fatturazione e sottoscrizioni** in console di Cloud Services.

In qualità di utente **Proprietario dell'Organizzazione** o **Membro dell'Organizzazione** con ulteriori autorizzazioni ruolo alla **Fatturazione in sola lettura**, è possibile visualizzare le seguenti informazioni di fatturazione per tutti i servizi acquistati da VMware:

- costi e addebiti maturati per il periodo di fatturazione corrente per tutti i servizi acquistati da VMware;
- crediti promozionali applicati ai costi correnti;
- pagamenti e saldo scoperto del periodo di fatturazione precedente per tutti i servizi acquistati da VMware;

- un conteggio dettagliato di tutti gli acquisti, addebiti, sconti, ecc. per tutti i servizi per mese.

**Nota** Per informazioni di fatturazione per i servizi acquistati tramite un venditore, è necessario accedere alla console di fatturazione del venditore. Per ulteriori informazioni, vedere Come visualizzare le informazioni sul venditore.

### Costi correnti

La sezione **Costi correnti** riflette i costi dei servizi acquistati da VMware. Ad esempio, l'utilizzo orario di cloud privati per CPU. Questi costi vengono maturati e rispecchiano l'utilizzo dei servizi dall'inizio del periodo di fatturazione corrente fino al giorno in cui vengono visualizzati. I costi maturati rispecchiano solo l'utilizzo su richiesta dei servizi nell'Organizzazione e non includono i costi degli impegni. Queste informazioni vengono aggiornate quotidianamente.

La sezione **Costi correnti** fornisce anche informazioni sugli eventuali crediti promozionali e sconti ricevuti dal programma VMware Discount.

### L'ultimo periodo di fatturazione

Nella sezione **Ultimo estratto conto fatturazione** è possibile visualizzare gli addebiti raggruppati maturati nel periodo di fatturazione precedente. Il periodo di fatturazione è determinato dalla data in cui il primo servizio è stato configurato nell'Organizzazione e dura un mese. Ad esempio, se il **Proprietario dell'Organizzazione** ha eseguito l'onboarding del primo servizio dell'Organizzazione il 15 del mese, il periodo di fatturazione per tutti i servizi nell'Organizzazione viene eseguito dal 15 di un mese al 14 del mese successivo.

La sezione **Ultimo estratto conto fatturazione** fornisce un riepilogo degli addebiti per i servizi su richiesta e ordinati per impegno maturati nel corso dell'ultimo periodo di fatturazione. Per visualizzare, scaricare e stampare un file dettagliato del rendiconto dell'attività per il periodo di fatturazione precedente, fare clic sul link **Visualizza rendiconto (PDF)** nella parte inferiore della sezione **Ultimo estratto conto fatturazione**.

Per visualizzare e stampare gli/le ultimi/e 15 rendiconti delle attività, fatture su richiesta e fatture di impegno annuale, fare clic sul link **Tutti gli estratti conto**. Per ulteriori informazioni, vedere Come visualizzare estratti conto e fatture.

In alcuni casi è possibile che un servizio cloud stimi l'utilizzo corrente dei costi per determinati elementi in una data diversa da quella dell'inizio del periodo di fatturazione. In un caso simile, potrebbe esservi un ritardo tra il momento in cui l'utilizzo si verifica e il momento in cui viene visualizzato nella fattura. Per ulteriori informazioni su come i servizi cloud stimano i costi correnti, vedere Modalità di stima dei costi correnti.

## Come sono stimati i costi correnti?

La sezione **Costi correnti** della panoramica relativa alla fatturazione rispecchia i costi dei servizi nell'Organizzazione in un dato momento. I costi visualizzati in questa sezione sono validi solo per i servizi acquistati da VMware. I costi sono maturati e riflettono l'utilizzo dei servizi dall'inizio di un periodo definito. Questo periodo definito potrebbe essere diverso dal periodo di fatturazione.

Per vedere come i servizi cloud stimano i costi correnti e in che modo questi costi influiscono sul ciclo di fatturazione, vedere la tabella seguente.

| VMware Cloud Services | Modalità di stima dei costi correnti |
| --- | --- |
| VMware Cloud on AWS | L'utilizzo dell'host per VMware Cloud on AWS viene monitorato in linea L ciclo di fatturazione. L'utilizzo dell'host mostrato nella fattura corrisponde all'intero utilizzo dell'host durante il periodo di fatturazione.<br>Altri tipi di utilizzo, tra cui il trasferimento di dati, l'utilizzo dell'indirizzo IP e i remapping, nonché l'utilizzo di EBS vengono ricevute il quinto giorno di ogni mese e includono i dati di utilizzo fino all'ultimo giorno del mese precedente. Per questi tipi di utilizzo, c'è un ritardo tra il momento in cui l'utilizzo si verifica e il momento in cui viene visualizzato nella fattura. Il tempo del ritardo dipende dal momento in cui si trova l'inizio del ciclo di fatturazione rispetto al quinto giorno del mese.<br>Per ulteriori informazioni, vedere Informazioni sulla fatturazione VMC. |

## Come viene stabilita la valuta di pagamento

Per VMware Cloud services è supportato il pagamento di servizi in varie valute con carta di credito, fondi e crediti promozionali. La valuta di pagamento viene selezionata in un elenco di opzioni durante la configurazione dell'Organizzazione.

Quando si configura un'Organizzazione, l'indirizzo aziendale che si immette determina le opzioni relative alla valuta che vengono visualizzate nel passaggio **Organizzazione e pagamento** del workflow di onboarding. Un'Organizzazione può pagare con la valuta predefinita, con una valuta di eccezione preapprovata o con USD se è selezionata l'opzione **`USD globale`**. Per informazioni dettagliate sull'onboarding del servizio, fare riferimento alla guida Introduzione a VMware Cloud Services.

Se è necessario modificare la valuta di pagamento impostando un'opzione diversa da quella già definita nell'Organizzazione, è possibile farlo in qualsiasi momento. Vedere Come modificare la valuta di pagamento nella propria Organizzazione.

VMware Cloud services supporta due unità di vendita: una per i clienti statunitensi e una per i clienti non statunitensi. Mentre gli importi fatturati per i clienti statunitensi sono espressi in dollari, gli importi fatturati per i Paesi dell'unità di vendita non USA sono espressi in varie valute. In che modo ciò potrebbe riguardarti?

- L'indirizzo dell'Organizzazione determina anche il tipo di imposte, ad esempio l'imposta sulle vendite o l'IVA. I codici di identificazione fiscale vengono utilizzati per facilitare l'amministrazione delle imposte locali. Se sei esente da imposte o se disponi di uno stato simile, è consigliabile inserire un identificativo fiscale. È possibile immettere un codice di identificazione fiscale quando si configura l'Organizzazione. Puoi eseguire questa operazione anche in un secondo momento, nella pagina Organizzazione, facendo clic sul tuo nome utente e selezionando **Visualizza organizzazione**.

- Per il pagamento dei servizi, puoi utilizzare qualsiasi carta di credito con qualsiasi indirizzo di fatturazione. Se la valuta di pagamento dell'Organizzazione è diversa da quella della carta di credito, potresti incorrere in commissioni per le transazioni estere dal fornitore della tua carta di credito.
- Se desideri modificare l'indirizzo della tua Organizzazione, il nuovo indirizzo deve trovarsi nella stessa unità di vendita dell'indirizzo precedente. Inoltre, non è possibile cambiare l'indirizzo con l'indirizzo di un Paese con una valuta diversa da quella dell'indirizzo precedente. Per ulteriori informazioni, consultare la tabella seguente.

  Se è necessario passare a un indirizzo che si trova in un'unità di vendita diversa o in un paese con una valuta diversa, inviare una richiesta di assistenza.

  Se si desidera modificare la valuta di pagamento scegliendo una valuta diversa da quella impostata per l'Organizzazione, è necessario creare un ticket di assistenza. Le istruzioni per eseguire questa operazione sono disponibili in Capitolo 12 Come ricevere assistenza.
- Puoi utilizzare qualsiasi fondo come metodo di pagamento nella tua Organizzazione se la valuta del fondo è la stessa della valuta dell'Organizzazione e appartiene alla stessa unità di vendita. Per pagare con un fondo, la valuta dell'account di fatturazione deve corrispondere alla valuta del fondo e la valuta del fondo deve corrispondere alla valuta di sottoscrizione dell'ordine.

## Unità di vendita VMware Cloud Services

Utilizza le informazioni contenute in queste tabelle per determinare la valuta in cui ti verranno addebitati i servizi.

### Tabella 11-1. Scambio internazionale dell'unità di vendita per clienti non statunitensi

| Se l'indirizzo dell'Organizzazione si trova in questo Paese... | La valuta di pagamento predefinita è... |
|---|---|
| Afghanistan, Algeria, Samoa americane, Angola, Anguilla, Antartide, Antigua e Barbuda, Argentina, Armenia, Aruba, Azerbaigian, Bahamas, Bahrain, Bangladesh, Barbados, Bielorussia, Belize, Benin, Bermuda, Bhutan, Bolivia, Bonaire, Sint Eustatius e Saba, Botswana, Isola Bouvet, Brasile, Territorio britannico dell'Oceano Indiano, Brunei Darussalam, Burkina Faso, Burundi, Cambogia, Camerun, Canada, Capo Verde, Isole Cayman, Repubblica Centrafricana, Ciad, Cile, Colombia, Comore, Congo, Isole Cook , Costa Rica, Costa d'Avorio, Cuba, Curacao, Gibuti, Dominica, Repubblica Dominicana, Timor Est, Ecuador, Egitto, El Salvador, Guinea Equatoriale, Eritrea, Estonia, Etiopia, Isole Falkland, Isole Faroe, Figi, Finlandia, Francese Guiana, Polinesia francese, French Southern Terr., Gabon, Gambia, Georgia, Ghana, Grenada, Guadalupa, Guam, Guatemala, Guinea, Guinea-Bissau, Guyana, Haiti, Isole Heard e Mcdonald, Honduras, Hong Kong, India, Indonesia , Iran, Iraq, Israele, Giamaica, Giordania, Kazakistan, Ke nya, Kiribati, Repubblica di Corea, Kuwait, Kirghizistan, Laos, Libano, Lesotho, Liberia, Libia, Macao, Madagascar, Malawi, Malesia, Maldive, Mali, Isole Marshall, Martinica, Mauritania, Mauritius, Mayotte, Messico, Micronesia, Moldavia , Montserrat, Marocco, Mozambico, Myanmar, Namibia, Nauru, Nepal, Antille Olandesi, Nuova Caledonia, Nuova Zelanda, Nicaragua, Niger, Nigeria, Niue, Corea del Nord, Isole Marianne Settentrionali, Oman, Pakistan, Palau, Territori palestinesi occupati, Panama , Papua Nuova Guinea, Paraguay, Perù, Filippine, Pitcairn, Porto Rico, Qatar, Reunion, Federazione Russa, Ruanda, Saint Barthelemy, Sant'Elena, Saint Kitts e Nevis, Santa Lucia, Saint Martin, Saint Pierre e Miquelon, Saint Vincent e Grenadine, Samoa, Sao Tome e Principe, Arabia Saudita, Senegal, Seychelles, Sierra Leone, Singapore, Isole Salomone, Somalia, Sud Africa, Georgia del Sud e Isole Sandwich meridionali, Sud Sudan, Sri Lanka, Sudan, Suriname, Svalbard e Jan Mayen, Swaziland, Siria a, Taiwan, Tagikistan, Tanzania, Thailandia, Timor Est, Togo, Tokelau, Tonga, Trinidad e Tobago, Tunisia, Turchia, Turkmenistan, Isole Turks e Caicos, Tuvalu, Uganda, Ucraina, Emirati Arabi Uniti, Isole Minori Esterne degli Stati Uniti , Uruguay, Uzbekistan, Vanuatu, Venezuela, Vietnam, Isole Vergini, Wallis e Futuna, Sahara occidentale, Yemen, | USD |
| Albania, Andorra, Austria, Belgio, Bosnia ed Erzegovina, Bulgaria, Croazia, Cipro, Repubblica Ceca, Danimarca, Francia, Germania, Grecia, Groenlandia, Ungheria, Islanda, Irlanda, Italia, Lettonia, Liechtenstein, Lituania, Lussemburgo, Macedonia, Malta , Monaco, Montenegro, Norvegia, Polonia, Portogallo, Romania, San Marino, Serbia, Slovacchia, Slovenia, Spagna, Svezia, Svizzera, Paesi Bassi, Città del Vaticano, Jugoslavia, Zambia, Zimbabwe, Isole Aland | EUR |
| Gibilterra, Guernsey, Isola di Man, Jersey, Regno Unito, | GBP |
| Giappone | JPY |
| Cina, Mongolia | CNY |
| Australia, Isola di Natale, Isole Cocos (Keeling), Isola di Norfolk | AUD |

### Tabella 11-2. Unità di vendita USA per clienti statunitensi

| Se l'indirizzo dell'Organizzazione si trova in questo Paese | Gli addebiti saranno espressi in |
|---|---|
| Stati Uniti d'America | USD |

### Come modificare la valuta di pagamento nella propria Organizzazione

La valuta di pagamento viene determinata durante il workflow di onboarding del servizio quando si configura l'Organizzazione. Il **Proprietario dell'Organizzazione** che configura l'Organizzazione seleziona la valuta predefinita o un'eccezione preapprovata.

La valuta di pagamento dell'Organizzazione può essere una delle seguenti:

- La valuta predefinita in base all'indirizzo aziendale.
- USD globale.
- Una valuta preapprovata diversa.

#### Prerequisiti

Per modificare la valuta di pagamento nell'Organizzazione, è necessario creare un ticket di supporto con VMware Customer Connect. I proprietari dell'organizzazione possono avviare la modifica in qualsiasi momento tramite console di Cloud Services.

.

#### Procedura

1. Accedere a console di Cloud Services e selezionare **Fatturazione e sottoscrizioni > Gestisci metodi di pagamento**.
2. Fare clic sul pulsante **Modifica valuta**.
3. Nella finestra di dialogo che viene aperta, fare clic su **Crea una richiesta di assistenza**.

   Verrà aperta la pagina Assistenza VMware in VMware Customer Connect.
4. In **Assistenza non tecnica**, fare clic su **Richiedi assistenza guidata**.
5. In **Cloud Services**, fare clic su **Fatturazione e utilizzo** e seguire le istruzioni visualizzate per creare la richiesta.

## Come visualizzare le informazioni sul venditore

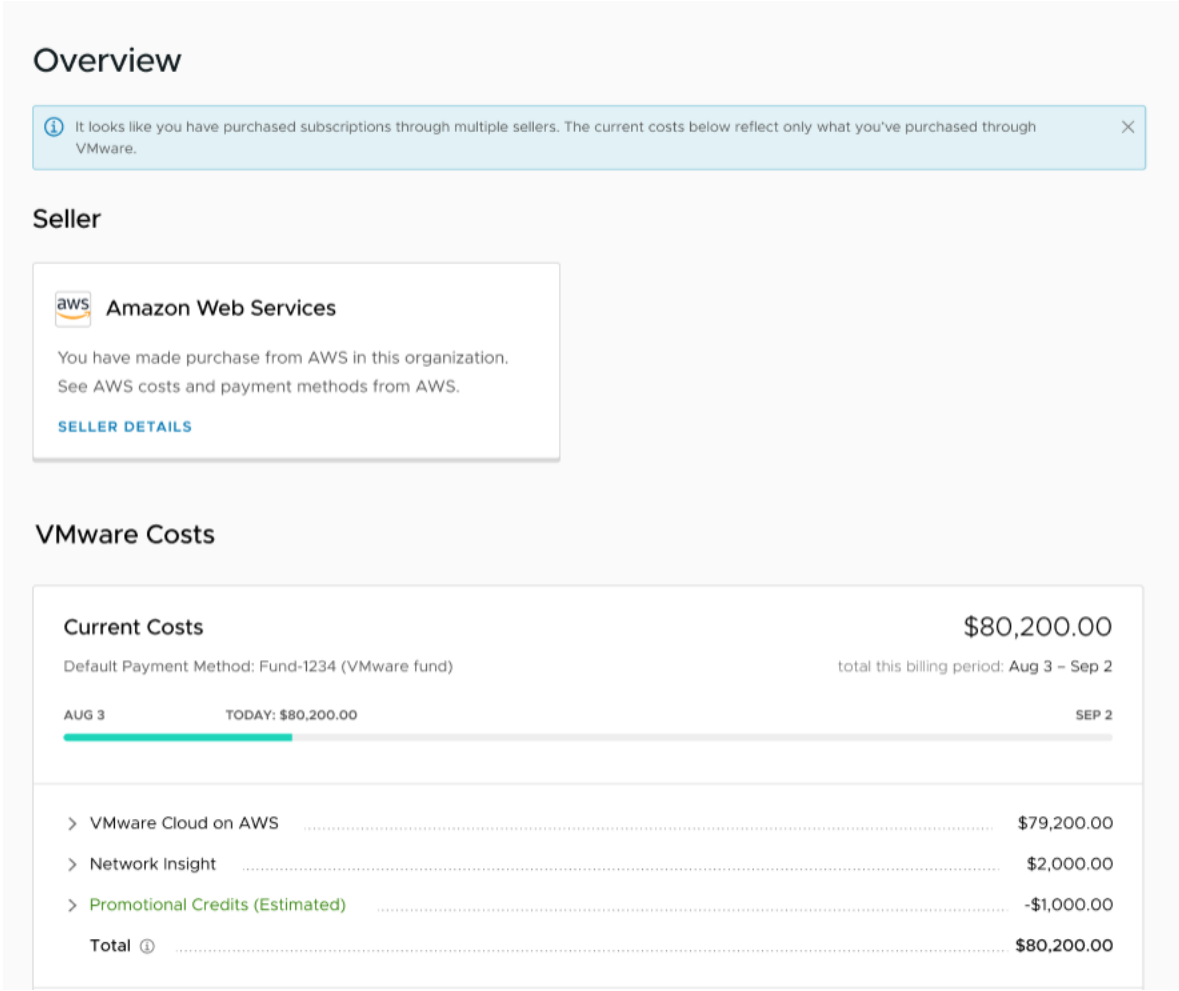
Le Informazioni sul venditore sono disponibili solo se l'Organizzazione dispone di servizi e sottoscrizioni acquistati da uno o più partner VMware.

Ogni file nell'Organizzazione è rappresentato da un riquadro separato.

#### Procedura

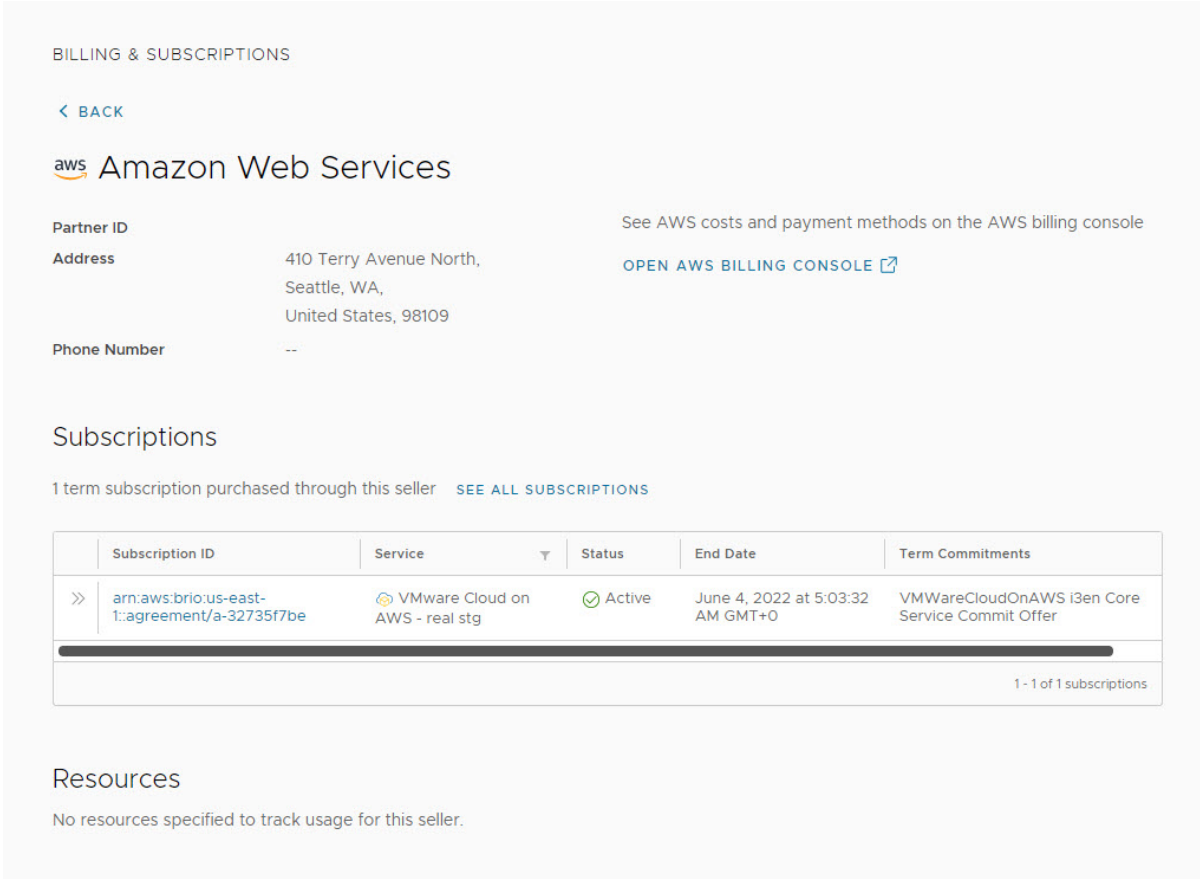
1. Accedere a console di Cloud Services e selezionare **Fatturazione e sottoscrizioni > Panoramica**.

   La sezione **Venditori** include i venditori da cui l'Organizzazione ha acquistato i servizi. Ad esempio, se un'Organizzazione ha acquistato servizi da VMware e Amazon Web Services, verranno visualizzati due venditori.




2 Per visualizzare i servizi e le sottoscrizioni acquistati da qualsiasi partner VMware nell'Organizzazione, fare clic sul link **Dettagli venditore** nel rispettivo riquadro.

Si apre la pagina dei dettagli del venditore.




3 Per visualizzare i costi e i metodi di pagamento associati a questo venditore, fare clic sul link alla relativa console di fatturazione.

4 Per visualizzare i dettagli di una sottoscrizione acquistata da questo venditore, fare clic sul link dell' ID sottoscrizione.

   Viene aperta la pagina dei dettagli della sottoscrizione in cui è possibile visualizzare ulteriori dettagli, come impegni di durata prestabilita, date di inizio e fine della sottoscrizione, metodo di pagamento, cronologia delle sottoscrizioni e così via.

### Operazioni successive

Se VMware non figura come venditore nell'Organizzazione, scoprire Come aggiungere VMware come venditore in modo da poter acquistare direttamente i servizi cloud.

## Come registrare il codice del contratto del venditore partner in VMware Cloud Services

Quando si acquista una sottoscrizione tramite un venditore partner non VMware, l'ordine potrebbe contenere sconti. In qualità di utente **Proprietario dell'Organizzazione**, è necessario registrare il codice del contratto fornito dal venditore partner in console di Cloud Services dopo aver eseguito l'onboarding del servizio nell'Organizzazione.

Associando il codice del contratto al profilo del venditore in VMware Cloud Services, si fa in modo che gli sconti dell'ordine vengano applicati nella fattura.

Prerequisiti

- Si dispone del ruolo di **Proprietario dell'Organizzazione** all'interno dell'Organizzazione.
- Si dispone del numero di contratto per la sottoscrizione acquistata tramite il venditore partner.
- È stato eseguito l'onboarding del servizio e il venditore fa parte dell'Organizzazione.

Procedura

1. Accedere a console di Cloud Services e selezionare **Fatturazione e sottoscrizioni > Panoramica**.

   La sezione **Venditori** della pagina include i venditori da cui l'Organizzazione ha acquistato i servizi.
2. Fare clic sul collegamento **Aggiungi contratto** nel riquadro o nella pagina dei dettagli del venditore.
3. Nella finestra popup che viene visualizzata, digitare il numero di contratto, quindi fare clic su **Invia**.

Risultati

Il codice del contratto è ora associato all'Organizzazione e vengono applicati tutti gli sconti correlati.

È inoltre possibile creare autonomamente sottoscrizioni per il servizio correlato.

## Come aggiungere VMware come venditore

Se l'Organizzazione ha acquistato VMware Cloud services da un venditore non VMware, è possibile aggiungere VMware quando si esegue l'onboarding del servizio o in un momento successivo. In questo modo è possibile acquistare VMware Cloud services direttamente da VMware insieme al proprio venditore esistente.

L'aggiunta di VMware come venditore all'Organizzazione significa che è necessario creare un account di fatturazione con VMware e completare il profilo per l'Organizzazione. È possibile creare l'account di fatturazione aggiungendo un indirizzo aziendale per l'Organizzazione e il metodo di pagamento preferito.

Prerequisiti

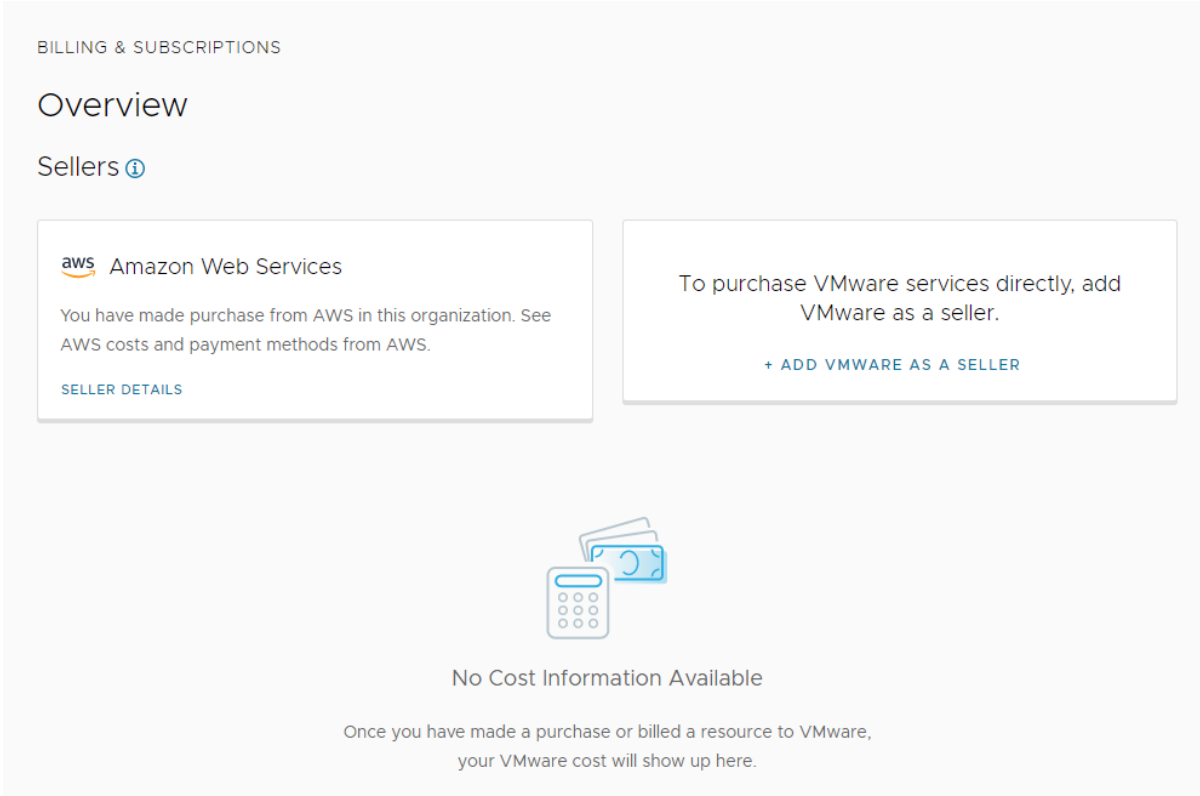
Per aggiungere VMware fra i venditori in console di Cloud Services, è necessario disporre del ruolo di **Proprietario dell'Organizzazione** e l'Organizzazione deve avere acquistato i servizi da un venditore non VMware.

Procedura

1. Accedere a console di Cloud Services con il proprio account My VMware.

2 Andare in **Fatturazione e sottoscrizioni > Panoramica**.

Nella sezione **Venditori** vengono visualizzati i venditori non VMware nell'Organizzazione.




3 Fare clic sul link **Aggiungi VMware come venditore**.

4 Completare il profilo dell'Organizzazione inserendo un indirizzo di fatturazione e selezionando la valuta e il metodo di pagamento.

**Nota** Per modificare la valuta dell'Organizzazione dopo aver creato l'account di fatturazione, è necessario inviare un ticket di supporto.

5 Rivedere e accettare i **Termini di servizio**.

6 Fare clic su **Completato**.

**Risultati**

VMware è ora aggiunto come venditore nell'Organizzazione.

# Come gestire i metodi di pagamento per l'Organizzazione

L'account di fatturazione determina i metodi di pagamento disponibili per l'Organizzazione. È possibile utilizzare fondi, carta di credito o collegare un account con Pagamento con fattura senza limitazioni.

**Fondi**

Per utilizzare uno dei fondi di VMware per i costi della tua Organizzazione, puoi collegarli all'Organizzazione e impostarne uno come metodo di pagamento predefinito. In questo modo, potrai utilizzare lo stesso fondo per tutte le tue Organizzazioni. È possibile utilizzare qualsiasi fondo che sia specifico dell'account VMware Entitlement associato a VMware Cloud services e usi la stessa valuta utilizzata dall'Organizzazione. Per ulteriori informazioni, vedere Pagamento con fondi.

**Carte di credito**

Puoi utilizzare una carta di credito per pagare i tuoi servizi a meno che non vi siano limitazioni per l'utilizzo delle carte di credito nel tuo Paese. Per ulteriori informazioni, vedere Quali sono le limitazioni per l'utilizzo delle carte di credito come metodo di pagamento?.

Se la valuta di pagamento dell'Organizzazione è diversa dalla valuta della carta di credito, potresti incorrere in costi di transazione esterni da parte del provider della carta di credito. Per ulteriori informazioni, vedere Pagamento con carta di credito.

**Account con pagamento con fattura**

Se un ordine di vendita per un nuovo servizio è associato a un account con pagamento con fattura (Pay by Invoice, PBI), viene visualizzato come metodo di pagamento durante l'onboarding del servizio. In questo caso, il metodo di pagamento PBI è limitato e può essere applicato solo alle sottoscrizioni incluse nell'ordine di vendita, ma non può essere aggiunto come metodo di pagamento predefinito all'Organizzazione.

Se si desidera utilizzare un account PBI come metodo di pagamento predefinito per coprire eventuali acquisti, risorse e eccedenze maturate dall'Organizzazione, è necessario attivare PBI senza restrizioni per l'autorizzazione di pagamento per tutti i servizi dell'Organizzazione. L'abilitazione del pagamento PBI senza limitazioni comporta un processo di approvazione offline che può essere avviato inviando una richiesta di supporto. Per ulteriori informazioni, vedere Pagamento con fattura.

È possibile aggiungere all'Organizzazione tutti i metodi di pagamento desiderati, ma solo uno può essere impostato come metodo di pagamento predefinito.

## Come aggiungere un nuovo metodo di pagamento

In qualità di utente **Proprietario dell'Organizzazione**, è possibile aggiungere nuovi metodi di pagamento all'Organizzazione. I metodi di pagamento definiti a livello dell'Organizzazione diventano disponibili per tutti gli utenti **proprietari dell'Organizzazione**.

**Procedura**

1. Aprire console di Cloud Services e andare in **Fatturazione e sottoscrizioni > Gestisci metodi di pagamento**.
2. Nell'area **Altri metodi di pagamento** della pagina, fare clic su **Aggiungi metodo di pagamento**.

3 Selezionare il tipo di metodo di pagamento da aggiungere.

| Per | Procedere così |
| --- | --- |
| **Collegare account con pagamento tramite fattura** | Selezionare uno o più degli account Pagamento tramite fattura disponibili che si desidera aggiungere e fare clic su **Collega account**.<br><br>**Nota** È possibile aggiungere solo account PBI senza limitazioni come metodi di pagamento a livello dell'Organizzazione. Se l'account PBI che si desidera aggiungere è limitato, è innanzitutto necessario attivare PBI senza limitazioni inviando un ticket di assistenza. |
| **Collegare fondi VMware** | Selezionare il fondo VMware che si desidera aggiungere come metodo di pagamento, quindi fare clic su **Collega fondo**. |
| **Aggiungere una carta di credito** | Aggiungere i dettagli della carta di credito e fare clic su **Aggiungi carta**.<br><br>**Nota** Se si fa clic su **Aggiungi carta di credito e rendi metodo predefinito**, verrà modificato il metodo di pagamento predefinito per l'Organizzazione. L'operazione influirà su tutti i servizi e le sottoscrizioni che utilizzano il metodo di pagamento predefinito. |

## Che cos'è il metodo di pagamento predefinito?

Quando ci si iscrive a VMware Cloud services, si aggiunge il metodo di pagamento che si desidera utilizzare per coprire i costi dell'Organizzazione. Questo metodo di pagamento diventa il metodo di pagamento predefinito per l'Organizzazione e può essere utilizzato da tutti gli utenti **proprietari dell'Organizzazione** al suo interno.

Il metodo di pagamento predefinito sarà applicato a tutti gli acquisti, le risorse e le eccedenze nell'Organizzazione, a meno che non si specifichi un metodo di pagamento diverso per l'acquisto. È possibile aggiungere nuovi metodi di pagamento o modificare il metodo di pagamento predefinito per l'Organizzazione dalla scheda **Fatturazione e sottoscrizioni > Gestisci metodi di pagamento** nella console di Cloud Services.

Come metodi di pagamento nella propria Organizzazione, è possibile aggiungere fondi, carte di credito o collegare un account con Pagamento con fattura senza limitazioni, ma solo uno di essi può essere impostato come metodo di pagamento predefinito.

Quando si configura l'Organizzazione, l'indirizzo dell'Organizzazione determina la valuta in cui si effettuano i pagamenti per i servizi dell'Organizzazione. Per ulteriori informazioni sui metodi di pagamento e sulla valuta, vedere Come viene stabilita la valuta di pagamento.

Quando si sottoscrivono servizi aggiuntivi, si acquistano componenti aggiuntivi e si applicano impegni alla propria Organizzazione, l'ordine di vendita può determinare un metodo di pagamento diverso per la sottoscrizione o il contratto di termine che si applica solo a tale acquisto specifico. In seguito è possibile modificare il metodo di pagamento per una sottoscrizione. Per ulteriori informazioni, vedere Come modificare il metodo di pagamento della sottoscrizione.

## Come modificare il metodo di pagamento predefinito dell'Organizzazione

In qualità di utente **Proprietario dell'Organizzazione**, è possibile modificare il metodo di pagamento predefinito dell'Organizzazione.

Tutti i metodi di pagamento disponibili per l'Organizzazione sono elencati nella sezione **Altri metodi di pagamento** della pagina **Gestisci metodi di pagamento** in console di Cloud Services. Se si desidera modificare il metodo di pagamento predefinito dell'Organizzazione con un nuovo metodo di pagamento non elencato, è innanzitutto necessario aggiungere il metodo di pagamento.

### Procedura

1. Aprire console di Cloud Services e andare in **Fatturazione e sottoscrizioni > Gestisci metodi di pagamento**.
2. Nell'area **Metodo di pagamento predefinito** della pagina, fare clic su Modifica metodo di pagamento predefinito.
3. Dall'elenco dei metodi di pagamento disponibili visualizzati, selezionare il metodo di pagamento che si desidera utilizzare.
4. Fare clic su **Conferma**.

   Il nuovo metodo di pagamento predefinito viene attivato immediatamente.

## Come modificare il metodo di pagamento della sottoscrizione

Quando si esegue l'onboarding di un nuovo servizio nell'Organizzazione o si aggiunge una nuova sottoscrizione a un servizio esistente, è possibile selezionare il metodo di pagamento predefinito o aggiungere un metodo di pagamento diverso per la nuova sottoscrizione. È possibile modificare in seguito il metodo di pagamento per qualsiasi sottoscrizione nell'Organizzazione.

La modifica del metodo di pagamento per una sottoscrizione attuale non influisce sul metodo di pagamento predefinito per l'Organizzazione. Il metodo di pagamento predefinito verrà comunque applicato ad altri acquisti e risorse che lo stanno utilizzando. Il metodo di pagamento appena impostato verrà utilizzato solamente per il pagamento della sottoscrizione attuale finché non viene modificato da un utente **Proprietario dell'Organizzazione**.

### Procedura

1. Aprire console di Cloud Services e andare in **Fatturazione e sottoscrizioni > Sottoscrizioni**.

2 Nell'elenco delle sottoscrizioni dell'Organizzazione fare clic sul link **ID sottoscrizione** di quella che si desidera modificare.

   Si apre la pagina dei **Dettagli sottoscrizione**.

3 Nell'area **Metodo di pagamento** della pagina, fare clic su **Modifica**.

4 Nell'elenco dei metodi di pagamento disponibili nell'Organizzazione, selezionare il nuovo metodo di pagamento per la sottoscrizione.

5 Fare clic su **Conferma**.

#### Risultati

La pagina dei dettagli della sottoscrizione si aggiorna per visualizzare il nuovo metodo di pagamento selezionato.

## Pagamento con fattura

L'utente **Proprietario dell'Organizzazione** può cambiare il metodo di pagamento predefinito per l'Organizzazione in Pagamento con fattura (PBI) se è attivato il PBI illimitato. L'abilitazione del pagamento PBI senza limitazioni comporta un processo di approvazione offline che può essere avviato inviando una richiesta di supporto.

Una volta attivato, PBI può essere applicato come metodo di pagamento predefinito per tutti i servizi e le sottoscrizioni nell'Organizzazione. È possibile applicare PBI illimitato anche come metodo di pagamento per le sottoscrizioni correnti.

#### Procedura

1 In console di Cloud Services, selezionare **Centro di assistenza** e fare clic su **Crea richiesta di assistenza**.

2 Nella casella di testo **Categoria**, selezionare **VMware Cloud Services - Fatturazione e utilizzo**.

3 Nella casella di testo **Oggetto** immettere **`Attiva PBI illimitato`**.

4 Immettere i dettagli della richiesta di assistenza e fare clic su **Crea richiesta di assistenza**.

   Seguirà contatto da parte di un rappresentante di VMware Cloud Services per fornire tutte le informazioni di cui alla richiesta. Quando l'opzione PBI illimitato è attivata, si riceverà una notifica.

## Pagamento con carta di credito

VMware Cloud services supportano il pagamento con varie carte di credito. È possibile utilizzare le carte di credito MasterCard, VISA, American Express, Discover, JCB, Diners Club personali o aziendali. È inoltre possibile utilizzare carte di debito MasterCard, VISA o American Express.

Se si desidera utilizzare una carta di credito per pagare i propri servizi:

- L'entità delle transazioni è determinato dal limite della carta di credito e dal gestore dei pagamenti. L'importo massimo spendibile in una singola transazione è di $ 25.000. Per ulteriori informazioni sul limite del credito relativo alla propria carta, rivolgersi alla banca emittente.
- L'indirizzo dell'Organizzazione determina la valuta in cui vengono addebitati i pagamenti. Per un elenco dei paesi e delle relative valute, vedere Come viene stabilita la valuta di pagamento.
- L'uso delle carte di credito presenta specifiche Quali sono le limitazioni per l'utilizzo delle carte di credito come metodo di pagamento? in base all'indirizzo dell'Organizzazione e all'indirizzo di fatturazione della carta di credito.

  **Importante** Se l'indirizzo di fatturazione dell'Organizzazione si trova in un paese membro dello Spazio Economico Europeo (SEE) o in un paese cooperante, i pagamenti con carta di credito sono interessati dalla seconda direttiva sui servizi di pagamento dell'Unione Europea (Direttiva 2015/2366 nota come "PSD2"). La Direttiva PSD2 richiede l'autenticazione forte del cliente (SCA) per le transazioni elettroniche tramite un'autenticazione a due fattori. Quando richiesto, la richiesta di autenticazione forte del cliente (SCA) verrà visualizzata durante il flusso di pagamento e chiederà di fornire informazioni di sicurezza aggiuntive, che verranno quindi verificate dalla banca o dall'emittente della carta.

- Quando si aggiunge una carta di credito come metodo di pagamento, verrà effettuato un controllo di validità della carta senza alcun addebito. Un controllo di validità potrebbe includere una richiesta di pre-autorizzazione da parte dell'istituto di credito interessato. Sull'estratto conto potrebbe essere presente una richiesta di autorizzazione in sospeso di $ 1,00 o importo equivalente. La pre-autorizzazione non rappresentra un costo e non viene addebitato alcun importo sul conto.

È possibile aggiungere una carta di credito come metodo di pagamento quando si esegue l'onboarding di un servizio cloud o in un secondo momento scegliendo **Fatturazione e sottoscrizioni > Gestisci metodi di pagamento** in console di Cloud Services.

Consultare Come modificare il metodo di pagamento predefinito dell'Organizzazione per reperire ulteriori informazioni.

## Quali sono le limitazioni per l'utilizzo delle carte di credito come metodo di pagamento?

Per motivi di rischio e di frode, possono essere applicate alcune limitazioni all'uso delle carte di credito come metodo di pagamento. Queste si basano sull'indirizzo della tua Organizzazione o sull'indirizzo di fatturazione della tua carta di credito.

### Elenco dei paesi in cui si applicano le limitazioni per l'utilizzo delle carte di credito

Se il paese dell'utente è soggetto a limitazioni per l'utilizzo delle carte di credito, il metodo di pagamento verrà disattivato in VMware Cloud Services.

| Non è possibile utilizzare una carta di credito come metodo di pagamento se... | |
|---|---|
| L'indirizzo dell'Organizzazione si trova in uno di questi paesi: | Afghanistan, Antille olandesi, Angola, Bosnia-Erzegovina, Bangladesh, Burkina Faso, Bahrain, Brasile, Bielorussia, Camerun, Cina, Cuba, Capo Verde, Cipro, Eritrea, Isole Falkland, Guiana francese, Guadalupa, Guam, Haiti, Isola di Man, Iraq, Iran, Corea, Kuwait, Laos, Mongolia, Mali, Martinica, Montserrat, Messico, Nigeria, Nepal, Territori palestinesi occupati, Sudan, Senegal, Siria, Turkmenistan, Timor Est, Ucraina, Stato della Città del Vaticano, Venezuela, Mayotte, Zimbabwe. |
| L'indirizzo di fatturazione della carta di credito si trova in uno di questi paesi: | Afghanistan, Antille Olandesi, Angola, Antartide, Isole Aland, Bosnia ed Erzegovina, Bangladesh, Burkina Faso, Bahrain, Saint Barthelemy, Bonaire, Sint Eustatius e Saba, Brasile, Isola Bouvet, Bielorussia, Cocos, Repubblica Democratica del Congo, Repubblica Centrafricana , Camerun, Cina, Cuba, Capo Verde, Curacao, Isole Natale, Cipro, Sahara occidentale, Eritrea, Isole Falkland, Guyana francese, Guadalupa, Georgia del Sud e Isole Sandwich meridionali, Guam, Hong Kong, Isole Heard e McDonald, Haiti , Isola di Man, India, Territorio britannico dell'Oceano Indiano, Iraq, Kiribati, Corea, Kuwait, Laos, Lituania, Lussemburgo, Lettonia, Saint Martin, Mali, Montserrat, Messico, Malesia, Norfolk, Isola, Nigeria, Norvegia, Nepal, Nauru , Niue, Pitcairn, Territori palestinesi occupati, Ruanda, Sudan, Svezia, Singapore, Svalbard e Jan Mayen, Senegal, Somalia, Sud Sudan, Sao Tome e Principe, Siria, Ciad, Territori francesi australi, Thailandia, Tokelau, Turkmenistan, Timor orientale , Turchia, Tuvalu, Isole Minori Esterne degli Stati Uniti, Stato della Città del Vaticano, Venezuela, Mayotte, Zimbabwe |

## Pagamento con i crediti promozionali

Se si dispone di crediti promozionali per qualsiasi VMware Cloud services, è possibile applicarli a una delle Organizzazioni e riscattarli sui costi mensili dell'Organizzazione.

I crediti promozionali possono essere specifici del servizio, il che significa che è possibile utilizzarli sui costi mensili di un servizio specifico, di un gruppo di servizi o applicarli a tutti i servizi. Prendere nota della data di scadenza del credito e riscattarlo prima della scadenza.

I crediti promozionali possono essere riscattati in una qualsiasi delle valute supportate dai VMware Cloud Services. I crediti promozionali a volte vengono offerti quando si esegue l'onboarding di uno dei nostri servizi per la prima volta. Questi crediti vengono riscattati per l'utente durante l'onboarding del servizio.

Procedura

1 In console di Cloud Services, fare clic su **Fatturazione e sottoscrizioni > Crediti promozionali**.

   Tutti i crediti promozionali che possono essere applicati nell'Organizzazione vengono visualizzati nella scheda **Crediti disponibili**.

2 Per riscattare un credito promozionale, fare clic sul link **Attiva** nel riquadro dei dettagli.

   Il credito verrà riscattato durante il successivo periodo di fatturazione. È possibile controllare il saldo del credito promozionale in qualsiasi momento accedendo a **Fatturazione e sottoscrizioni > Crediti promozionali > Crediti attivati**.

## Informazioni importanti sui fondi VMware

I fondi VMware sono un metodo di pagamento specifico di VMware che può essere utilizzato per acquistare servizi o prodotti. Ogni fondo è costituito da uno o più depositi.

Quando si desidera aggiungere "denaro" al fondo, è possibile rivolgersi al servizio commerciale e acquistare un nuovo deposito. Un deposito è costituito da "crediti", che rappresentano il denaro spendibile per servizi e prodotti di VMware.

È possibile visualizzare i dettagli e gestire le impostazioni dei fondi collegati tramite la piattaforma di gestione dei fondi nel portale di VMware Connect, che richiede autorizzazioni di accesso. Per ulteriori informazioni, vedere la panoramica delle pagine dei fondi, dettagli dei fondi e navigazione.

Per utilizzare i fondi VMware per pagare i servizi cloud e le sottoscrizioni, è necessario collegare ciascun fondo come metodo di pagamento all'Organizzazione di VMware Cloud services. I fondi possono essere collegati come metodo di pagamento predefinito o un metodo di pagamento una tantum per le Organizzazioni e le sottoscrizioni. Possono inoltre essere utilizzati per pagare le fatture in sospeso direttamente da console di Cloud Services. Per pagare i costi dell'Organizzazione con i fondi collegati, tali fondi devono avere un saldo positivo e includere una quantità di "denaro" sufficiente.

Si tenga presente che per collegare un fondo in console di Cloud Services:

- È necessario disporre del ruolo di **Proprietario dell'Organizzazione** in cui si desidera collegare il fondo.
- Solo i fondi inclusi nell'account VMware Entitlement possono essere associati all'Organizzazione VMware Cloud services.
- La valuta e l'unità di vendita del fondo devono corrispondere a quelle dell'Organizzazione.

Se un fondo collegato utilizzato come metodo di pagamento predefinito nell'Organizzazione è esaurito, scade o è orfano, il fondo deve essere sostituito con un altro fondo, noto come fondo di sopravvivenza, o con un metodo di pagamento diverso. I fondi orfani sono gruppi di fondi vuoti che interrompono i flussi di pagamento e devono essere sostituiti immediatamente.

Per consentire ai **proprietari dell'Organizzazione** di gestire i propri fondi in modo tempestivo, VMware Cloud Services invia tramite e-mail e nell'app notifiche sullo stato e le modifiche dei fondi nell'Organizzazione. Per ulteriori informazioni, vedere Come gestire i fondi VMware in VMware Cloud Services.

## Pagamento con fondi

In qualità di utente **Proprietario dell'Organizzazione** è possibile utilizzare i fondi VMware collegati per pagare i costi dei servizi. Oltre a utilizzare i fondi come metodo di pagamento predefinito nella propria Organizzazione, è possibile pagare le fatture in sospeso direttamente da console di Cloud Services.

| Operazione da eseguire | Procedere così... |
| --- | --- |
| Impostare un fondo VMware collegato come metodo di pagamento predefinito nell'Organizzazione. | Vedere Come modificare il metodo di pagamento predefinito dell'Organizzazione. |
| Impostare un fondo VMware collegato come metodo di pagamento per una sottoscrizione attiva. | Vedere Come modificare il metodo di pagamento della sottoscrizione. |

| Operazione da eseguire | Procedere così... |
| --- | --- |
| Pagare una fattura in sospeso per un'eccedenza o un impegno a termine. | 1 Accedere a console di Cloud Services e passare a **Fatturazione e sottoscrizioni > Fatture ed estratti conto > Fatture**.<br>2 Individuare la fattura non pagata che si desidera pagare e fare clic sull'icona con i puntini di sospensione verticali ⋮.<br>3 Fare clic sul collegamento **Paga ora**.<br>4 Nella finestra pop-up che viene aperta, rivedere i dettagli della fattura e selezionare il fondo che si desidera utilizzare per questo pagamento.<br>**Nota** L'elenco a discesa **Metodo di pagamento** include solo i fondi collegati all'Organizzazione che hanno un saldo positivo.<br>5 Fare clic su **Paga ora**.<br>Il pagamento viene inviato e la pagina **Fatture** viene aggiornata con lo stato `In Progress` (In Progress) accanto alla fattura che è stata pagata.<br>Al completamento della transazione, si riceverà una notifica tramite e-mail. La transazione può essere completata immediatamente o richiedere alcune ore. Il saldo della fattura verrà aggiornato solo dopo il completamento della transazione.<br>È possibile effettuare un pagamento aggiuntivo mentre è in corso il primo pagamento parziale. Nella fattura aggiornata verranno applicati entrambi i pagamenti e un saldo aggiornato. |
| Per visualizzare la cronologia dei pagamenti per le fatture pagate con fondi tramite console di Cloud Services | 1 Passare a **Fatturazione e sottoscrizioni > Fatture ed estratti conto > Fatture**.<br>2 Individuare la fattura di cui si desidera controllare i pagamenti e quindi fare clic sull'icona con i puntini di sospensione verticali ⋮.<br>3 Fare clic sul collegamento **Cronologia pagamenti**.<br>La sezione **Cronologia pagamenti** include il metodo di pagamento, lo stato e l'importo pagato per la fattura selezionata. |

## Come gestire i fondi VMware in VMware Cloud Services

In qualità di **Proprietario dell'Organizzazione** è possibile collegare e scollegare i fondi VMware come metodo di pagamento nell'Organizzazione in console di Cloud Services. Solo i fondi

collegati all'Organizzazione possono essere impostati come metodo di pagamento predefinito o utilizzati per pagare le fatture in sospeso per le eccedenze o gli impegni a termine.

**Nota** In console di Cloud Services viene gestito solo il collegamento dei fondi all'Organizzazione. I fondi effettivi vengono gestiti tramite il portale di VMware Connect, che richiede autorizzazioni di accesso.

Le notifiche relative alle modifiche apportate ai fondi VMware nell'Organizzazione vengono inviate automaticamente tramite e-mail e nell'app a tutti gli utenti **proprietari dell'Organizzazione** e ai **membri dell'Organizzazione** che dispongono del ruolo **Fatturazione in sola lettura** nell'Organizzazione.

La seguente tabella descrive come utilizzare il metodo di pagamento con fondi VMware nell'Organizzazione di VMware Cloud Services.

| Operazione da eseguire | Procedere così... |
| --- | --- |
| Per collegare un fondo VMware come metodo di pagamento nell'Organizzazione. | È possibile utilizzare qualsiasi fondo che sia specifico dell'account VMware Entitlement associato a VMware Cloud services e usi la stessa valuta utilizzata dall'Organizzazione.<br>1 Accedere a console di Cloud Services e passare a **Fatturazione e sottoscrizioni > Gestisci metodi di pagamento**.<br>2 Nell'area **Altri metodi di pagamento** della pagina, fare clic su **Aggiungi metodo di pagamento**.<br>3 Selezionare **Collega fondi VMware** e fare clic su **Continua**.<br>4 Nell'elenco dei fondi VMware disponibili che viene visualizzato, selezionare il fondo che si desidera collegare come metodo di pagamento nell'Organizzazione.<br>**Nota** In questo elenco verranno visualizzati solo i fondi VMware collegati all'account VMware.<br>5 Collega il fondo selezionato:<br>■ Per collegare il fondo come metodo di pagamento predefinito nell'Organizzazione, fare clic su **Collega il fondo e rendilo predefinito**.<br>■ Per collegare il fondo e renderlo disponibile come metodo di pagamento nell'Organizzazione, fare clic su **Collega fondi**. |
| Per scollegare un fondo già collegato come metodo di pagamento nella propria Organizzazione. | I metodi di pagamento nell'Organizzazione sono disponibili per tutti gli utenti **proprietari dell'Organizzazione**. Se si desidera rimuovere un fondo attivo dall'Organizzazione, eseguire questa operazione:<br>1 Aprire la pagina **Gestisci metodi di pagamento**.<br>2 Fare clic sull'icona con i puntini di sospensione orizzontali (⋯) accanto al nome del fondo e selezionare **Scollega fondo**. |

| Operazione da eseguire | Procedere così... |
| --- | --- |
| Per visualizzare i dettagli di un fondo già collegato come metodo di pagamento nell'Organizzazione. | 1 Passare a **Fatturazione e sottoscrizioni > Gestisci metodi di pagamento**.<br>2 Fare clic sull'icona dei tre puntini orizzontali (***) accanto al nome del fondo e selezionare **Visualizza dettagli su MyVMware**.<br>Questo apre il sito Web di VMware Customer Connect in cui è possibile visualizzare i dettagli del fondo dopo aver effettuato l'accesso all'account VMware. |
| Per gestire un fondo scaduto già collegato come metodo di pagamento predefinito nell'Organizzazione. | Se si utilizza un fondo come metodo di pagamento predefinito nell'Organizzazione, si riceve una notifica tramite e-mail prima della data di scadenza. Per un fondo in attesa di scadenza, è possibile eseguire una delle seguenti azioni:<br>■ Modificare il metodo di pagamento predefinito per l'Organizzazione in un altro fondo attivo collegato nell'Organizzazione.<br>■ Modificare il metodo di pagamento predefinito in carta di credito o PBI.<br>■ Se è presente un altro fondo attivo non collegato all'Organizzazione, è possibile collegarlo all'Organizzazione e quindi impostarlo come metodo di pagamento predefinito. |
| Per gestire un fondo esaurito | Se nel fondo che si sta utilizzando come metodo di pagamento predefinito o per il pagamento di una fattura non è presente "denaro" sufficiente per pagare l'intero importo della fattura, la fattura verrà visualizzata come parzialmente pagata. Per pagare il costo rimanente, è necessario utilizzare un altro fondo con "crediti" sufficienti o un metodo di pagamento diverso. |
| Per gestire un fondo orfano collegato come metodo di pagamento predefinito nell'Organizzazione | Un fondo può diventare orfano per uno dei seguenti motivi:<br>■ Modifica del proprietario del fondo<br>■ Unione del fondo<br>■ Modifica del **Proprietario dell'Organizzazione**<br>■ Il **Proprietario dell'Organizzazione** non è più un utente del fondo<br>Quando ciò si verifica, VMware Cloud Services informa gli utenti **proprietari dell'Organizzazione** del fondo che è diventato orfano e sostituisce il fondo orfano con un fondo di sopravvivenza. A tutti gli utenti **proprietari dell'Organizzazione** viene inviata un'ulteriore notifica relativa al metodo di pagamento predefinito aggiornato. Se sono necessarie ulteriori modifiche del pagamento, vedere Come gestire i metodi di pagamento per l'Organizzazione. |

# Come utilizzare le sottoscrizioni e gli impegni di VMware Cloud Services

Le sottoscrizioni VMware Cloud services consentono di risparmiare denaro impegnandosi ad acquistare una determinata quantità di capacità per un periodo predefinito di uno o tre anni a una tariffa ridotta o negoziata.

È possibile utilizzare VMware Cloud services su richiesta o acquistando sottoscrizioni per un periodo di 1 o 3 anni. L'utilizzo del servizio su richiesta viene addebitato a una tariffa più elevata, mentre le sottoscrizioni ai servizi vengono addebitate a una tariffa ridotta. Le sottoscrizioni si acquistano tramite il Programma di acquisto sottoscrizioni o Pagamento con fattura.

È possibile acquistare e utilizzare impegni multipli per ciascun servizio della sottoscrizione. Le date di inizio e fine di ogni impegno possono variare. L'ordine di acquisto indica la capacità, la durata e il prezzo negoziato dell'impegno.

VMware Cloud Services fattura in base ai termini delineati nell'impegno per la sottoscrizione al servizio.

Gli eventuali utilizzi aggiuntivi non coperti dai termini dell'impegno vengono addebitati in base ai prezzi su richiesta che sono stati concordati al momento della firma con il servizio.

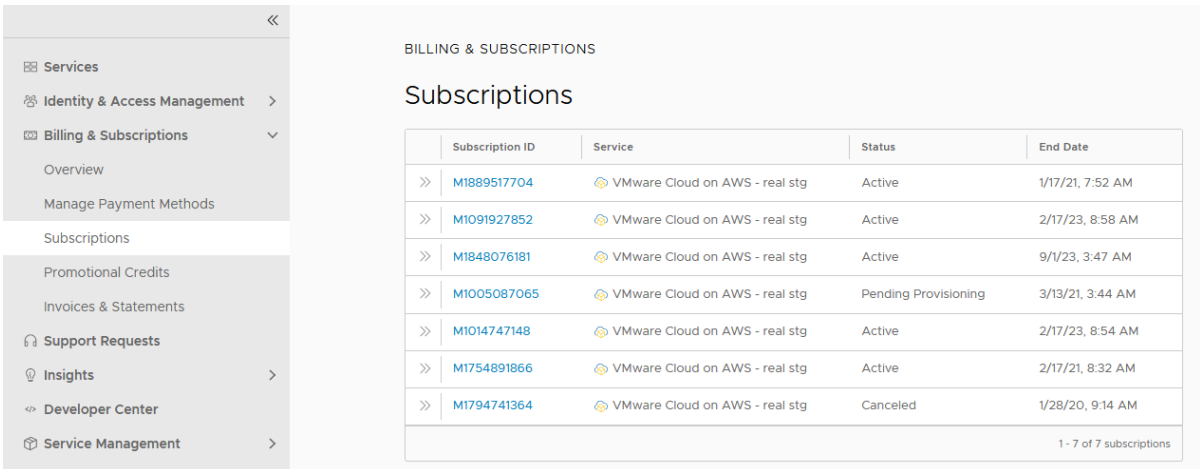
## Come visualizzare i dettagli delle sottoscrizioni per i servizi nell'Organizzazione

Per visualizzare i dettagli delle sottoscrizioni nell'Organizzazione, è necessario disporre di un ruolo di **Proprietario dell'Organizzazione** o di **Membro dell'Organizzazione** con autorizzazioni di **sola lettura delle fatturazioni**.

### Procedura

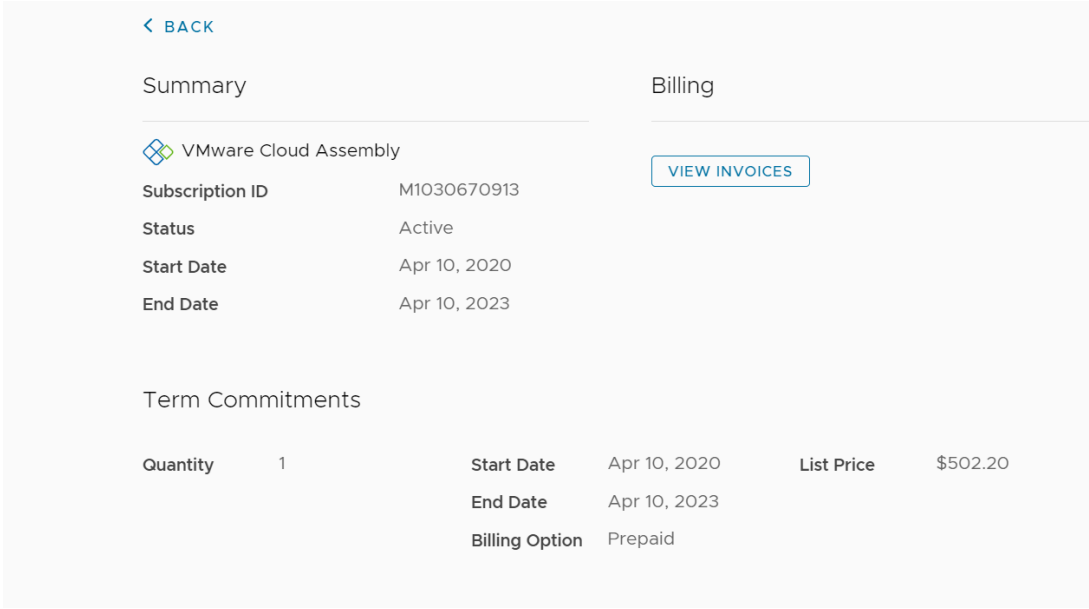
1 In console di Cloud Services passare a **Fatturazione e sottoscrizioni > Sottoscrizioni**.

La tabella che verrà visualizzata include informazioni su tutte le sottoscrizioni dell'Organizzazione. Nella tabella sono elencati gli ID di sottoscrizione, i VMware Cloud services per cui è stata acquistata la sottoscrizione e i termini della sottoscrizione.



2 Per visualizzare informazioni più dettagliate per una sottoscrizione specifica, individuare la sottoscrizione che si desidera visualizzare e fare clic sul collegamento **ID sottoscrizione**.

La pagina che viene aperta mostra ulteriori dettagli relativi alla sottoscrizione e agli impegni rispetto ai termini accettati con la sottoscrizione.




3 (Facoltativo) Per visualizzare e scaricare le fatture, fare clic su **Visualizza fatture** nella sezione **Fatturazione** della pagina.

## Come configurare un impegno

Se si è utente **Proprietario dell'Organizzazione**, contattare il proprio commerciale VMware per negoziare un preventivo e organizzare il pagamento per un impegno.

Una volta completato l'acquisto, riceverai un'email di notifica che indica che il tuo impegno è attivo. Per ogni impegno, è possibile ricevere un'e-mail con un link univoco.

1 Per applicare l'impegno a una delle Organizzazioni correnti o a una nuova Organizzazione fare clic sul link nell'e-mail.

2 Eseguire i passaggi nel workflow di onboarding del servizio.

Per ulteriori informazioni sugli impegni, vedere Perché è necessario applicare degli impegni all'Organizzazione?.

Per ulteriori informazioni sui workflow di onboarding, vedere Come eseguire l'onboarding di un servizio cloud a pagamento acquistato tramite VMware Sales.

# Come acquistare una sottoscrizione

VMware Cloud Services dispone di un'opzione di acquisto della sottoscrizione self-service per i servizi e i venditori selezionati.

**Nota** L'opzione di acquisto della sottoscrizione self-service è attualmente disponibile solo per VMware Tanzu Service Mesh acquistato tramite VMware.

È possibile avviare un ordine di acquisto della sottoscrizione per i servizi elencati sopra nella pagina **Fatturazione e sottoscrizioni > Sottoscrizioni** o dal riquadro dei servizi nel catalogo dei servizi cloud nella console di Cloud Services.

### Prerequisiti

È necessario disporre del ruolo di **Proprietario dell'Organizzazione** in cui si acquista la nuova sottoscrizione.

### Procedura

1. Accedere a console di Cloud Services e passare a **Fatturazione e sottoscrizioni > Sottoscrizioni**.
2. Fare clic su **Crea sottoscrizione**.

   Viene aperto il primo passaggio del workflow **Crea sottoscrizione**.
3. Nella sezione **Seleziona il servizio** del passaggio del workflow **Servizio**, utilizzare i menu a discesa per selezionare il servizio o il bundle di servizi e il venditore presso cui si desidera acquistare la nuova sottoscrizione.
4. Fare clic su **Avanti**.

   Se l'Organizzazione non dispone di un indirizzo valido o non è definito il metodo di pagamento predefinito per l'Organizzazione, il passaggio successivo che si apre è **Dati di fatturazione**.
5. Nel passaggio **Dati di fatturazione** del workflow, specificare l'indirizzo dell'organizzazione e selezionare il metodo di pagamento predefinito.
6. Fare clic su **Avanti**.
7. Nel passaggio **Configurazione** del workflow, selezionare le opzioni di configurazione per la sottoscrizione. In base alla soluzione o al servizio che si sta sottoscrivendo, il passaggio di configurazione della sottoscrizione potrebbe richiedere di selezionare quanto segue:
   - Versione e/o regione.
   - Quantità impegno, frequenza di fatturazione e termine dell'impegno.

   La sezione **Riepilogo dell'ordine** della pagina mostra le informazioni e il costo della sottoscrizione in base all'ultima selezione.
8. Quando si è pronti con la configurazione della sottoscrizione, fare clic su **Salva**.

9 Se si desidera modificare o eliminare la configurazione della sottoscrizione, è possibile farlo utilizzando i pulsanti **Modifica** o **Rimuovi** nella sezione **Offerta** del passaggio **Configurazione**.

10 Per procedere con l'ordine di acquisto, fare clic su **Avanti**.

11 Nella fase finale del workflow, rivedere il riepilogo dell'ordine di acquisto e il riepilogo del pagamento, quindi selezionare un metodo di pagamento.

12 Fare clic su **Crea sottoscrizione**.

13 Nella finestra a comparsa visualizzata, fare clic su **Crea** per confermare l'acquisto.

#### Risultati

Nella schermata viene visualizzata una conferma della richiesta di acquisto dell'ordine della sottoscrizione. L'elaborazione dell'ordine di acquisto e l'attivazione della nuova sottoscrizione potrebbero richiedere un po' di tempo. In seguito, è possibile visualizzare i dettagli della sottoscrizione nella pagina **Sottoscrizioni** dell'organizzazione.

## Come espandere la sottoscrizione

In qualità di **Proprietario dell'Organizzazione**, è possibile espandere la capacità di alcune sottoscrizioni nell'Organizzazione.

**Nota** Al momento, solo VMware Tanzu Service Mesh utilizza questa funzionalità ed è disponibile solo se la sottoscrizione è stata acquistata tramite VMware.

#### Prerequisiti

- È stata acquistata la sottoscrizione che si desidera espandere da VMware.
- Si dispone del ruolo di **Proprietario dell'Organizzazione** all'interno dell'Organizzazione.

#### Procedura

1 Accedere a console di Cloud Services e passare a **Fatturazione e sottoscrizioni > Sottoscrizioni**.

2 Individuare la sottoscrizione che si desidera espandere, fare clic sull'icona con i puntini di sospensione verticali ( ⋮ ) accanto all'ID della sottoscrizione, quindi fare clic su **Espandi**.

3 Immettere la nuova quantità della sottoscrizione e fare clic su **Salva**.

La sezione **Riepilogo dell'ordine** mostra le informazioni e il costo della sottoscrizione in base all'ultima selezione.

4 Se si desidera modificare la quantità selezionata, fare clic su **Modifica** e immettere un nuovo valore.

5 Per confermare l'espansione della sottoscrizione, fare clic su **Avanti**.

6 Nella fase finale del workflow, rivedere il riepilogo dell'ordine di acquisto e il riepilogo del pagamento, quindi selezionare un metodo di pagamento.

7 Fare clic su **Crea sottoscrizione**.

### Risultati

Nella schermata viene visualizzata una conferma della richiesta di acquisto dell'ordine della sottoscrizione. L'elaborazione dell'ordine di acquisto e la modifica della sottoscrizione potrebbero richiedere un po' di tempo. In seguito, è possibile visualizzare i dettagli della sottoscrizione nella pagina **Sottoscrizioni** dell'organizzazione.

## Perché è necessario applicare degli impegni all'Organizzazione?

È possibile acquistare più sottoscrizioni per VMware Cloud Services diversi, nonché più impegni di termine per ogni sottoscrizione. Ogni sottoscrizione può essere utilizzata in un'Organizzazione. Se si dispone di più Organizzazioni VMware Cloud services, è possibile applicare i nuovi impegni acquistati a un'Organizzazione di propria scelta.

Quando si acquista un impegno, l'offerta di vendita indica la capacità, il termine e il prezzo negoziato. In qualità di utente **Proprietario dell'Organizzazione**, l'utente applica l'impegno a un'Organizzazione nuova o esistente una volta completato l'acquisto. A tale scopo, aprire il collegamento per il nuovo impegno e seguire i passaggi nel workflow.

Una volta associato a un'Organizzazione specifica, l'impegno può essere utilizzato dai membri di tale Organizzazione fino a quando il suo termine non scade.

## Come modificare le preferenze di rinnovo della sottoscrizione

L'utente **Proprietario dell'Organizzazione** può gestire i rinnovi per le proprie sottoscrizioni dalla pagina **Dettagli sottoscrizione** di console di Cloud Services.

Ogni sottoscrizione all'interno dell'Organizzazione presenta una preferenza di rinnovo predefinita che può essere modificata fino a 30 giorni prima della scadenza.

**Importante** La pagina **Dettagli sottoscrizione** mostra solo le opzioni delle preferenze di rinnovo supportate dalla sottoscrizione acquistata. Se manca una delle preferenze di rinnovo elencate di seguito, significa che non è attualmente disponibile per la sottoscrizione.

| Se la preferenza di rinnovo è impostata su... | In questo caso... |
|---|---|
| **Rinnovo automatico** | La sottoscrizione verrà rinnovata automaticamente senza alcun input aggiuntivo necessario da parte dell'utente. |
| **Rinnovo manuale** | Un account manager contatterà il cliente prima della data di rinnovo per discutere i dettagli del rinnovo.<br>È inoltre possibile inviare una richiesta di assistenza per informarsi sulle opzioni di rinnovo. |
| È inoltre possibile annullare una sottoscrizione prima che venga rinnovata modificando la preferenza di rinnovo in **Annulla rinnovo**. | È inoltre possibile annullare una sottoscrizione prima che venga rinnovata. In questo caso, l'Organizzazione perde il permesso per la sottoscrizione oltre la data di scadenza. |

### Prerequisiti

È necessario disporre del ruolo di **Proprietario dell'Organizzazione**.

Procedura

1 Accedere a console di Cloud Services, quindi passare a **Fatturazione e sottoscrizioni > Sottoscrizioni**.

2 Nell'elenco di sottoscrizioni visualizzato, fare clic sull'ID della sottoscrizione.

Verrà aperta la pagina **Dettagli sottoscrizione**.

3 Nella sezione **Preferenze di rinnovo** fare clic su **Modifica**.

4 Selezionare una nuova preferenza di rinnovo predefinita per la sottoscrizione e fare clic su **Conferma**.

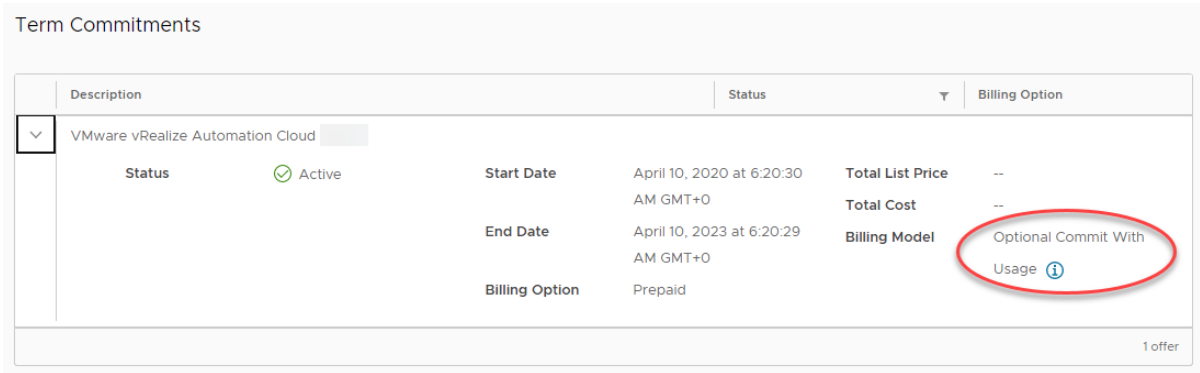
## Che cos'è un modello di fatturazione

VMware Cloud Services utilizza tre diversi modelli di fatturazione. Il modello di fatturazione per la sottoscrizione determina il modo in cui i servizi e gli impegni acquistati e utilizzati all'interno dell'Organizzazione vengono addebitati.

Le informazioni sul modello di fatturazione vengono visualizzate come parte dei dettagli degli **Impegni a termine** per una sottoscrizione.

1 Accedere a console di Cloud Services e andare in **Fatturazione e sottoscrizioni > Sottoscrizioni**.

2 Fare clic sull'ID di una sottoscrizione per aprirne la pagina dei dettagli, quindi espandere la sezione **Impegni a termine**.




**Nota** È possibile visualizzare il modello di fatturazione solo per le sottoscrizioni acquistate tramite VMware.

Nella tabella seguente sono illustrate le differenze tra i tre modelli di fatturazione.

| | Solo impegno | Impegno con uso facoltativo | Impegno con uso obbligatorio |
|---|---|---|---|
| Descrizione: | Per utilizzare il servizio è necessario acquistare le iscrizioni. | Non sono necessarie sottoscrizioni per iniziare a utilizzare il servizio, ma è possibile che si verifichi l'utilizzo su richiesta. | Sarà necessario acquistare le sottoscrizioni per utilizzare il servizio e verrà addebitato l'utilizzo eccedente. |
| Metodo di pagamento predefinito: | Non necessario | Obbligatorio | Non necessario |
| Costo determinato da: | Impegni | Impegni + utilizzo su richiesta (se presente) | Impegni + utilizzo eccedente (se presente) |

# Come funziona il dashboard Gestione utilizzo

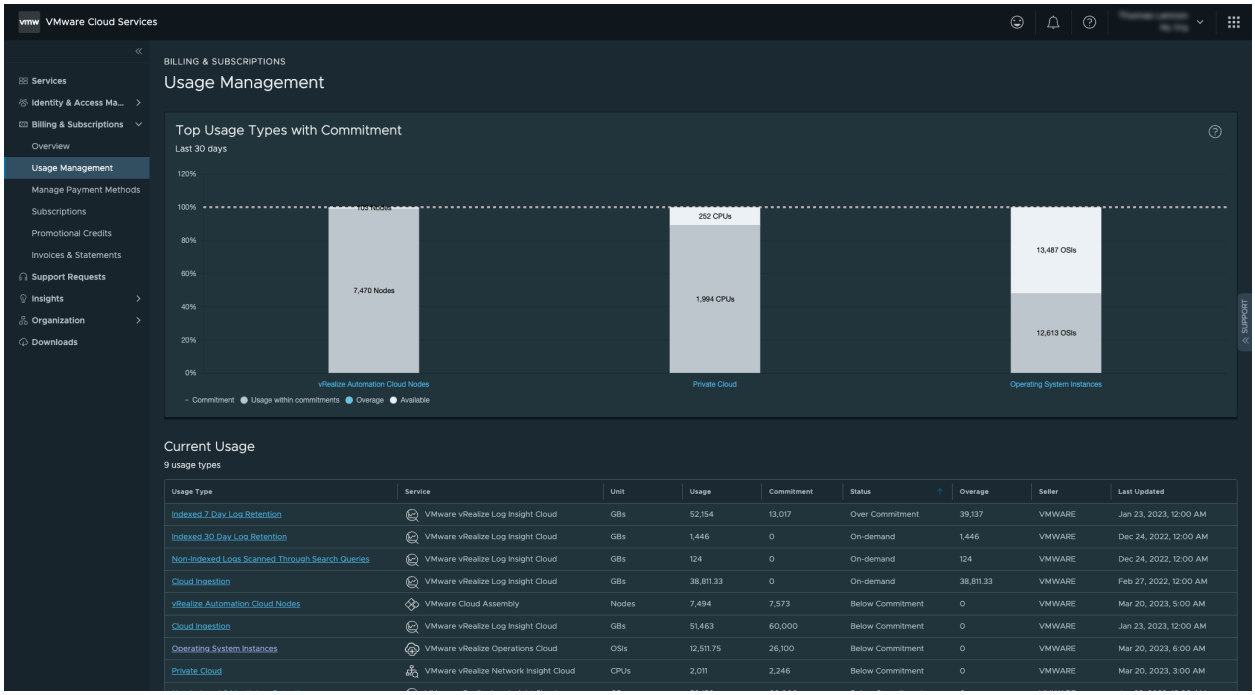
In qualità di utente **Proprietario dell'Organizzazione**, è possibile monitorare il modo in cui i servizi dell'Organizzazione vengono utilizzati nel tempo e in base al tipo di utilizzo tramite il dashboard **Gestione utilizzo** in console di Cloud Services.

**Nota** Gestione utilizzo non è disponibile per tutti i VMware Cloud services. Alcuni dei servizi che attualmente forniscono dati sull'utilizzo sono VMware Cloud on AWS, VMware Aria Operations for Networks, VMware Aria Operations, VMware Aria Operations for Logs, VMware Aria Automation, VMware Cloud Disaster Recovery, VMware Cloud Director VMware Lab Platform.

Nel video seguente è possibile visualizzare una panoramica della funzionalità Gestione utilizzo:

 (Procedura dettagliata di Gestione utilizzo della console di Cloud Services)

È possibile accedere al dashboard **Gestione utilizzo** passando a **Fatturazione e sottoscrizioni > Gestione utilizzo**.

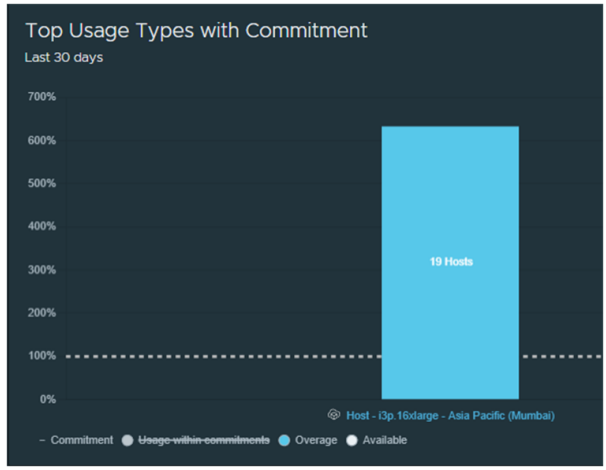
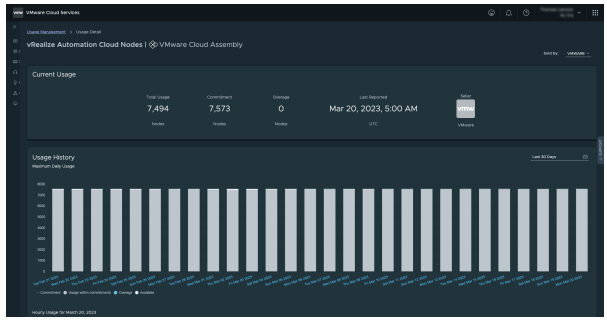



I dati sull'utilizzo sono organizzati in due sezioni: un grafico che include i tipi di utilizzo principale nell'Organizzazione negli ultimi 30 giorni e una tabella con i dettagli sull'utilizzo corrente per tutti i tipi di utilizzo nell'organizzazione.

VMware Cloud services usa molti tipi di utilizzo. Il tipo di utilizzo si basa sul servizio specifico di cui è stato eseguito il provisioning nell'Organizzazione e include le unità utilizzate per misurare la capacità impegnata per il servizio. Le unità più comunemente utilizzate sono Core, Host, vCPU, CPU e OSI. Di seguito sono riportati alcuni esempi di tipi di utilizzo:

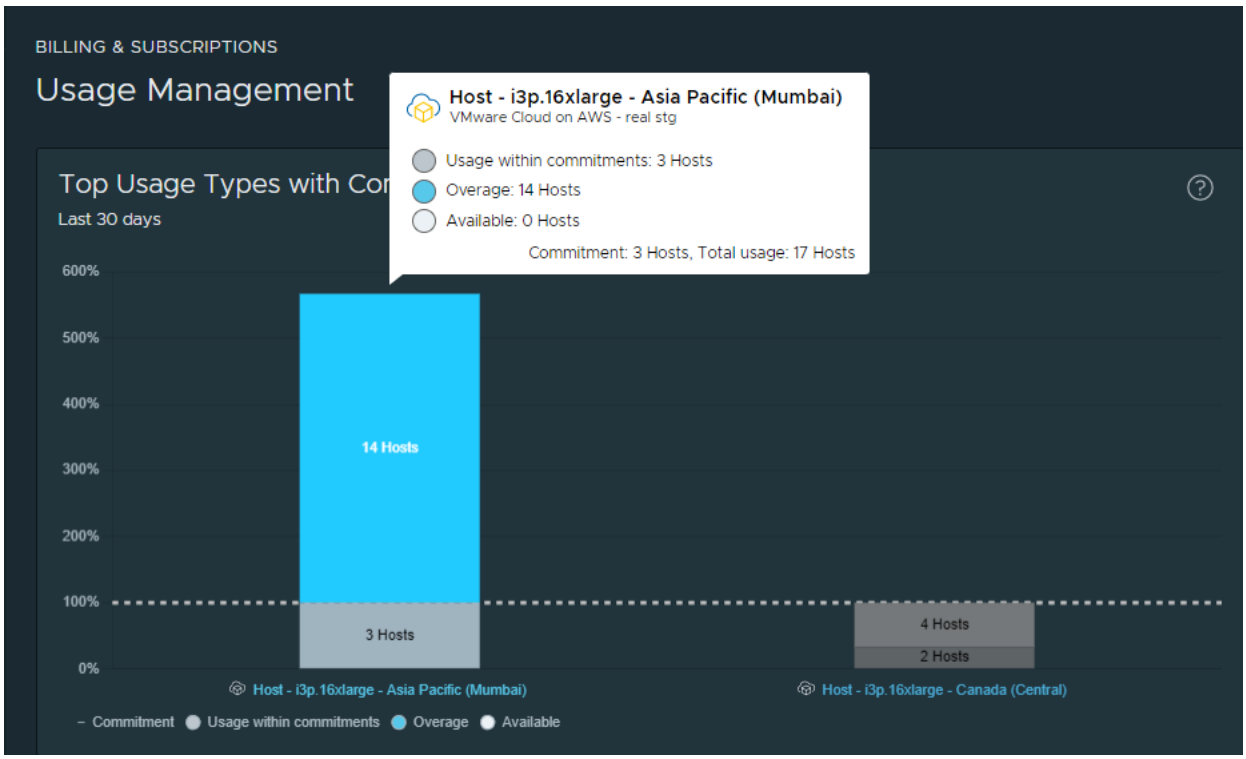
- `Operating System Instances`
- `Cloud Director Cores`
- `Host - r.5metal - Europe (Ireland)`

| Operazione da eseguire | Procedere così... |
|---|---|
| Ulteriori informazioni sui tipi di utilizzo principali. | Vedere Informazioni importanti sul grafico Tipi di utilizzo principale con impegno. |
| Ulteriori informazioni sull'utilizzo corrente. | Vedere Informazioni importanti sulla tabella Utilizzo corrente. |

| Operazione da eseguire | Procedere così... |
| --- | --- |
| Filtrare l'utilizzo in base alla capacità, ad esempio con impegni, eccedenza o impegno disponibile. | Nella sezione **Tipi di utilizzo principale** del dashboard **Gestione utilizzo**, fare clic sull'etichetta sotto il grafico che corrisponde alle informazioni che si desidera escludere dalla visualizzazione.<br>Ad esempio, se si desidera visualizzare solo l'eccedenza per i tipi di utilizzo principali, fare clic sull'etichetta **Utilizzo con impegni**. Quando l'etichetta viene barrata, la visualizzazione viene aggiornata per mostrare solo i tipi di utilizzo in eccesso.<br>  |
| Visualizzazione dell'utilizzo corrente e cronologico per tipo di utilizzo | Fare clic sul link del tipo di utilizzo per cui si desidera visualizzare i dettagli dell'utilizzo corrente e cronologico. Se il tipo di utilizzo si trova nella sezione **Tipi di utilizzo principale con impegno**, il link si trova appena sotto la rispettiva barra del grafico. Se il tipo di utilizzo è elencato nella sezione **Utilizzo corrente**, il link è disponibile nella colonna Tipo di utilizzo.<br>Viene aperta una pagina che mostra la visualizzazione dell'utilizzo corrente e cronologico per il tipo di utilizzo selezionato.<br>  <br>Per ulteriori informazioni sull'utilizzo corrente e cronologico, vedere Informazioni importanti sui dettagli di utilizzo corrente e cronologico. |

## Informazioni importanti sul grafico Tipi di utilizzo principale con impegno

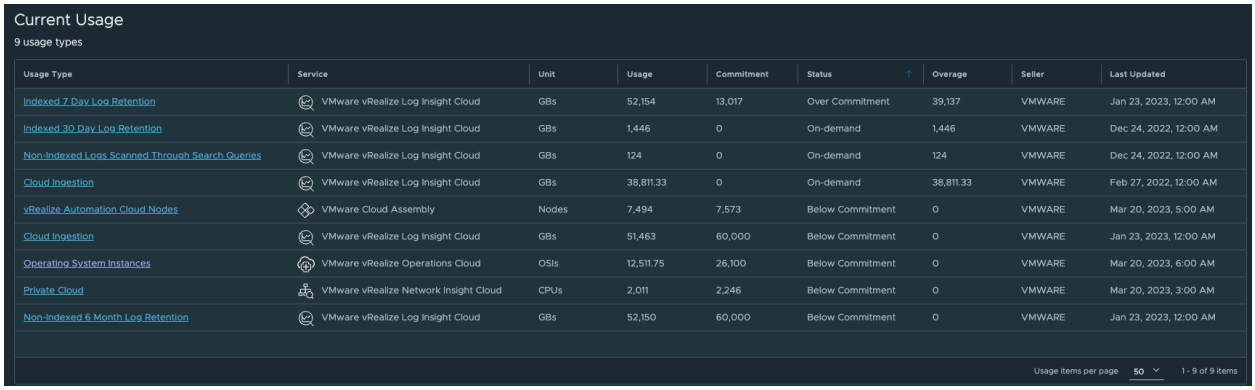
Il grafico **Tipi di utilizzo principale con impegno** del dashboard **Gestione utilizzo** mostra un riepilogo del punteggio elevato di utilizzo dei tipi di utilizzo principale all'interno dell'Organizzazione negli ultimi 30 giorni, ordinati in base alla percentuale di impegno.




L'impegno è il numero di unità acquistate nell'organizzazione tramite la sottoscrizione. La linea orizzontale punteggiata indica un livello di impegno pari al 100%. Le barre che si trovano sotto questa linea indicano un sottoutilizzo per questo servizio e tipo di utilizzo. Le parti blu delle barre indicano che l'impegno è stato superato ed è possibile ridurre l'utilizzo o acquistare ulteriori impegni. Nel grafico, il numero di unità in base a cui l'utilizzo dell'organizzazione ha superato l'impegno viene visualizzato come eccedenza.

## Informazioni importanti sulla tabella Utilizzo corrente

La tabella **Utilizzo corrente** si trova sotto la sezione principale **Tipi di utilizzo principale con impegno** del dashboard **Gestione utilizzo** in console di Cloud Services.




La tabella fornisce dettagli di alto livello sui tipi di utilizzo dei servizi di cui è stato eseguito il provisioning nelle organizzazioni. Ecco una spiegazione dettagliata sulle informazioni che è possibile trovare in ogni colonna della tabella:

| Colonna | Descrizione |
|---|---|
| Tipo di utilizzo | Utilizzo ottenuto confrontando un servizio specifico di cui è stato eseguito il provisioning nell'organizzazione e le unità utilizzate per misurare la capacità impegnata per tale servizio. Ad esempio `Host - r5.metal - US West Oregon`.<br>Il tipo di utilizzo viene visualizzato come link. Se si fa clic sul link, viene aperta una pagina di dettagli che mostra l'utilizzo corrente e cronologico del tipo di utilizzo selezionato. |
| Servizio | Servizi cloud a cui è collegato il tipo di utilizzo specifico. Ad esempio, VMware Cloud on AWS. |
| Unità | Rappresenta l'unità di misurazione per il tipo di utilizzo specifico. Ad esempio Host, Core, GB (storage), IP/EIP, CPU/vCPU e così via. |
| Utilizzo | Rappresenta l'utilizzo effettivo al momento del report: il numero di unità attualmente in uso. |
| Impegno | Numero di unità acquistate tramite sottoscrizioni nell'organizzazione. |
| Stato | Rappresenta un riepilogo dello stato dell'utilizzo. Le opzioni sono:<br>■ Overcommit: quando l'utilizzo supera l'impegno.<br>■ Su richiesta: quando l'utilizzo si riferisce a un tipo di utilizzo senza impegno.<br>■ Conforme all'impegno o Inferiore all'impegno: alcuni servizi non dispongono di dati quando l'utilizzo è conforme o inferiore a un impegno. Questo stato indica che non si sta consumando più di quanto acquistato. Non viene visualizzata la quantità specifica utilizzata. |
| Eccedenza | Rappresenta il valore di utilizzo che supera l'impegno. |

| Colonna | Descrizione |
| --- | --- |
| Venditore | Rappresenta il venditore da cui è stata acquistata la sottoscrizione. Può mostrare un consumo eccessivo che può essere fatturato per l'utilizzo. |
| Ultimo aggiornamento | Rappresenta la data e l'ora dell'ultimo recupero dei dati. |

### Come scaricare i dati di utilizzo corrente

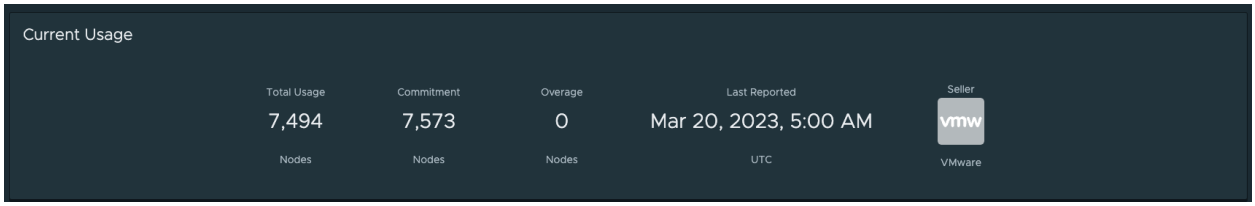
È possibile scaricare un file CSV con i dati di utilizzo corrente per l'Organizzazione facendo clic sul pulsante **Esporta** nell'angolo superiore sinistro della tabella **Utilizzo corrente**.

## Informazioni importanti sui dettagli di utilizzo corrente e cronologico

Per ogni tipo di utilizzo mostrato nel dashboard **Gestione utilizzo** nell'Organizzazione, è possibile visualizzare i dettagli di utilizzo corrente e cronologico. Per aprire i dettagli, fare clic sul link del tipo di utilizzo.

### Utilizzo corrente

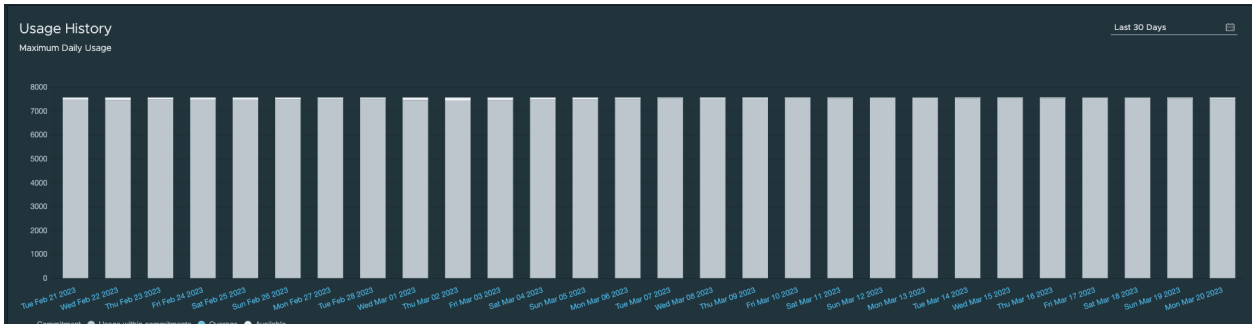
Il dashboard **Utilizzo corrente** mostra una vista di alto livello di alcuni dettagli di base.




- **Utilizzo totale** mostra le unità per utilizzo totale e tipo di metrica di utilizzo. Ad esempio `7,494 Nodes`.
- **Impegno** mostra le unità impegnate per l'utilizzo per la sottoscrizione di un servizio specifico. Ad esempio `7,573 Nodes`.
- **Eccedenza** mostra se l'utilizzo effettivo supera l'utilizzo confermato, la differenza viene indicata da un valore espresso in unità.
- **Ultima segnalazione** mostra la data e l'ora dell'ultimo aggiornamento dei dettagli del tipo di utilizzo corrente.
- **Venditore** rappresenta il venditore del tipo di utilizzo della sottoscrizione.

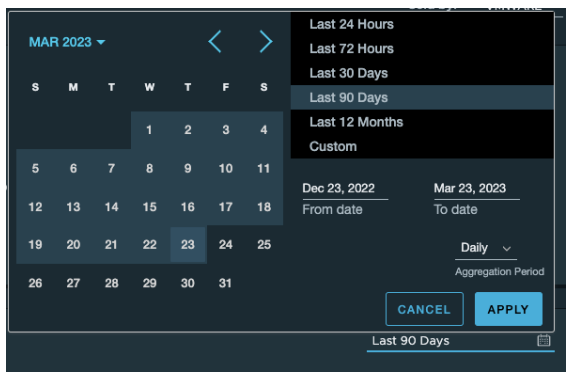
### Cronologia utilizzo

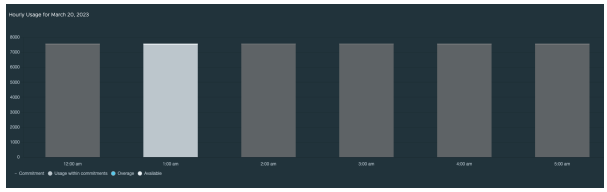
La vista **Cronologia utilizzo** mostra l'utilizzo giornaliero massimo in un periodo di tempo predefinito e l'utilizzo orario per una data specifica.




- L'asse verticale nella vista **Utilizzo giornaliero massimo** rappresenta la metrica di utilizzo e la quantità di unità.
- L'asse orizzontale rappresenta l'intervallo di tempo dei dati visualizzati nel grafico.

## Come utilizzare la vista dell'utilizzo corrente e cronologico

| Operazione da eseguire | Procedere così... |
|---|---|
| Visualizzare informazioni più dettagliate sull'utilizzo. | Passare il puntatore del mouse su una barra del grafico. È possibile visualizzare:<br>■ L'indicazione oraria del grafico.<br>■ Utilizzo conforme agli impegni: numero di unità disponibili tramite impegni che erano in uso nel momento specificato.<br>■ Eccedenza: il numero di unità che hanno causato l'eccedenza nel momento specificato, ovvero la percentuale risultante dell'eccedenza.<br>■ Disponibile: numero di unità disponibili per l'utilizzo in quel momento. |
| Modificare il periodo di tempo del grafico **Utilizzo giornaliero massimo**. | 1 Fare clic sull'icona Calendario nell'angolo superiore destro del grafico **Utilizzo giornaliero massimo**.<br>Il periodo di tempo predefinito per questa visualizzazione è di 30 giorni. Il periodo di tempo minimo per cui è possibile filtrare il numero massimo di dati sull'utilizzo giornaliero è di 24 ore. Il periodo di tempo massimo è di 2 anni.<br>  <br>2 Modificare le impostazioni del periodo di tempo e fare clic su **Applica**. |

| Operazione da eseguire | Procedere così... |
| --- | --- |
| Visualizzare il grafico **Utilizzo orario** per una data specifica. | Fare clic su una barra di data qualsiasi nel grafico **Utilizzo giornaliero massimo**. Il grafico **Utilizzo orario** viene aggiornato per mostrare una ripartizione oraria dell'utilizzo per il giorno selezionato.<br>Esempio di grafico<br>  <br>**Nota** I dati sull'utilizzo orario sono disponibili solo per gli ultimi 30 giorni. |
| Visualizzare l'utilizzo orario in formato tabella. | È possibile visualizzare la ripartizione dell'utilizzo orario nella tabella, appena sotto il grafico **Utilizzo orario**.<br>  <br>Fare clic sull'icona della doppia freccia accanto a una data qualsiasi per organizzare la vista dell'utilizzo orario esteso nelle seguenti colonne:<br>■ Ora: l'ora specifica del giorno a cui si riferiscono i dati.<br>■ Impegno: rappresenta la quantità impegnata dall'Organizzazione con una sottoscrizione.<br>■ Utilizzo conforme all'impegno: rappresenta l'utilizzo effettivo rispetto all'impegno dell'Organizzazione.<br>■ Utilizzo in eccedenza: rappresenta la quantità di utilizzo che non rientra nell'impegno dell'Organizzazione e viene considerato come eccedenza.<br>■ Utilizzo totale: rappresenta l'utilizzo complessivo combinando tutto quello che rientra nell'impegno dell'Organizzazione insieme a qualsiasi eccedenza.<br>■ Unità: la metrica applicabile per il tipo di utilizzo selezionato, ovvero host/IP/EIP/CPU/vCPU e così via |

Il video seguente illustra come utilizzare la funzionalità di zoom.

(Console di Cloud Services - Funzionalità di zoom di Gestione utilizzo)

## Domande frequenti su Gestione utilizzo

Questo argomento illustra le domande frequenti relative al dashboard **Gestione utilizzo** in console di Cloud Services.

### D: Perché l'acquisto non viene visualizzato nella pagina Gestione utilizzo?

R: Tutti i dati di utilizzo vengono elaborati su base giornaliera. In base a quando si è verificato l'utilizzo del servizio, la visualizzazione in questo report può richiedere fino a 48 orre. Si noti che alcuni servizi forniscono dati su base mensile.

### D: Perché l'utilizzo è ritardato?

R: Tutti i dati di utilizzo vengono elaborati su base giornaliera. In base a quando si è verificato l'utilizzo del servizio, la visualizzazione in questo report. Si noti che alcuni servizi forniscono dati su base mensile.

### D: Come si trovano informazioni sui costi?

R: È possibile visualizzare gli addebiti per i servizi consultando i rendiconti delle attività. Per ulteriori dettagli, fare riferimento a Come leggere il rendiconto attività.

### D: I dati di utilizzo non sono visualizzati. Perché?

R: Gestione utilizzo non è disponibile per tutti i VMware Cloud services. Alcuni dei servizi che attualmente forniscono dati sull'utilizzo sono VMware Cloud on AWS, VMware Aria Operations for Networks, VMware Aria Operations, VMware Aria Operations for Logs, VMware Aria Automation, VMware Cloud Disaster Recovery, VMware Cloud Director VMware Lab Platform. Se il servizio è supportato, in base a quando si è verificato l'utilizzo del servizio, la visualizzazione di questo report potrebbe richiedere fino a 48 ore. Si noti che alcuni servizi forniscono dati su base mensile.

### D: Per quanto tempo è possibile visualizzare i dati sull'utilizzo?

R: Il periodo di tempo predefinito visualizzato nel dashboard è 30 giorni. Il periodo di tempo minimo per cui è possibile filtrare il numero massimo di dati sull'utilizzo giornaliero è di 24 ore. Il periodo di tempo massimo è di due anni. Si noti che in ogni momento il grafico mostra dati per un periodo massimo di 1 anno.

### D: Non è possibile visualizzare i dati orari. Perché?

R: I dati orari sono disponibili solo per gli ultimi 30 giorni. Sono disponibili solo dati giornalieri.

### I dati di utilizzo non riflettono la fattura. Perché?

R: La maggior parte dei servizi viene fatturata in base alla somma dell'eccedenza oraria che si è verificata durante il periodo di fatturazione. In questo grafico, verrà visualizzato l'utilizzo effettivo per una determinata ora e l'utilizzo massimo per un determinato giorno.

### D: Il grafico Utilizzo principale non viene visualizzato. Perché?

R: Il grafico **Utilizzo principale** mostra solo l'utilizzo che si è verificato negli ultimi 30 giorni per un servizio per cui è previsto un impegno. Se non è presente alcun servizio con un utilizzo idoneo, il grafico non verrà visualizzato. L'utilizzo potrebbe non essere visualizzato per alcuni motivi:

- Tutto l'utilizzo è per un servizio su richiesta. L'utilizzo su richiesta non viene visualizzato nel grafico Utilizzo principale.
- L'utilizzo è per un servizio che non fornisce dati sull'utilizzo.
- L'utilizzo si è verificato da più di 30 giorni.

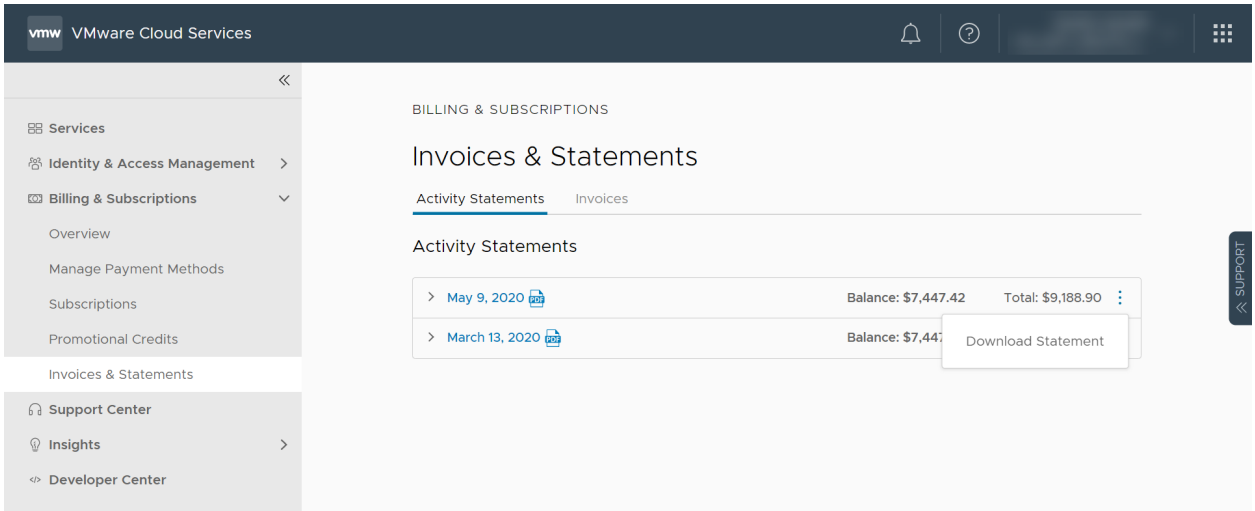
## Come visualizzare estratti conto e fatture

L'utente **Proprietario dell'Organizzazione** può visualizzare e stampare gli ultimi 15 estratti conto dell'attività, fatture su richiesta e fatture annuali di impegno.

Per visualizzare gli estratti conto e le fatture, selezionare **Fatturazione e sottoscrizioni > Fatture ed estratti conto** nella console di Cloud Services.

### Estratti conto dell'attività

La pagina **Estratti conto attività** visualizza riepiloghi mensili di tutti i servizi utilizzati in un determinato periodo di fatturazione. Ogni estratto conto dell'attività fornisce un riepilogo dei pagamenti effettuati a fronte di costi, crediti promozionali e bilancio. È possibile visualizzare e scaricare gli estratti conto dell'attività facendo clic sul relativo collegamento o selezionando un'opzione dall'icona con i puntini di sospensione verticali accanto.

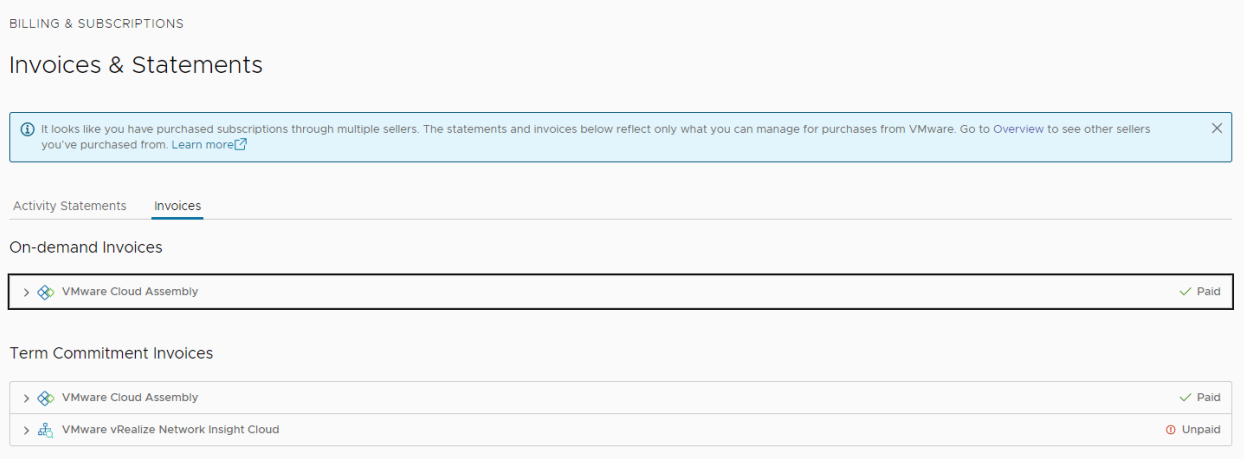



### Fatture

Per accedere alle fatture, fare clic sulla scheda **Fatture** nella pagina **Fatture ed estratti conto**

- La sezione **Fatture su richiesta** della pagina elenca i costi di fatturazione per le sottoscrizioni su richiesta.

- La sezione **Fatture impegni a termine** riporta le fatture relative agli impegni a termine della sottoscrizione.




È possibile scaricare una fattura facendo clic sul relativo link oppure selezionando **Scarica** dal menu con i puntini di sospensione verticali ( ⋮ ) accanto.

## Come leggere il rendiconto attività

In qualità di utente **Proprietario dell'Organizzazione**, puoi visualizzare informazioni dettagliate su tutti i servizi utilizzati dalla tua Organizzazione durante un determinato periodo di fatturazione nel rendiconto delle attività per quel periodo di fatturazione. Il rendiconto attività non è una fattura.

### Cosa è incluso nel rendiconto attività

Ciascun rendiconto attività fornisce un riepilogo e un'analisi dettagliata di tutti gli addebiti di servizio maturati nel periodo di fatturazione e dei pagamenti effettuati a fronte degli addebiti di servizio.

#### Riepilogo periodo di fatturazione

Il riepilogo del periodo di fatturazione è una panoramica degli addebiti totali, dei crediti, degli sconti, degli adeguamenti e dei pagamenti per il periodo di fatturazione. L'importo del saldo corrisponde agli addebiti non pagati per il periodo corrente, mentre il saldo residuo corrisponde al saldo del periodo di fatturazione precedente, qualora non sia stato pagato.

**Nota** I pagamenti effettuati dopo la data di generazione del rendiconto attività non vengono riportati nel riepilogo.

#### Dettagli addebiti

La sezione Dettagli addebiti fornisce una rappresentazione visiva in grafico a torta degli addebiti maturati per ciascun servizio nell'Organizzazione. L'importo indicato per ciascun servizio corrisponde all'importo di eventuali addebiti al netto di tutti gli sconti, le promozioni e gli adeguamenti. Questo grafico viene generato solo se la tua Organizzazione ha sostenuto addebiti per più di un servizio.

### Cronologia addebiti

Se l'Organizzazione ha sostenuto addebiti per più periodi di fatturazione, nella sezione Cronologia addebiti sarà riportato un grafico a linee con la cronologia degli addebiti per ciascun servizio per un massimo di 12 mesi. L'importo indicato per ciascun servizio corrisponde all'importo di eventuali addebiti al netto di tutti gli sconti, le promozioni e gli adeguamenti.

### Addebiti servizi

La sezione Addebiti servizi include addebiti e crediti calcolati durante il periodo di fatturazione e tutti i pagamenti effettuati per tali addebiti. I crediti riguardano tutti gli sconti, le promozioni e gli adeguamenti per servizio e sono indicati con un segno meno davanti all'importo. Gli addebiti per il servizio possono riguardare servizi con impegni rispetto ai termini, servizi utilizzati su richiesta e costi aggiuntivi di utilizzo del servizio. I subtotali di impegni a termine, utilizzo su richiesta e altri addebiti vengono riportati per riga, seguiti dai pagamenti e dal saldo corrente. I pagamenti includono tutti gli sconti, le promozioni e gli adeguamenti per servizio.

### Dettagli su richiesta

Tutti gli addebiti per i servizi su richiesta utilizzati dall'Organizzazione sono riportati nella sezione Dettagli su richiesta. I costi vengono addebitati solo se la tua Organizzazione ha utilizzato i servizi su richiesta e solo per il tempo in cui sono stati utilizzati.

### Dettagli altri addebiti

Eventuali costi aggiuntivi addebitati alla tua Organizzazione, come trasferimento dei dati, Direct Connect, EBS, costi dell'IP flessibile e crediti di registrazione, sono riportati in Altri addebiti. Gli addebiti vengono aggregati per regione e per SID (ID sottoscrizione) univoci.

## Glossario delle abbreviazioni utilizzate nel rendiconto attività

Il rendiconto attività mostra le abbreviazioni di prodotti, servizi e unità di misura che contribuiscono al calcolo dei costi. Il seguente glossario fornisce un rapido riferimento utile per la lettura del tuo rendiconto.

Tabella 11-3. Glossario delle abbreviazioni di VMware Cloud Services

| Nome prodotto | Unità di misura | Descrizione unità di misura |
|---|---|---|
| vRealize Automation Cloud | EA | Each |
| | NDH | Node per Hour |
| vRealize Log Insight Cloud | EA | Each |
| | NDH | Node per Hour |
| | GB | Gigabyte |
| vRealize Network Insight Cloud | CPU | Central Processing Unit |

Tabella 11-3. Glossario delle abbreviazioni di VMware Cloud Services (continua)

| Nome prodotto | Unità di misura | Descrizione unità di misura |
|---|---|---|
| | GB | Gigabyte |
| | EA | Each |
| | VCP | Virtual Central Processing Unit |
| NSX Cloud | CRM | Core al mese |
| | EA | Each |
| Tanzu Application Catalog | EA | Each |
| Tanzu Application Service | COH | Compute Unit Hour |
| | EA | Each |
| VMware Cloud Director | CRM | Core al mese |
| | EA | Each |
| VMware SD-WAN by VeloCloud | EA | Each |
| VMware Learning Platform | ALH | Active Lab Hour |
| | BIH | Bring Your Own Cloud |
| | COH | Compute Unit Hour |
| | EA | Each |
| | STH | Storage Unit Hour |
| | WIH | Windows Unit Hour |
| VMware Cloud on AWS | ATG | Attachment per GB |
| | ATH | Attachment per Hour |
| | EA | Each |
| | GB | Gigabyte |
| | GBM | Gigabyte Month |
| | HST | Host |
| | HPH | Host per Hour |
| | IPR | IP Address per Hour |
| | IP | Indirizzo IP |
| | VMH | Virtual Machine per Hour |
| VMware Cloud on AWS GovCloud (US) | EA | Each |

Tabella 11-3. Glossario delle abbreviazioni di VMware Cloud Services (continua)

| Nome prodotto | Unità di misura | Descrizione unità di misura |
|---|---|---|
| | HPH | Host per Hour |
| | IP | Indirizzo IP |
| | VMH | Virtual Machines per Hour |
| | ATH | Attachment per Hour |
| | ATG | Attachment per Giga Byte |
| | IPR | IP Address per Hour |
| | GB | Gigabyte |
| VMware Cloud on DELL EMC | EA | Each |
| | NDM | Node per Month |
| | EDM | Edge per Month |
| vRealize Operations Cloud | EA | Each |
| | OSI | Operating System Instance |

## Come inserire un numero di PO nella fattura

Per elaborare il pagamento della fattura, potrebbe essere necessario includere nella fattura informazioni aggiuntive, come ad esempio un numero di PO. Aggiungere le informazioni di riferimento e ristampare la fattura dalla pagina **Fatture** di console di Cloud Services.

### Prerequisiti

È necessario disporre del ruolo di **Proprietario dell'Organizzazione** in cui è stata generata la fattura.

### Procedura

1. Accedere a console di Cloud Services e passare a **Fatturazione e sottoscrizioni > Fatture e rendiconti > Fatture**.
2. Individuare la fattura che si desidera ristampare e fare clic sull'icona con i puntini verticali ( ⋮ ) accanto a essa.
3. Dal menu che si aprirà, selezionare **Inserisci n. di riferimento**.

**Nota** Il link **Inserisci n. di riferimento** è disponibile solo se la fattura è disponibile come PDF scaricabile, non è ancora stata saldata e il metodo di pagamento non è una carta di credito. Non è disponibile se è già stata richiesta la ristampa della fattura ma quella aggiornata non è ancora disponibile per il download.

4 Nella finestra popup che si aprirà, immettere il numero di PO che si desidera includere nella fattura, quindi fare clic su **Invia**.

**Importante** La generazione della nuova fattura potrebbe richiedere fino a 24 ore. Si riceverà una notifica via e-mail una volta che la fattura sarà ristampata.

# Come ricevere assistenza

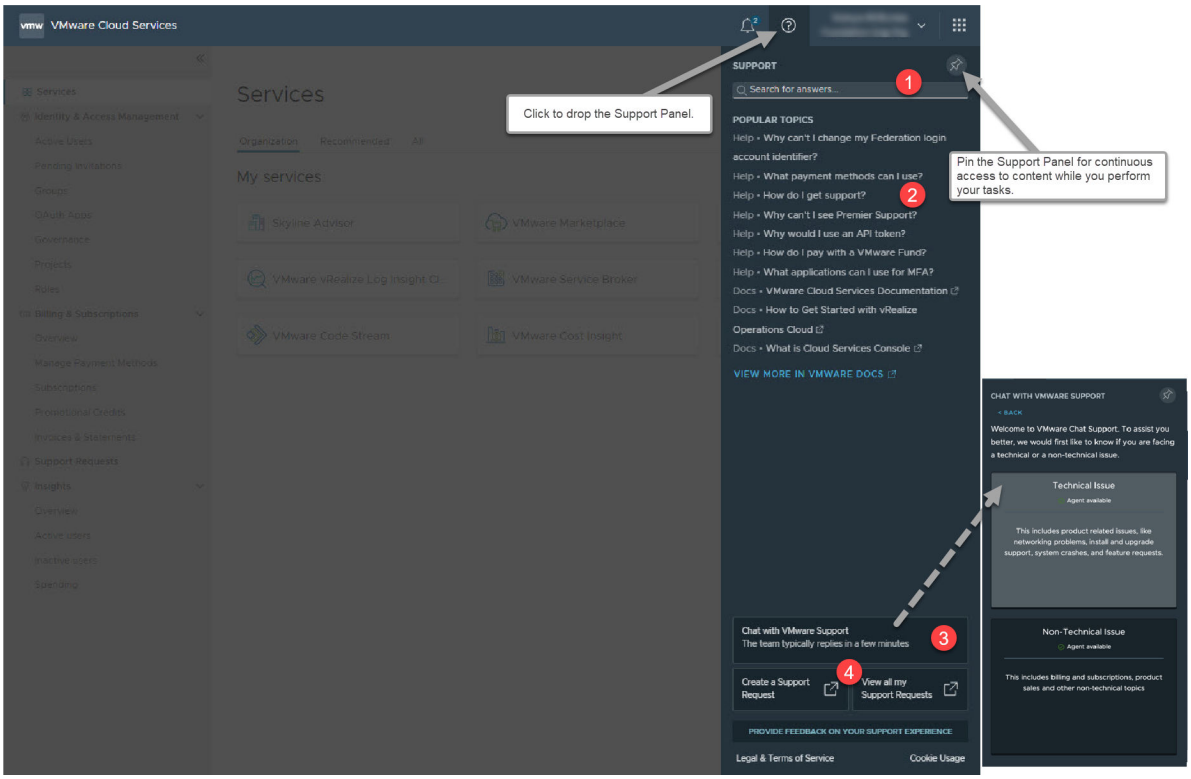
12

Diamo il benvenuto all'esperienza di assistenza interna al prodotto VMware Cloud services. Qui è possibile visualizzare il contenuto della guida contestuale che consente di eseguire le attività, cercare risposte alle domande e contattare un membro del team di assistenza clienti, se si desidera chattare con loro.

La nostra esperienza di assistenza è in continua evoluzione, con nuove funzionalità in fase di distribuzione per tutti i servizi cloud. Al momento, è possibile visualizzare alcune o tutte le funzionalità seguenti nel pannello Assistenza.

Procedura

1 Aprire il pannello Assistenza facendo clic sull'icona **Domanda** nel menu o sulla scheda **Assistenza** a destra del riquadro.



2 Accedere al livello di assistenza di cui si ha bisogno.

Nel pannello **Assistenza**, è possibile visualizzare il contenuto della guida contestuale ed effettuare potenti ricerche per aiutare a trovare più contenuti e rispondere a domande, il tutto senza contattare l'assistenza. Quando si chatta con un rappresentante dell'assistenza clienti, è possibile continuare a interagire con il servizio cloud contemporaneamente.

| **Accedere a questa funzionalità di assistenza...** | **Per ricevere assistenza...** |
|---|---|
| 1. Ricerca intelligente. | Cercare nei nostri contenuti per trovare le risposte alle proprie domande. È possibile consultare la nostra documentazione, argomenti di assistenza scritti appositamente, community e articoli della knowledge base. |
| 2. Contenuto relativo alla pagina. | Eseguire le attività. Quando si apre il pannello **Assistenza**, si visualizzano argomenti di aiuto relativi alle pagine che contengono informazioni sufficienti per assisterti nelle tue attività. Nel corso delle attività e passando da una pagina all'altra, il contenuto della guida cambia di conseguenza. In questo elenco di contenuti sono riportati anche i risultati della ricerca. I risultati della ricerca includono ulteriori argomenti della guida, articoli della knowledge base, contenuti del Centro documentazione e contenuti dalle nostre community.<br>Se non si trova quello che si sta cercando, fare clic su **Visualizza altro in VMware Docs** per eseguire una ricerca correlata alla pagina che si sta visualizzando o se è stato digitato un elemento di ricerca, correlato all'elemento di ricerca. I risultati saranno visualizzati nel Centro documentazione. |

| Accedere a questa funzionalità di assistenza... | Per ricevere assistenza... |
| --- | --- |
| 3. Chattare con l'assistenza VMware. | Contattare gli ingegneri dell'assistenza e i rappresentanti dell'assistenza clienti.<br>Ecco cosa è necessario sapere sulla chat live di assistenza:<br>■ L'avvio di una chat con l'assistenza VMware è sensibile al contesto. Ciò significa che quando si avvia una chat live con l'assistenza VMware da console di Cloud Services, è possibile ricevere assistenza per i problemi relativi a console di Cloud Services. Per accedere al supporto della chat per un servizio, assicurarsi di avviare una chat dopo aver effettuato l'accesso al servizio.<br>■ È possibile continuare a interagire con console di Cloud Services o con console di Cloud Services mentre si chatta con i nostri ingegneri dell'assistenza clienti. È sempre possibile tornare alla chat facendo clic sul pulsante **Assistenza** presente sul bordo destro della finestra del browser  , quindi fai clic sull'icona **Ritorna alla chat**  .<br>■ I tecnici dell'assistenza clienti possono anche aiutare ad aprire una richiesta di assistenza.<br>■ A seconda delle impostazioni della lingua configurate per il browser e il profilo di VMware Cloud Services, si riceverà assistenza online sia in lingua inglese sia giapponese.<br>■ Quando si utilizza la chat live di assistenza in console di Cloud Services:<br>  ■ È innanzitutto necessario selezionare se il problema per il quale si ha bisogno di assistenza è tecnico o non tecnico. Ciò garantisce che la richiesta venga rivolta al rappresentante dell'assistenza clienti appropriato.<br>  ■ Non è possibile avere più chat di assistenza contemporaneamente. Per aprire una nuova chat per un nuovo problema, è necessario chiudere la chat corrente.<br>  ■ Durante la chat, è possibile inviare file o screenshot al rappresentante dell'assistenza clienti direttamente dalla finestra di chat.<br>**Nota** Per evitare problemi di timeout durante una sessione di chat attiva, è consigliabile tenere aperta la finestra o la scheda del browser in primo piano. |
| 4. Crea una richiesta di assistenza/Visualizza tutte le mie richieste di assistenza. | Apre VMware Customer Connect, dove è possibile creare e gestire le richieste di assistenza. |

3 Per gestire le richieste di assistenza, fare clic sul link **Richieste di assistenza** nel menu di console di Cloud Services.

Tutte le funzionalità correlate all'assistenza sono ora disponibili tramite il portale VMware Customer Connect.

a Fare clic su **Crea una richiesta di assistenza**.

Viene aperta la pagina **Assistenza VMware** in Customer Connect. Per istruzioni dettagliate sulla creazione di una nuova richiesta di assistenza, vedere Come inviare una richiesta di assistenza in Customer Connect e tramite il portale di Cloud Services.

Prima di aprire una richiesta di assistenza, potrebbe essere necessario disporre di ulteriori informazioni relative al servizio. Ad esempio, in VMC on AWS è possibile richiede le informazioni di assistenza per l'SDDC.

b Per accedere a tutte le richieste di assistenza aperte e chiuse per l'Organizzazione, fare clic su **Visualizza cronologia richieste di assistenza**.

Viene aperta la pagina **Cronologia richieste di assistenza** su Customer Connect.

È quindi possibile filtrare le richieste di assistenza in base all'Organizzazione, al tipo e al periodo di tempo. È inoltre possibile ordinare ed esportare i dati.

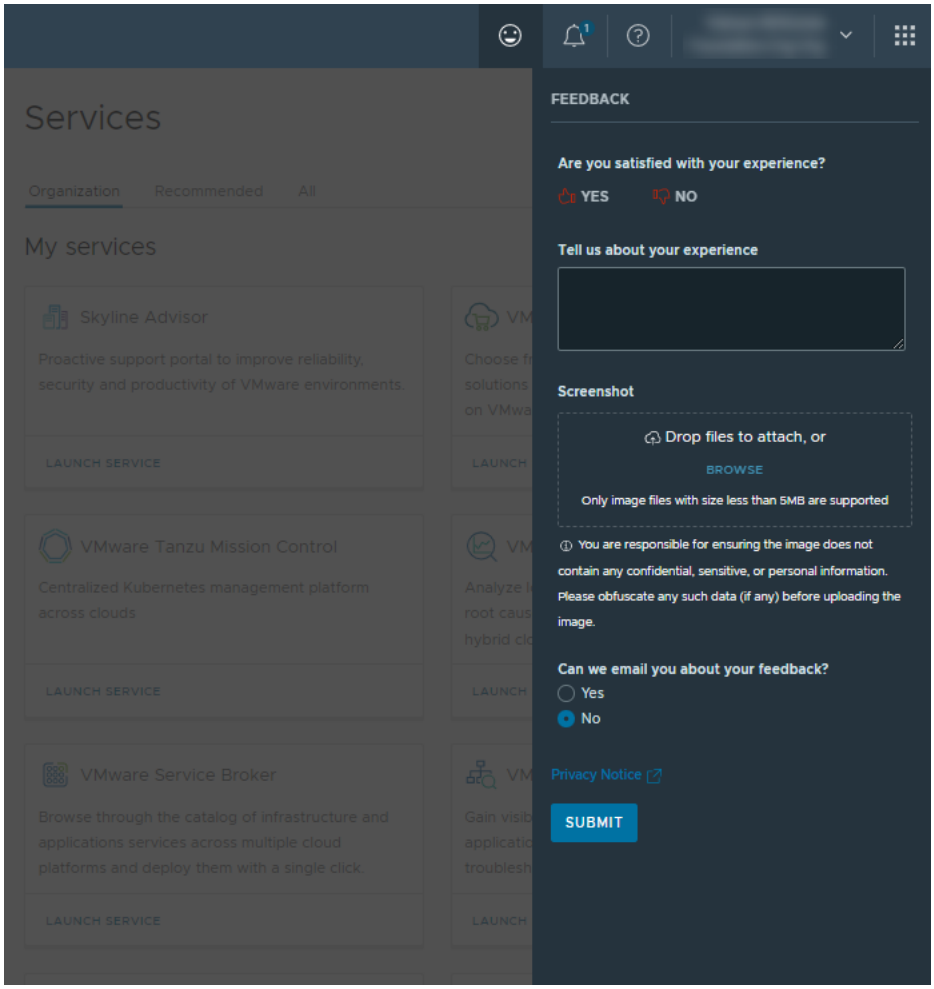
# Come fornire feedback

13

Il feedback degli utenti consente di migliorare i prodotti. È possibile inviare un feedback su console di Cloud Services direttamente dal prodotto.

1 Nel menu orizzontale in console di Cloud Services fare clic sull'icona **Fornisci feedback** ( ).

Viene aperto il pannello del feedback.




2 Utilizzare una o più delle opzioni disponibili per fornire il feedback:

- Utilizzare l'icona del pollice in su o del pollice in giù per comunicare il proprio livello di soddisfazione dell'utilizzo di console di Cloud Services.

- Utilizzare il campo di testo per descrivere la propria esperienza in modo più dettagliato.
- Se si desidera migliorare visivamente il messaggio del feedback, allegare uno screenshot facendo clic su **Sfoglia** o trascinando un'immagine nel campo designato.
- Scegliere se si desidera essere contattati dal team di VMware console di Cloud Services in merito al feedback fornito.

3 Fare clic su **Invia**.