Configurazione e risoluzione dei problemi di Single Sign-On in AppDynamics

Sommario

Introduzione

In questo documento viene descritto come configurare Single Sign-On (SSO) in AppDynamics e come risolvere i problemi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Per configurare Single Sign-On, l'utente deve disporre del ruolo Proprietario account (predefinito) o di un ruolo personalizzato con l'autorizzazione Amministrazione, Agenti, Guida introduttiva.
- Accesso amministrativo a IdPaccount.
- Metadati o dettagli di configurazione da AppDynamics (ad esempio, ID entità, URL ACS).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- AppDynamics Controller

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Single Sign-On (SSO) è un meccanismo di autenticazione che consente agli utenti di accedere una sola volta a più applicazioni, sistemi o servizi senza dover ripetere l'autenticazione per ognuno di essi.

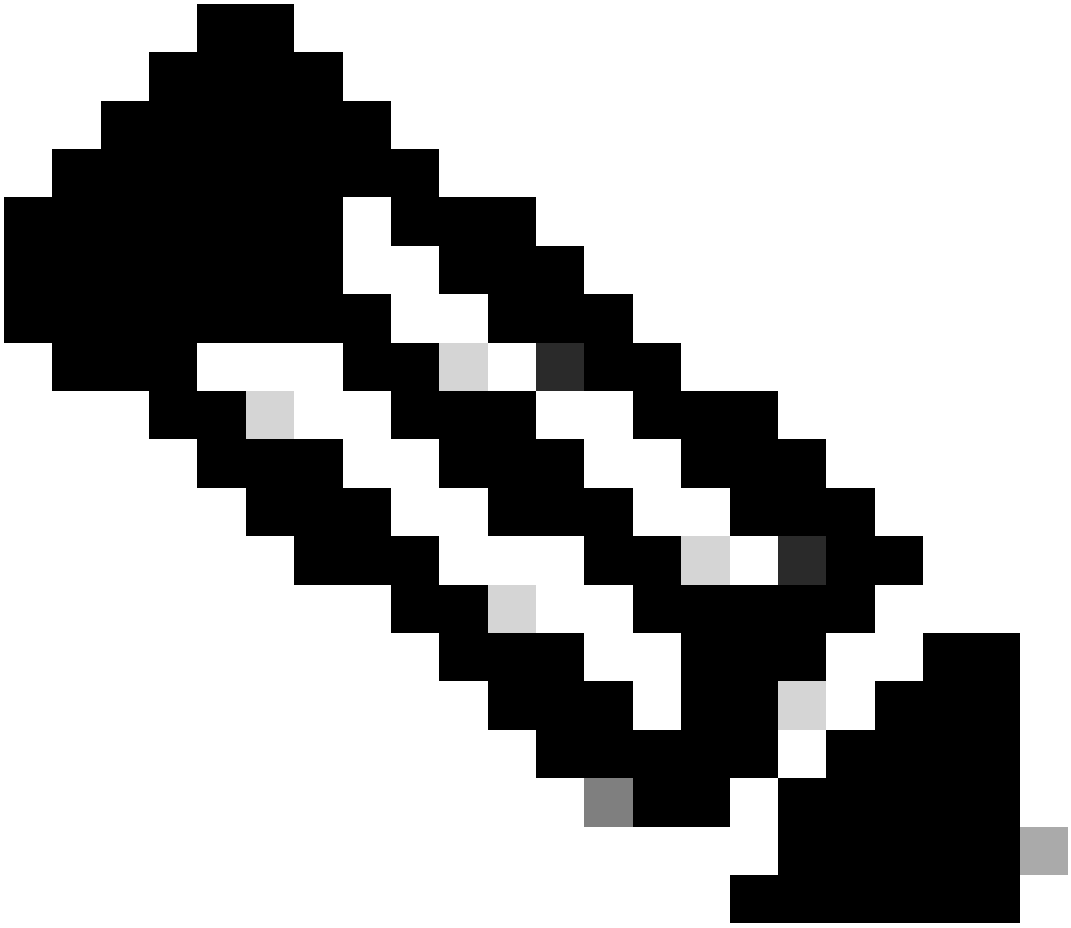
SAML (Security Assertion Markup Language) è una delle tecnologie utilizzate per implementare l'SSO. Fornisce la struttura e i protocolli che consentono l'SSO scambiando in modo sicuro i dati di autenticazione e autorizzazione tra un provider di identità (IdP) e un provider di servizi (SP).

Asserzione SAML

- Scambio di messaggi basati su XML tra IdP e SP.
- Sono disponibili tre tipi di asserzioni:
    - Asserzioni di autenticazione: Conferma l'autenticazione dell'utente.
    - Asserzioni attributi: Condivide gli attributi utente, ad esempio il nome utente o i ruoli.
    - Asserzioni decisioni autorizzazione: Indica l'operazione che l'utente è autorizzato a eseguire.

Ruoli chiave in SAML

- Provider di identità (IdP)
    - Verifica l'identità dell'utente.
    - Generare l'asserzione SAML che contiene le informazioni di identificazione dell'utente.
- Provider di servizi (SP)
    - L'applicazione o il sistema a cui l'utente desidera accedere.
    - Utilizza l'IdP per autenticare l'utente.
    - Accetta l'asserzione SAML per concedere all'utente l'accesso alle proprie risorse o applicazioni.
- Utente (entità)
    - Utente effettivo che ha avviato la richiesta o che sta tentando di accedere a una risorsa dal provider di servizi.
    - Interagisce sia con l'IdP (autenticazione) che con l'SP.



Nota: AppDynamics supporta sia l'avvio di IdP che l'avvio di SP SSO.

Flusso avviato SP:

- L'utente accede al provider di servizi digitando l'URL dell'applicazione (ad esempio, AppDynamics) o facendo clic su un collegamento.
- L'SP verifica se esiste una sessione. Se non esiste alcuna sessione, l'SP riconosce che l'utente non è autenticato e avvia il processo SSO.
- L'SP genera una richiesta di autenticazione SAML e reindirizza l'utente all'IdP per l'autenticazione.
    - La richiesta include:
        - ID entità: Identificatore univoco del provider di servizi.
        - URL Assertion Consumer Service (ACS): dove IdP invia SAML Assertion dopo l'autenticazione.
        - Metadati relativi all'SP e dettagli di protezione (ad esempio, richiesta firmata, requisiti di crittografia).
- L'utente viene reindirizzato alla pagina di accesso del provider di identità.

- Il provider di identità autentica l'utente, ad esempio tramite nome utente/password o autenticazione a più fattori.
- Dopo l'autenticazione, il provider di identità genera un'asserzione SAML (token di sicurezza).
- L'asserzione SAML viene restituita all'SP tramite il browser utente utilizzando l'associazione POST HTTP (nella maggior parte dei casi) o l'associazione di reindirizzamento HTTP.
- L'SP convalida l'asserzione SAML per garantire:
    - È stato rilasciato dal provider di identità attendibile.
    - È indirizzato all'SP (tramite l'ID entità SP).
    - Non è scaduto o non è stato manomesso (convalidato con la chiave pubblica IdP).
- Se l'asserzione SAML è valida, l'SP crea una sessione per l'utente.
- All'utente viene concesso l'accesso all'applicazione o alle risorse.

Flusso avviato da IdP:

- L'utente accede al portale di accesso IdP e immette le proprie credenziali.
- Il provider di identità autentica l'utente, ad esempio tramite una combinazione di nome utente e password e l'autenticazione a più fattori.
- Dopo l'autenticazione, il provider di identità fornisce all'utente un elenco delle applicazioni o dei servizi (SP) disponibili a cui può accedere.
- L'utente seleziona l'SP desiderato (ad esempio, AppDynamics).
- IdP genera un'asserzione SAML per l'SP selezionato.
- Il provider di identità reindirizza l'utente all'URL del servizio consumer di asserzione SP (ACS) e invia l'asserzione SAML insieme a essa (utilizzando l'associazione HTTP POST o l'associazione HTTP redirect).
- L'SP riceve l'asserzione SAML e la convalida:
    - Assicura che l'asserzione sia emessa da un provider di identità attendibile.
    - Verifica l'integrità e la scadenza dell'asserzione.
    - Conferma l'identità utente e altri attributi.
- Se l'asserzione SAML è valida, l'SP crea una sessione per l'utente.
- All'utente viene concesso l'accesso all'applicazione o alle risorse.

Configurazione

AppDynamics Controller può utilizzare l'identità del cliente Cisco o un provider di identità SAML (IdP) esterno per autenticare e autorizzare gli utenti.

Provider di identità supportati

AppDynamiccertifica il supporto per questi provider di identità (IdP):

- Okta
- Onelogin
- Identità ping
- Azure AD

- IBM Cloud Identity
- ADFS (Active Directory Federation Service)

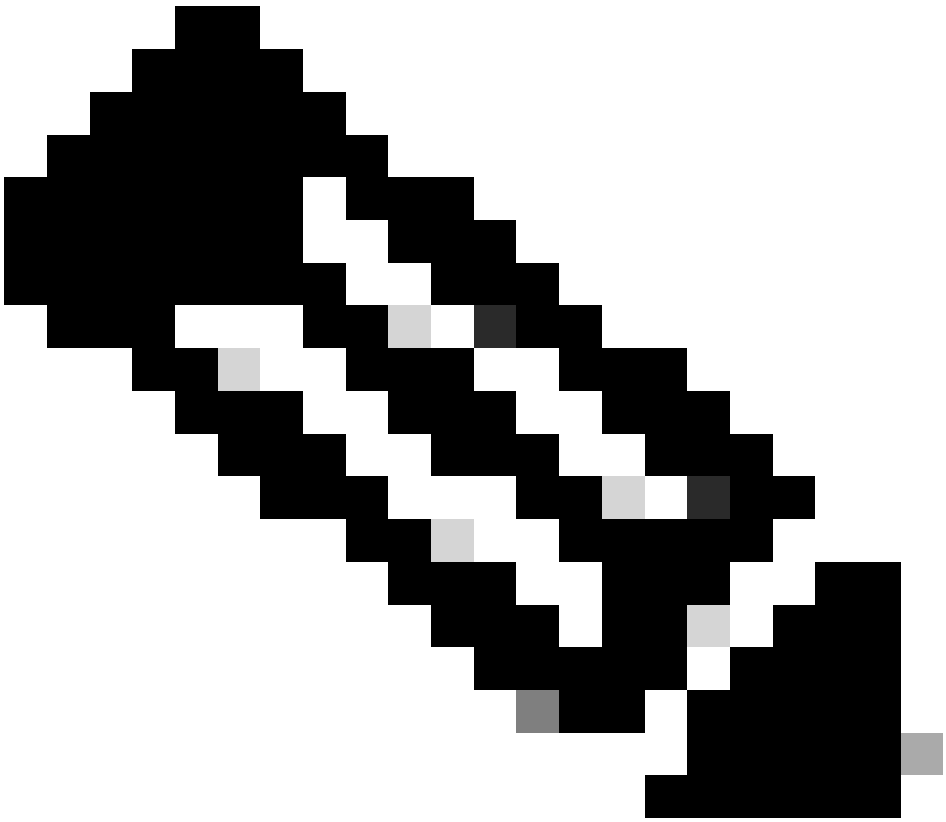
Altri IdP che supportano il binding HTTP POST sono compatibili anche con l'autenticazione SAML di AppDynamics.

Passaggi per configurare SAML in AppDynamics

Passaggio 1. Raccolta dei dettagli di AppDynamics Controller

- ID entità (ID entità SP): identificatore univoco per AppDynamics (ad esempio, https://<host-controller>:<porta>/controller).
  - Sintassi: https://<dominio_controller>/controller
  - esempio: https://<dominio_controller_utente>/controller

- URL risposta (servizio consumer di asserzione, URL ACS): l'endpoint nel provider di servizi (ad esempio, AppDynamics) in cui il provider di identità invia la risposta SAML dopo l'autenticazione.
  - Sintassi: https://<dominio_controller>/controller/saml-auth?accountName=<nome_account>
  - esempio: https://your_controller_domain/controller/saml-auth?accountName=youraccountname



Nota: In caso di controller locale, il nome account predefinito è customer1, a meno che non si disponga di un controller multi-tenant con accountName diverso.

- URL di disconnessione singolo (facoltativo): l'endpoint sull'SP per gestire le richieste di disconnessione SAML (ad esempio, https://<controller_domain>/controller).

Passaggio 2. Creare una nuova applicazione in IdP e scaricare i metadati

- Individuare l'area di creazione dell'applicazione: generalmente si trova all'interno della console di amministrazione o del dashboard IdP, spesso etichettati come Applicazioni, Applicazioni Web e Mobile, Applicazioni Enterprise o Relying Party.
- Aggiungere un'applicazione SAML personalizzata o generica: selezionare un'opzione che consente di configurare un'applicazione SAML personalizzata o un'integrazione con un provider di servizi SAML generico.
- Specificare i dettagli dell'applicazione: assegnare un nome all'applicazione e, se possibile, caricare un'icona per l'identificazione (facoltativo).
- Aggiungere i mapping di attributi (Nome utente, NomeVisualizzato, Posta elettronica o Ruoli) per passare le informazioni utente a AppDynamics.
- Scaricate il file di metadati IdP o, in alternativa, annotate i seguenti dettagli:
    - URL di accesso IdP

- URL di disconnessione
- Nomi attributo
- Certificato

Passaggio 3. Configurare l'autenticazione SAML in AppDynamics Controller

- Accedere all'interfaccia utente del controller come ruolo del proprietario dell'account o con l'autorizzazione Amministrazione, Agenti, Guida introduttiva.
- Fare clic su Nome utente (angolo superiore destro)> Amministrazione > Provider di autenticazione > Seleziona SAML.

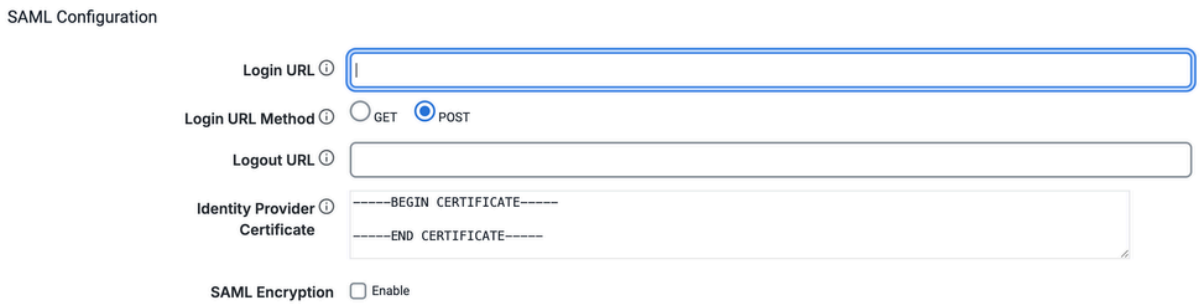
- Nella sezione Configurazione SAML aggiungere i seguenti dettagli:

  - URL di accesso: URL di accesso IdP in cui AppDynamics Controller instrada le richieste di accesso avviate da Service Provider (SP).

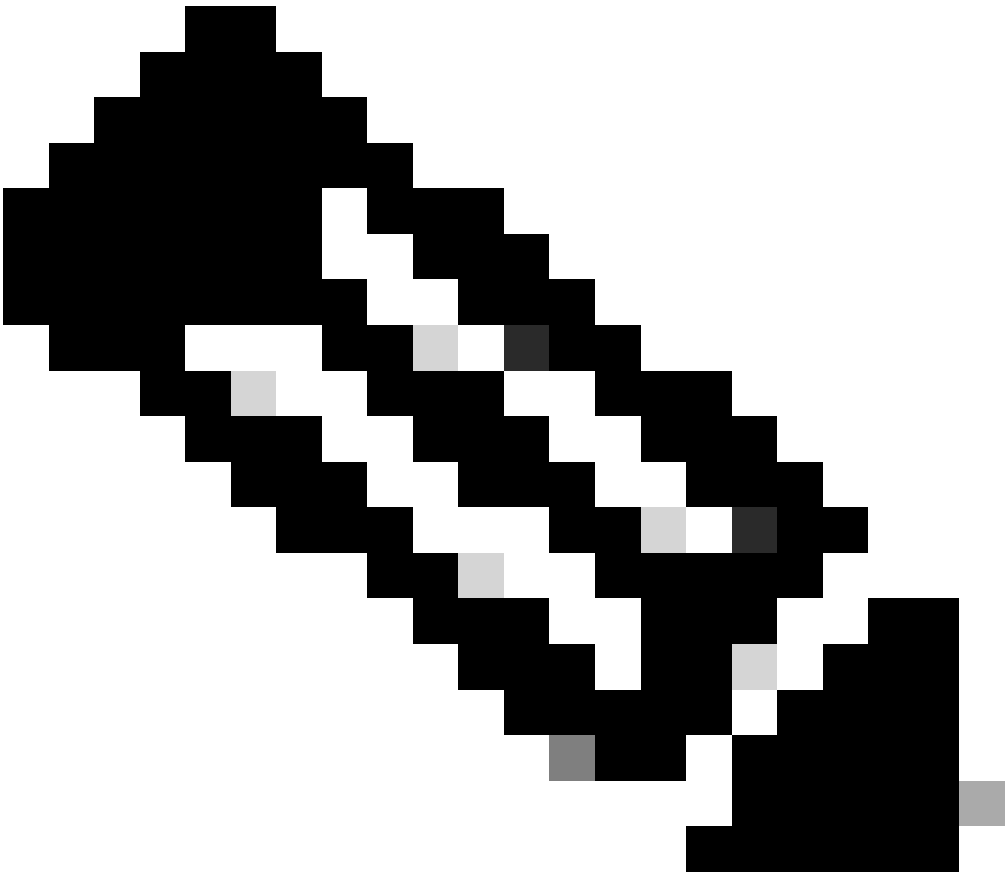
  - URL di disconnessione (facoltativo): URL a cui AppDynamics Controller reindirizza gli utenti dopo la disconnessione. Se non si specifica un URL di disconnessione, gli utenti visualizzeranno la schermata di accesso di AppDynamics al momento della disconnessione.

  - Certificato: Certificato X.509 da IdP. Incollare il certificato tra i delimitatori BEGIN CERTIFICATE e END CERTIFICATE. Evitare di duplicare i delimitatori BEGIN CERTIFICATE e END CERTIFICATE dal certificato di origine stesso.

  - Crittografia SAML (facoltativa): è possibile migliorare la sicurezza dell'autenticazione SAML crittografando la risposta SAML dall'IdP al provider di servizi. Per crittografare le risposte SAML in AppDynamics, è necessario configurare il provider di identità (IdP) per crittografare l'asserzione SAML e quindi configurare AppDynamics Controller in modo che utilizzi un certificato e una chiave privata specifici per la decrittografia.



- Nella sezione Mapping di attributi SAML, mappare gli attributi SAML (esempio: Username, DisplayName, Email) nei campi corrispondenti in AppDynamics.

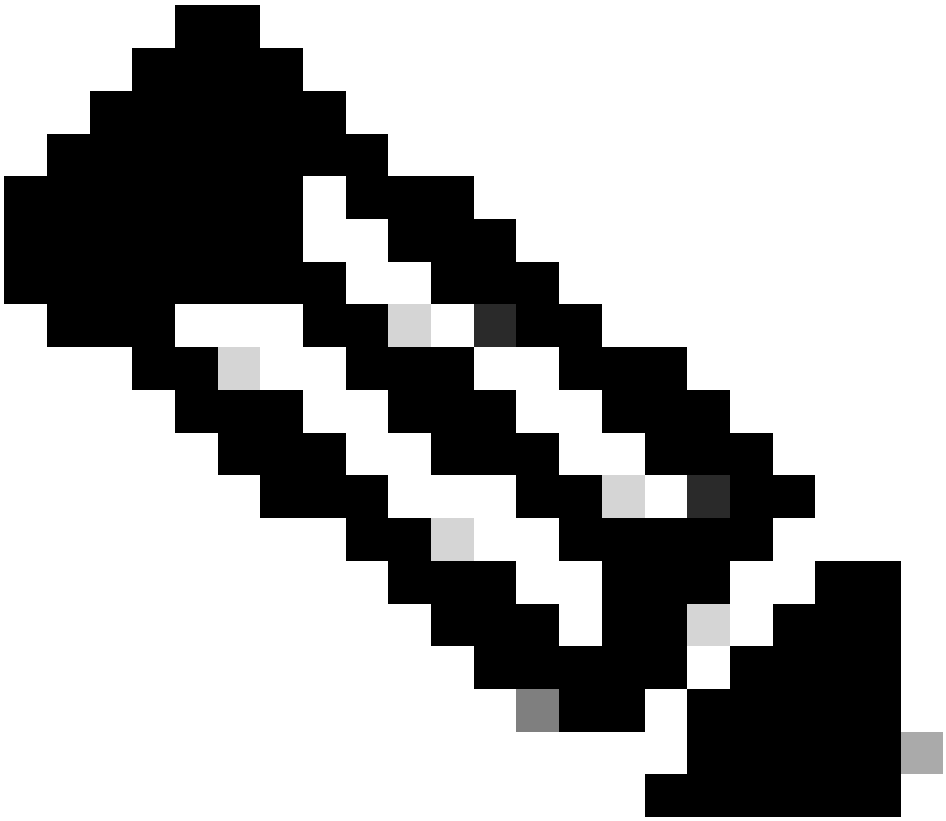


Nota: AppDynamics visualizza il nome utente, l'indirizzo di posta elettronica e il nome visualizzato di un utente SAML. Per impostazione predefinita, viene utilizzato l'attributo NameID della risposta SAML per creare un nome utente, che viene utilizzato anche come displayName. Questo comportamento può essere personalizzato includendo gli attributi username, email e displayname nella risposta SAML. Durante la configurazione delle impostazioni IdP in AppDynamics, l'utente può specificare questi nomi di attributo. Durante l'accesso, AppDynamics verifica se il mapping degli attributi è configurato. Se i mapping sono configurati e nella risposta SAML sono presenti attributi corrispondenti, AppDynamics utilizza tali valori per impostare il nome utente, l'indirizzo di posta elettronica e il nome visualizzato.

- Aggiungere questi dettagli nella sezione Mapping dei gruppi SAML.
  - Nome attributo gruppo SAML: immettere il nome dell'attributo SAML che contiene le

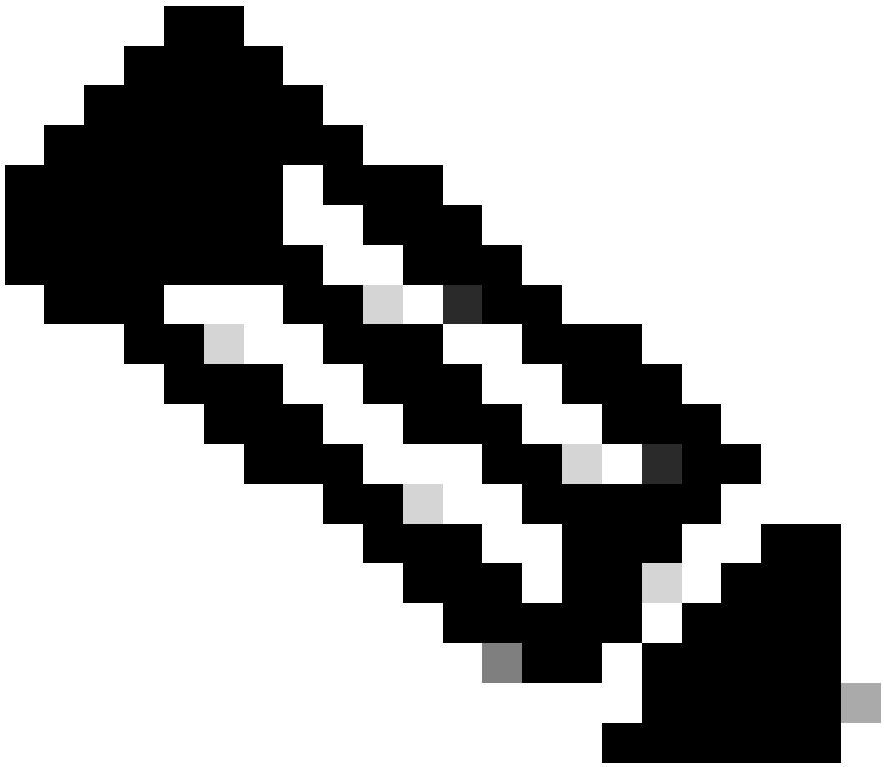
informazioni sul gruppo. In genere si tratta di Gruppi, gruppi o ruoli oppure Ruoli o appartenenza ai gruppi.

- Valore attributo gruppo: selezionare il formato di valore appropriato per l'attributo gruppo. Le opzioni comuni includono Valori gruppo nidificati multipli o Valore singolo a seconda di come il provider di identità struttura le informazioni sul gruppo.

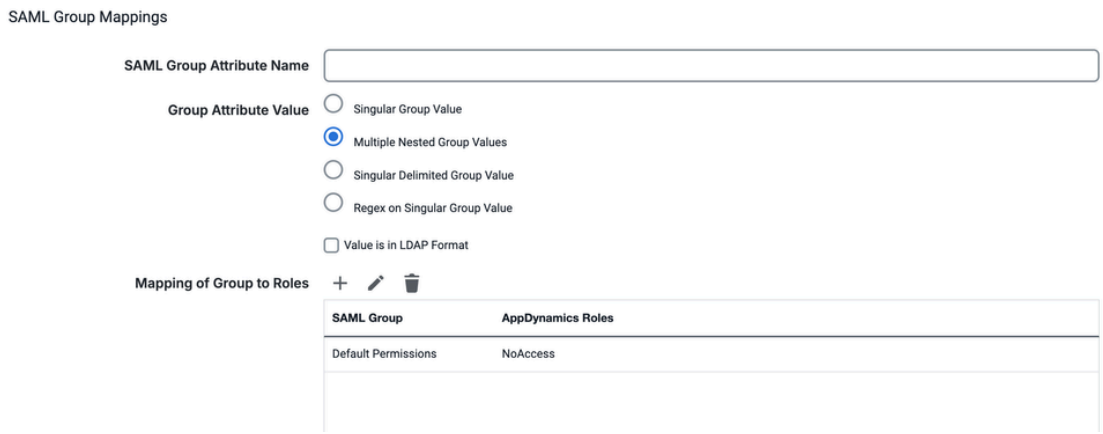


Nota: Selezionare Il valore è in formato LDAP se le informazioni sui gruppi sono in formato LDAP (Lightweight Directory Access Protocol).

- Mapping di gruppo a ruoli: fare clic sul pulsante + per aggiungere un nuovo mapping.
  - Gruppo SAML: immettere il nome del gruppo SAML (definito nel proprio IdP) di cui si desidera eseguire il mapping a un ruolo AppDynamics.
  - Ruoli: selezionare i ruoli AppDynamics corrispondenti dall'elenco disponibile che si desidera assegnare agli utenti appartenenti al gruppo SAML.
  - Autorizzazioni predefinite: se il mapping dei gruppi SAML non è configurato o se un'asserzione SAML utente non include informazioni sui gruppi, AppDynamics utilizza le autorizzazioni predefinite.



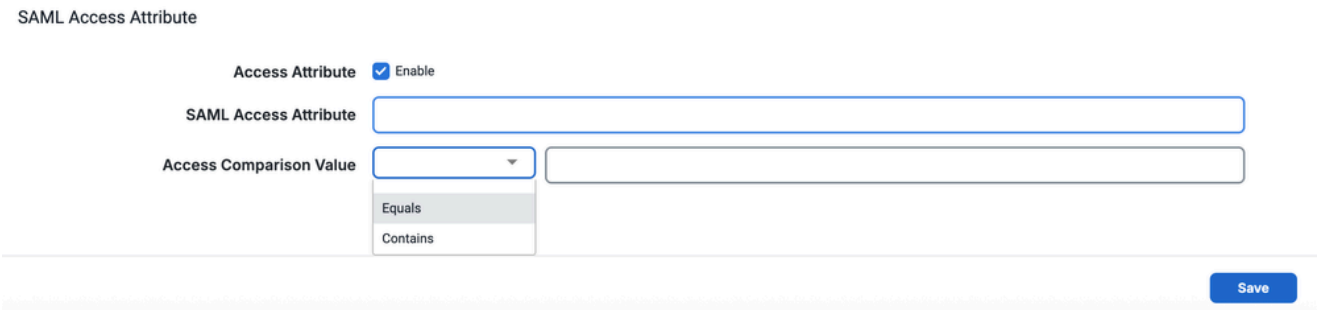
Nota: È consigliabile assegnare un ruolo con autorizzazioni minime a Autorizzazioni predefinite.



- Nella sezione Attributo di accesso SAML aggiungere i seguenti dettagli (facoltativo):
  - Attributo di accesso SAML: Immettere il nome degli attributi della risposta SAML. Verrà utilizzato per la convalida dell'accesso.

- Valore di confronto degli accessi: sono disponibili due opzioni:
  1. Uguale a: L'accesso viene concesso solo se il valore dell'attributo nella risposta SAML corrisponde esattamente al valore specificato nella configurazione.
  2. Contiene: L'accesso viene concesso se il valore dell'attributo nella risposta SAML contiene il valore specificato nella configurazione.
- Come funziona se abilitato:
  1. AppDynamics recupera l'attributo specificato nel campo Attributo di accesso SAML dalla risposta SAML.
  2. Il valore dell'attributo viene confrontato con il valore di confronto degli accessi definito dall'utente in base al metodo selezionato (Equal o Contains).
  3. Se il confronto ha esito positivo, all'utente viene concesso l'accesso.
  4. Se il confronto ha esito negativo, il tentativo di accesso viene negato.

- Fare clic su Save (angolo inferiore destro) per salvare la configurazione.



Verifica

- Aprire un browser e passare a AppDynamics Controller. Verrà visualizzata la finestra di dialogo Accedi per il servizio IdP di terze parti.
- Fare clic su Accedi con Single Sign-On. Il sistema reindirizza l'utente al proprio IdP.
- Immettere e inviare le credenziali.
- Una volta completata l'autenticazione, il provider di identità reindirizza l'utente al controller AppDynamics.

Problemi comuni e soluzioni

400 Richiesta non valida

- Problema: errore di richiesta non valida 400 durante il tentativo di accesso a AppDynamics Controller.
- Errore di esempio:

```
HTTP status 400 - Bad Request
Message: Error while processing SAML Authentication Response - see server log for details
Description: The request sent by the client was syntactically incorrect.
```

- Cause principali comuni:
    - Certificato SAML non valido
    - La lunghezza della risposta SAML è maggiore della lunghezza massima
    - ID entità o URL ACS non valido
- Soluzione:
    - Certificato SAML non valido
        - Verificare che il certificato fornito dal provider di identità (IdP) sia valido e aggiornato.
        - Verificare la data di scadenza del certificato del provider di identità. Se è scaduto, ottenere un nuovo certificato dal provider di identità.
        - Se il certificato è stato aggiornato sul lato IdP, verificare che il nuovo certificato sia caricato e configurato in AppDynamics.
        - Passaggi per aggiornare il certificato in AppDynamics:
            - Accedere all'interfaccia utente del controller come ruolo del proprietario dell'account o con l'autorizzazione Amministrazione, Agenti, Guida introduttiva.
            - Fare clic su Nome utente (angolo superiore destro)**>** Amministrazione **>** Provider di autenticazione **>** Seleziona SAML.
            - Nella sezione Configurazione SAML individuare il campo certificate e sostituire il vecchio certificato con quello nuovo fornito dall'IdP.
            - Fare clic su Save (Salva) per aggiornare la configurazione SAML.

    - La risposta SAML è maggiore della lunghezza massima.
        - Questo problema si verifica quando il controller viene spostato da GlassFish a Jetty Server, a partire dalla versione 23.11 del controller e successive. In Jetty Server è disponibile una proprietà denominata -Dorg.eclipse.jetty.server. Request.maxFormContentSize situato in .../appserver/jetty/start.d/start.ini. Se le dimensioni della risposta SAML superano il valore impostato per questa proprietà, il controller rifiuta il payload e restituisce una richiesta non valida 400 errore.
        - Cause delle risposte SAML grandi:
            - Attributi eccessivi: Troppi attributi inclusi nell'asserzione SAML.
            - Risposte SAML firmate o crittografate: La firma o la crittografia aumenta le dimensioni della risposta.
            - Dati aggiuntivi utente o gruppo: Il provider di identità (IdP) dispone di dati utente o gruppo aggiuntivi.

        - Esistono due modi per risolvere il problema. Implementando una o entrambe le soluzioni, è possibile risolvere il problema e impedire che il payload venga rifiutato.
            1. Aumentare il valore maxFormContentSize
                - Per i controller locali: Aggiornare la proprietà -Dorg.eclipse.jetty.server.Request.maxFormContentSize nel .../appserver/jetty/start.d/start.ini su un valore maggiore e riavviare il controller.

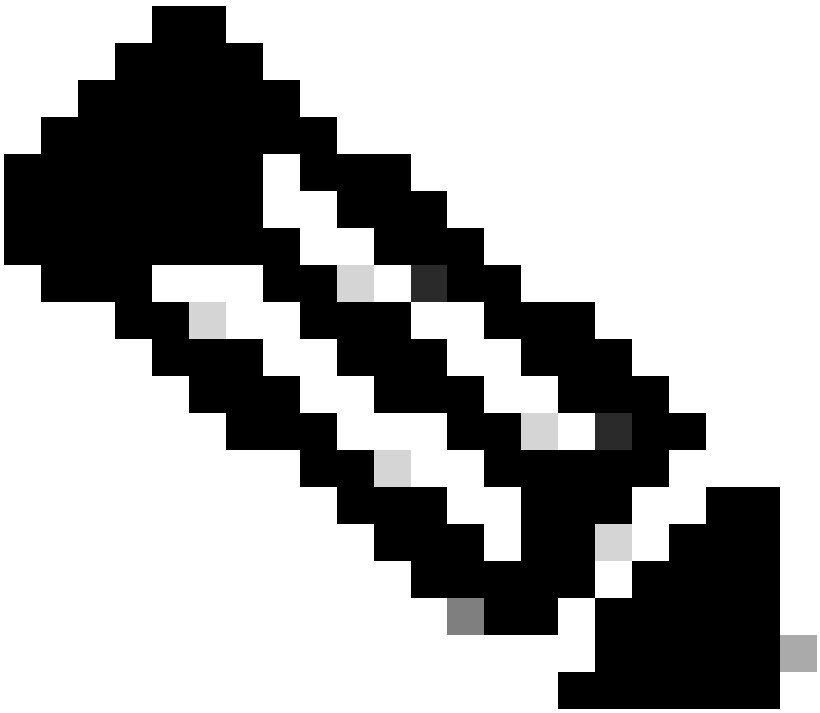
- Per i controller SaaS: Presentare un ticket di supporto per consentire al team di supporto di risolvere il problema.

2. Ottimizzazione della risposta SAML

   Collaborare con il provider di identità (IdP) per ridurre le dimensioni della risposta SAML apportando le seguenti modifiche:

   - Escludi attributi non necessari: Rimuovere gli attributi inutilizzati o ridondanti dall'asserzione SAML tramite la configurazione IdP.
   - Disabilita crittografia (se consentita): La crittografia aumenta le dimensioni della risposta SAML. Se la connessione è già protetta tramite HTTPS, disattivare la crittografia per ridurre le dimensioni.

- ID entità o URL ACS non valido
  - Sull'Idp:
    - Confermare che l'ID entità sia https://your_controller_domain/controller. Se l'ID entità è diverso, aggiornarlo.
    - Confermare che l'URL ACS sia https://your_controller_domain/controller/saml-auth?accountName=youraccountname. Se l'URL ACS è diverso, aggiornarlo di conseguenza.



Nota: AccountName deve corrispondere al nome dell'account AppDynamics. (ad esempio, cliente1)

- Autorizzazioni utente mancanti
  - Problema: l'accesso al controller è stato eseguito correttamente. Tuttavia, non sono stati ricevuti i ruoli e le autorizzazioni previsti.
  - Esempio di configurazione e risposta SAML:
    - Nell'utente SAML l l'attributo Group, name è Groups con i valori AppD_Admin & AppD_Power_User.

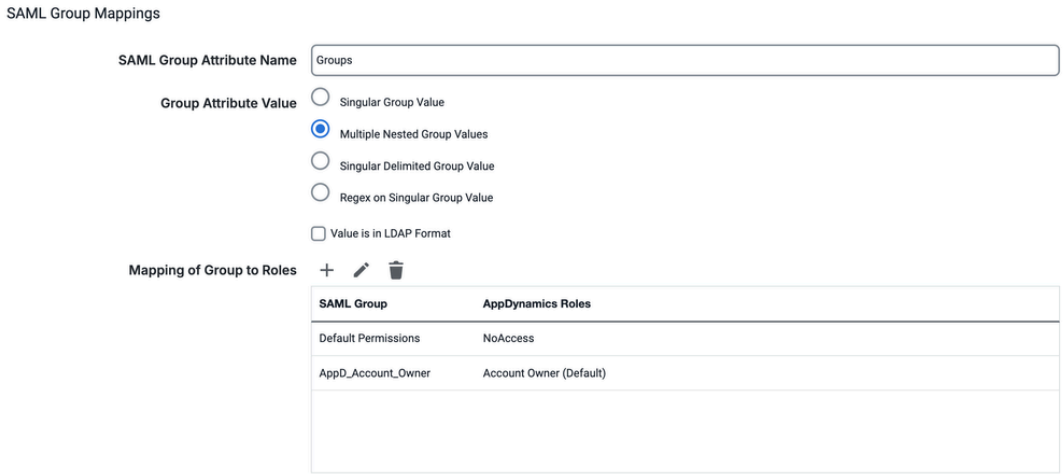
```
AppD_Admin
```

```
AppD_Power_User
```

    - In AppDynamics, nella sezione Mapping gruppi SAML, sono configurati.
      - Nome attributo gruppo SAML: Gruppi
      - Valore attributo gruppo: Valori di più gruppi nidificati
      - Mapping a ruoli di gruppo:

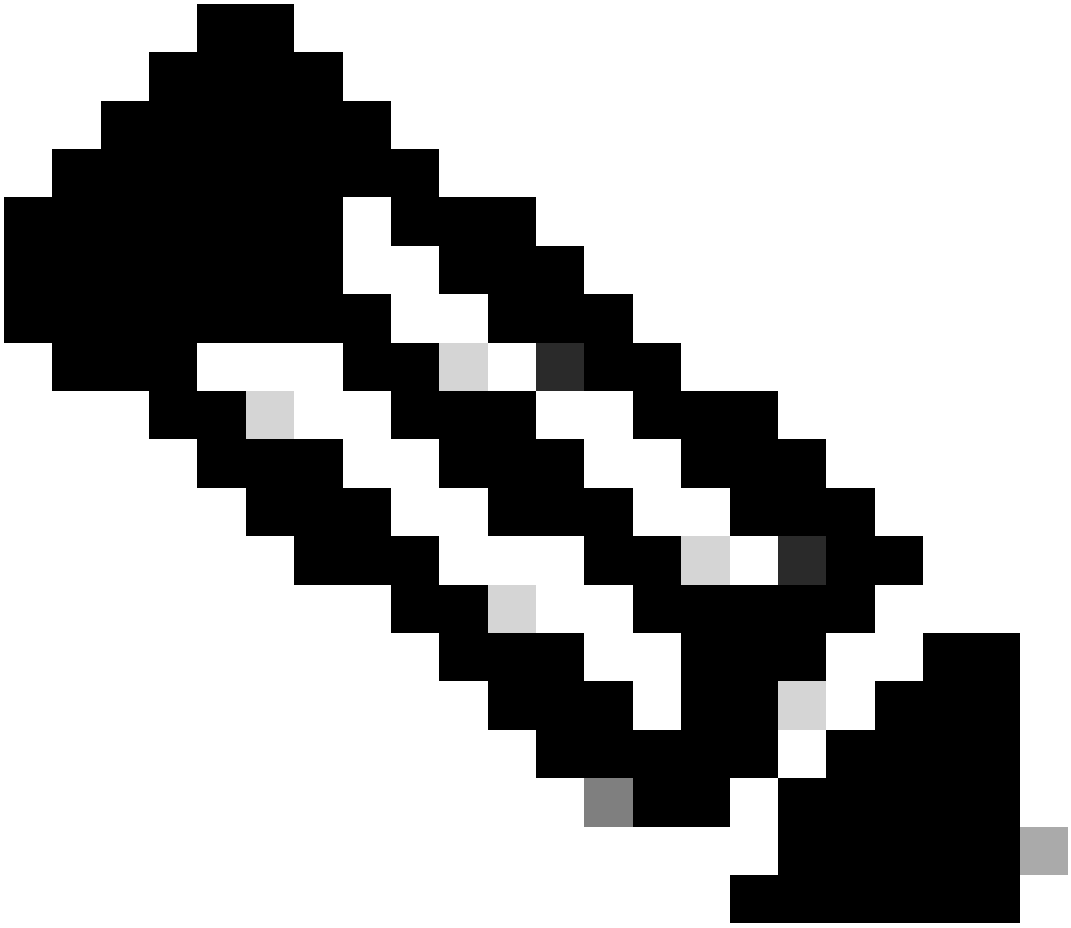
Gruppo SAML	Ruoli AppDynamics
Proprietario_account_App	Proprietario account (predefinito)
Autorizzazioni predefinite	Nessun accesso

        Nessun accesso è un ruolo personalizzato senza autorizzazioni.



- Problemi comuni e soluzione
  - Nessun attributo Group trovato nella risposta SAML.
    - Nella risposta SAML dell'IdP mancano gli attributi di gruppo richiesti oppure il nome dell'attributo per i gruppi nella risposta SAML è impostato come Ruoli mentre in AppDynamics è configurato come Gruppi.
    - Se non vengono specificati attributi di gruppo, all'utente vengono assegnati automaticamente i ruoli associati alle autorizzazioni predefinite in AppDynamics.
    - Per risolvere questo problema, verificare che l'IdP sia configurato per includere gli attributi di gruppo corretti nella risposta SAML e che il nome dell'attributo per i gruppi corrisponda alla configurazione in AppDynamics.

  - Nessun mapping di gruppi SAML corrispondente configurato in AppDynamics per i gruppi di utenti specificati nella risposta SAML.
    - Nella risposta SAML, l'attributo Groups contiene i valori AppD_Admin e AppD_Power_User. In AppDynamics, tuttavia, i mapping dei gruppi esistono solo per il gruppo AppD_Account_Owner.
    - Poiché non esiste alcun mapping corrispondente per AppD_Admin o AppD_Power_User, all'utente non vengono assegnati ruoli o autorizzazioni.
    - Per risolvere questo problema, aggiungere i mapping dei gruppi mancanti (ad esempio, AppD_Admin e AppD_Power_User) in AppDynamics per garantire l'assegnazione di ruoli e autorizzazioni appropriati.



Nota: Le autorizzazioni predefinite vengono applicate solo agli utenti SAML quando il nome dell'attributo del gruppo SAML configurato in AppDynamics non corrisponde agli attributi dei gruppi nella risposta SAML.

- Indirizzo di posta elettronica e/o nome degli utenti SAML mancante o non corretto
  - Problema: Questo si verifica in genere quando la configurazione Attribute in AppDynamics non corrisponde agli attributi inclusi nella risposta SAML.
  - Esempio di risposta SAML: Attributi Nella risposta SAML sono: User.email, User.fullName e Groups

example@domain.com

FirstName LastName

AppD_Admin

AppD_Power_User

- Esempio di mapping di attributi SAML in AppDynamics
  - Attributo nome utente: Nome.utente
  - Attributo nome visualizzato: User.firstName o vuoto
  - Attributo e-mail: User.userPrincipal o vuoto

    - Causa principale: gli attributi Display Name e Email configurati in AppDynamics non corrispondono ad alcuno degli attributi specificati nella risposta SAML.
        - Di conseguenza:
            - L'indirizzo di posta elettronica è vuoto.
            - Per impostazione predefinita, il nome visualizzato è il nome utente.

    - Soluzione: Verificare che gli attributi Display Name e Email configurati in AppDynamics corrispondano agli attributi corrispondenti nella risposta SAML.
        - Ad esempio:
            - Aggiornare l'attributo Display Name in User.fullName.
            - Aggiornare l'attributo Email in User.email.

- Errore HTTP 404

- Problema: l'utente non è in grado di accedere al controller e viene visualizzato il messaggio di errore 404 not found.
- Errore di esempio: Nei registri del controller (solo per il controller locale) viene visualizzato questo errore:

```
[#|2025-01-10T21:16:35.222+0000|SEVERE|glassfish 4.1|com.singularity.ee.controller.auth.saml.SAMLA
com.appdynamics.platform.services.auth.exception.SamlException: Requested url validation failed
    at com.appdynamics.platform.services.auth.impl.saml.SamlRequestResponseHandler.validateRequest
    at com.appdynamics.platform.services.auth.impl.saml.SamlRequestResponseHandler.getSamlAuthenti
```

- Causa principale: questo errore si verifica in genere quando l'URL del controller configurato nel database del controller non corrisponde all'URL del controller utilizzato per accedere o all'URL configurato nel provider di identità
- Soluzione:
    - Per i controller locali:
        - Eseguire questo comando per aggiornare l'URL del controller (scelta consigliata).

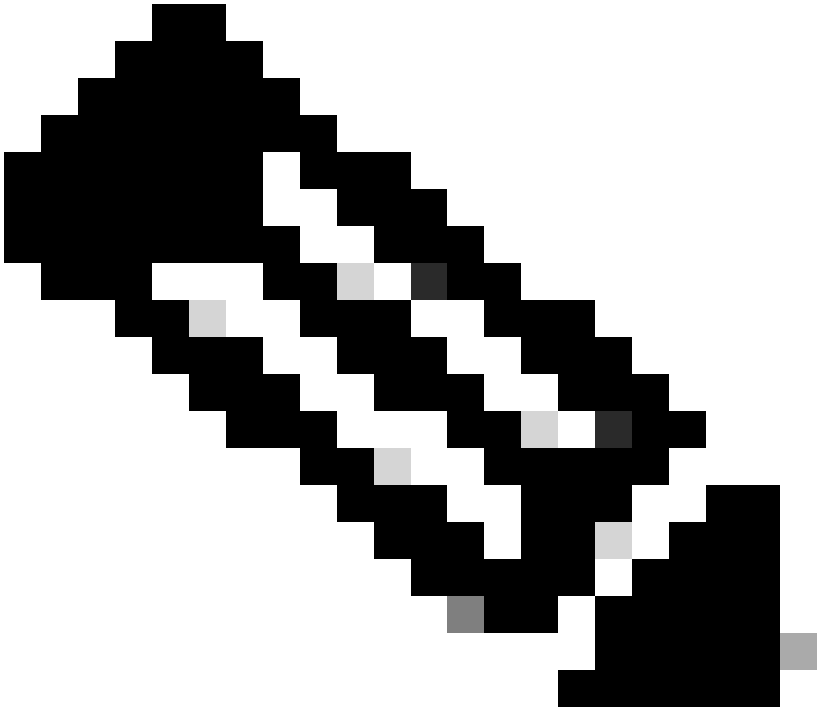
```
curl -k --basic --user root@system --header "Content-Type: application/json" --data '{

/controller" }' http://

/controller/rest/accounts/

/update-controller-url
```

- In alternativa, è possibile eseguire questi comandi nel database del controller per aggiornare l'URL del controller.

```
UPDATE controller.account SET controller_url ='

             ' WHERE id=

              ;
UPDATE mds_auth.account SET controller_url='

               ' WHERE name='

                ';
```

  - Eseguire questo comando per ottenere <ACCOUNT_ID>.

```
Select id from controller.account where name = '

                  ';
```



Nota: Eseguire curl -X POST -u root@system https://<dominio_controller>/controller/api/controllermds/syncAll se il problema persiste.

- Sostituisci:
  - <NEW_CONTROLLER_URL> con l'URL effettivo del controller utilizzato per accedere al controller.
  - <dominio_controller> con il dominio del controller.
  - <nomeaccount> con il nome dell'account.

- Per i controller SaaS: Presentare un ticket di supporto per consentire al team di supporto di risolvere il problema.

Ulteriore assistenza

In caso di domande o problemi, creare una richiesta di assistenza con i seguenti dettagli:

- Dettagli errore o schermata: fornire un messaggio di errore specifico o una schermata del problema.
- Risposta SAML: raccolta file SAML-Trace e HAR
- Controller Server.log (solo locale): se applicabile, fornire i registri del server controller da <controller-install-dir>/logs/server.log

Informazioni correlate

Documentazione di AppDynamics

SAML per distribuzioni SaaS

Crittografa risposte SAML per distribuzioni SaaS

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).