Configurar e solucionar problemas de logon único no AppDynamics

Contents

Introdução

Este documento descreve como configurar o Logon Único (SSO) no AppDynamics e solucionar problemas.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Para Configurar o Logon Único, o Usuário deve ter a função Proprietário da Conta (Padrão) ou uma função personalizada com a permissão Administração, Agentes e Assistente de Primeiros Passos.
- Acesso de administrador à sua IdPaccount.
- Os detalhes de metadados ou configuração do AppDynamics (por exemplo, ID da Entidade, URL do ACS).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador AppDynamics

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Single Sign-On (SSO) é um mecanismo de autenticação que permite que os usuários efetuem login uma vez e obtenham acesso a vários aplicativos, sistemas ou serviços sem precisar se autenticar novamente para cada um.

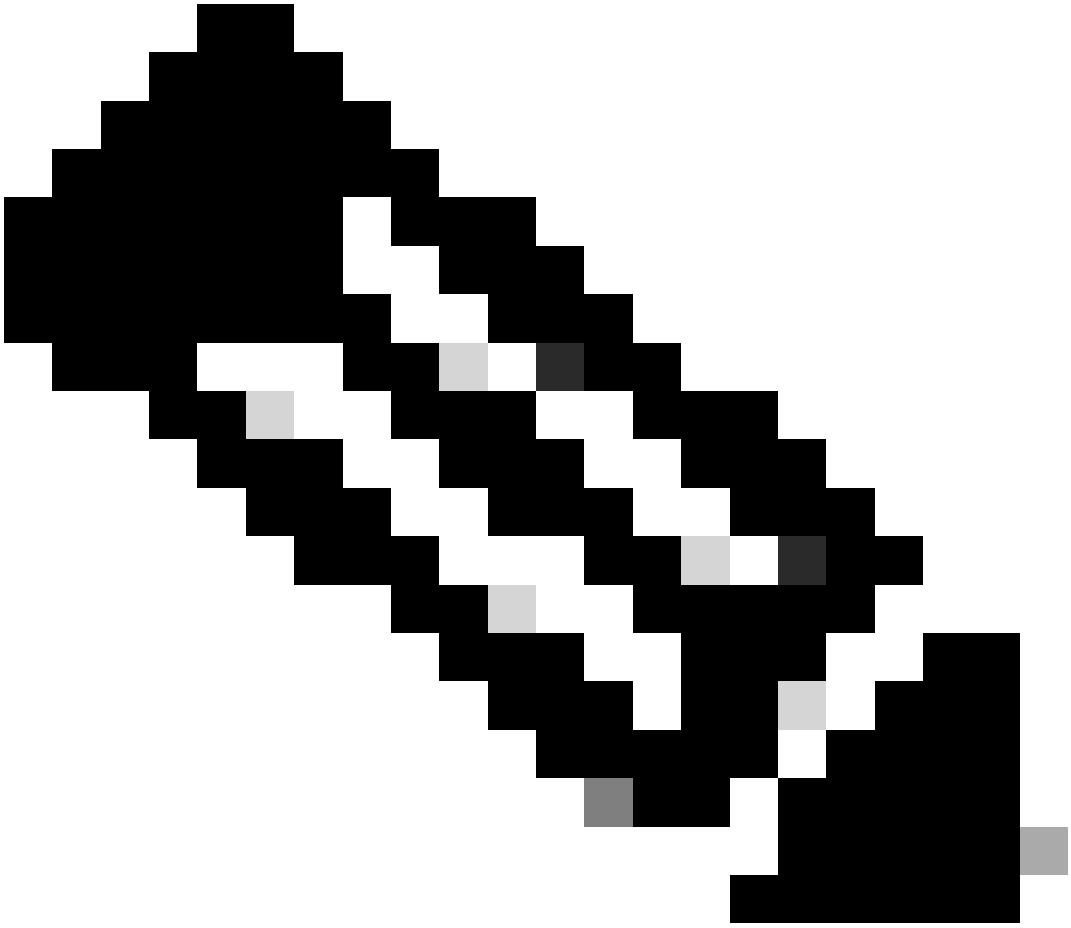
A SAML (Security Assertion Markup Language) é uma das tecnologias usadas para implementar o SSO. Ele fornece a estrutura e os protocolos que habilitam o SSO, trocando com segurança dados de autenticação e autorização entre um Identity Provider (IdP) e um Service Provider (SP).

Asserção SAML

- As mensagens baseadas em XML são trocadas entre o IdP e o SP.
- Ele fornece três tipos de asserções:
    - Asserções de autenticação: Confirma que o usuário foi autenticado.
    - Asserções de atributo: Compartilha atributos de usuário, como nome de usuário ou funções.
    - Afirmações de decisão de autorização: Indica o que o usuário está autorizado a fazer.

Funções-chave no SAML

- Provedor de identidade (IdP)
    - Verifica a identidade do Usuário.
    - Gerar a SAML Assertion que contém informações de identificação do usuário.
- Provedor de serviços (SP)
    - O aplicativo ou sistema que o usuário deseja acessar.
    - Depende do IdP para autenticar o usuário.
    - Aceita a asserção SAML para conceder ao usuário acesso a seus recursos ou aplicativos.
- Usuário (Principal)
    - O usuário real que inicia a solicitação ou tenta acessar um recurso do provedor de serviços.
    - Interage com o IdP (Autenticação) e o SP.



Note: O AppDynamics oferece suporte a SSO iniciado por IdP e iniciado por SP.

Fluxo iniciado pela controladora:

- O usuário navega para o provedor de serviços digitando a URL do aplicativo (por exemplo, AppDynamics) ou clicando em um link.
- A controladora de armazenamento verifica se há uma sessão existente. Se não houver sessão, a controladora de armazenamento reconhecerá que o usuário não está autenticado e iniciará o processo SSO.
- A controladora gera uma solicitação de autenticação SAML e redireciona o usuário para o IdP para autenticação.
    - Esse pedido inclui:
        - ID da entidade: Identificador exclusivo do provedor de serviços.
        - URL do Serviço de Consumidor de Asserção (ACS): em que o IdP envia a SAML Assertion após a autenticação.
        - Metadados sobre a controladora e detalhes de segurança (por exemplo, solicitação assinada, requisitos de criptografia).

- O usuário é redirecionado para a página de login do IdP.
- O IdP autentica o usuário (por exemplo, através de nome de usuário/senha ou autenticação multifator).
- Após a autenticação bem-sucedida, o IdP gera uma SAML Assertion (token de segurança).
- A SAML Assertion é enviada de volta ao SP através do navegador do usuário usando a vinculação HTTP POST (na maioria dos casos) ou a vinculação HTTP Redirect.
- O SP valida a SAML Assertion para garantir:
    - Foi emitido pelo IdP confiável.
    - Ele é endereçado ao SP (por meio da ID de entidade do SP).
    - Ele não expirou ou foi violado (validado usando a chave pública IdP).

- Se a SAML Assertion for válida, o SP criará uma sessão para o usuário.
- O usuário recebe acesso ao aplicativo ou aos recursos.

Fluxo iniciado por IdP:

- O usuário navega para o portal de login do IdP e digita suas credenciais.
- O IdP autentica o usuário (por exemplo, com uma combinação de nome de usuário/senha, autenticação multifator).
- Após a autenticação, o IdP apresenta ao usuário uma lista de aplicativos ou serviços (SPs) disponíveis que ele pode acessar.
- O usuário seleciona o SP desejado (por exemplo, AppDynamics).
- O IdP gera uma SAML Assertion para a controladora de armazenamento selecionada.

- O IdP redireciona o usuário para a URL do SP Assertion Consumer Service (ACS) e envia a SAML Assertion junto com ela (usando a Associação HTTP POST ou a Associação HTTP Redirect).
- O SP recebe a SAML Assertion e a valida:
    - Garante que a asserção seja emitida por um IdP confiável.
    - Verifica a integridade e a expiração da asserção.
    - Confirma a identidade do usuário e outros atributos.

- Se a SAML Assertion for válida, o SP criará uma sessão para o usuário.
- O usuário recebe acesso ao aplicativo ou aos recursos.

Configurar

O AppDynamics Controller pode usar a Cisco Customer Identity ou um provedor de identidade SAML (IdP) externo para autenticar e autorizar usuários.

Provedores de identidade suportados

O AppDynamics certifica suporte para estes provedores de identidade (IdPs):

- Okta
- Onelogin
- Identidade do ping

- AD do Azure
- Identidade de nuvem da IBM
- Serviço de Federação do Ative Diretory (AD FS)

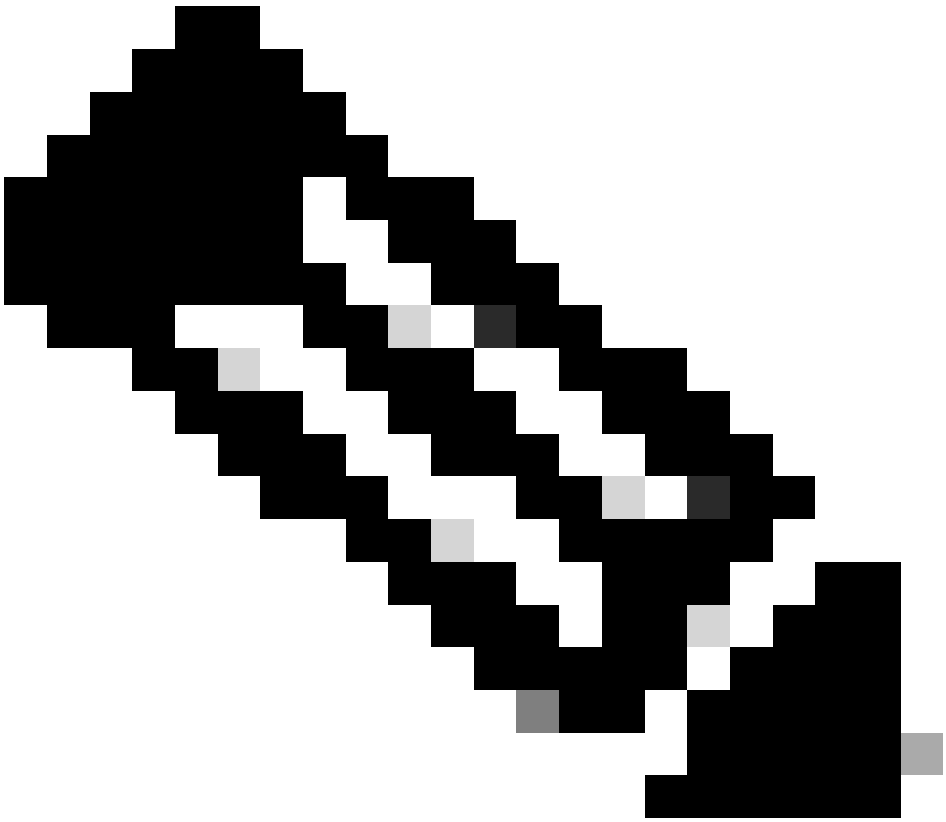
Outros IdPs que suportam associação HTTP POST também são compatíveis com a autenticação AppDynamics SAML.

Etapas para Configurar SAML no AppDynamics

Etapa 1. Coletar Detalhes do AppDynamics Controller

- ID da entidade (ID da entidade SP): um identificador exclusivo do AppDynamics (por exemplo, https://<host-controlador>:<porta>/controlador).
    - Sintaxe: https://<domínio_do_controlador>/controlador
    - exemplo: https://<your_controller_domain>/controller

- URL de Resposta (Assertion Consumer Service, ACS URL): o ponto de extremidade no Provedor de Serviços (por exemplo, AppDynamics) em que o IdP envia a resposta SAML após a autenticação.
    - Sintaxe: https://<domínio_do_controlador>/controller/saml-auth?accountName=<nome_da_conta>
    - exemplo: https://your_controller_domain/controller/saml-auth?accountName=youraccountname



Note: No caso do controlador Local, o nome da conta padrão é customer1, a menos que você tenha um controlador multilocatário com accountName diferente.

- URL de logoff único (opcional): o ponto final no SP para lidar com solicitações de logoff SAML (por exemplo, https://<domínio_controlador>/controlador).

Etapa 2. Criar um novo Aplicativo no IdP e Fazer Download dos Metadados

- Localize a área de criação de aplicativos: Geralmente, ela está dentro do console ou painel administrativo do IdP, geralmente rotulado como Aplicativos, Aplicativos Web e Móveis, Aplicativos Corporativos ou Terceiras Partes Confiáveis.
- Adicionar um aplicativo SAML personalizado ou genérico: Selecione uma opção que permita configurar um aplicativo SAML personalizado ou uma integração de provedor de serviços SAML genérico.
- Forneça detalhes do aplicativo: dê um nome ao aplicativo e carregue um ícone para identificação (opcional).
- Adicione mapeamentos de atributo (Nome de usuário, nome para exibição, email ou funções) para passar informações de usuário para o AppDynamics.
- Baixe o arquivo de metadados IdP ou, como alternativa, anote estes detalhes:
  - URL de login do IdP

- URL de logoff
- Nomes de atributo
- Certificado

Etapa 3. Configurar a Autenticação SAML no AppDynamics Controller

- Faça login na interface do usuário do controlador como uma função de proprietário de conta ou uma função com a permissão Administração, Agentes, Assistente de introdução.
- Clique no Nome de usuário(canto superior direito)> Administração > Provedor de autenticação > Selecionar SAML.

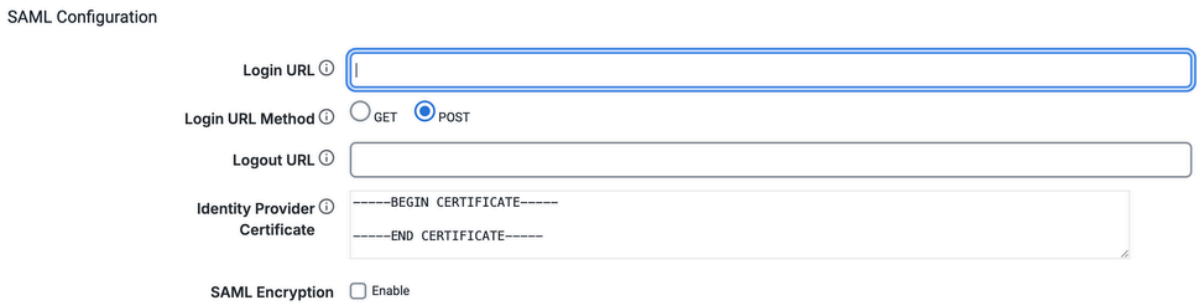
- Na seção Configuração SAML, adicione estes detalhes:

  - URL de login: A URL de Logon do IdP em que o AppDynamics Controller roteia solicitações de logon iniciadas pelo Provedor de Serviços (SP).

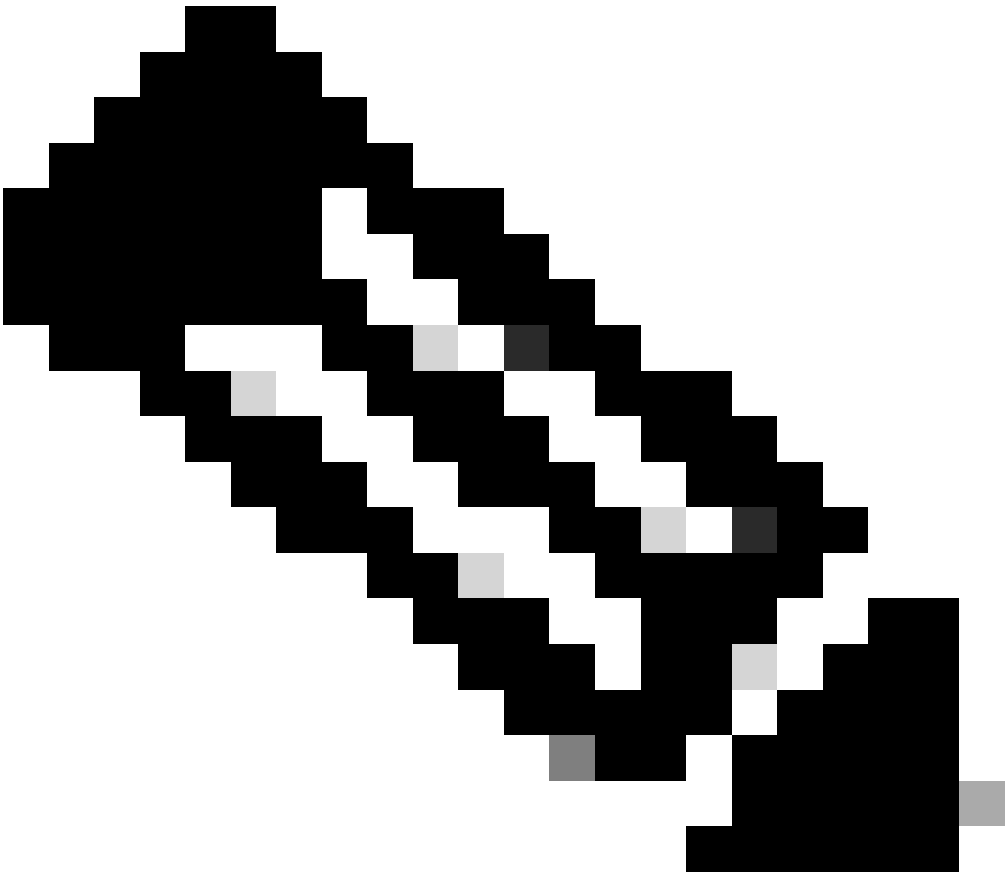
  - URL de logoff (opcional): A URL em que o AppDynamics Controller redireciona os usuários após o logoff. Se você não especificar uma URL de logoff, os usuários obterão a tela de logon do AppDynamics quando fizerem logoff.

  - Certificado: O certificado X.509 do IdP. Cole o certificado entre os delimitadores BEGIN CERTIFICATE e END CERTIFICATE. Evite duplicar os delimitadores BEGIN CERTIFICATE e END CERTIFICATE a partir do próprio certificado de origem.

  - Criptografia SAML (Opcional): você pode melhorar a segurança da autenticação SAML criptografando a resposta SAML do IdP para o provedor de serviços. Para criptografar respostas SAML no AppDynamics, você precisa configurar seu IdP (Provedor de Identidade) para criptografar a asserção SAML e depois configurar o AppDynamics Controller para usar um certificado e uma chave privada específicos para descriptografia.



- Na seção Mapeamentos de atributos SAML, mapeie os atributos SAML (exemplo: Nome de usuário, Nome para exibição, Email) para seus campos correspondentes no AppDynamics.

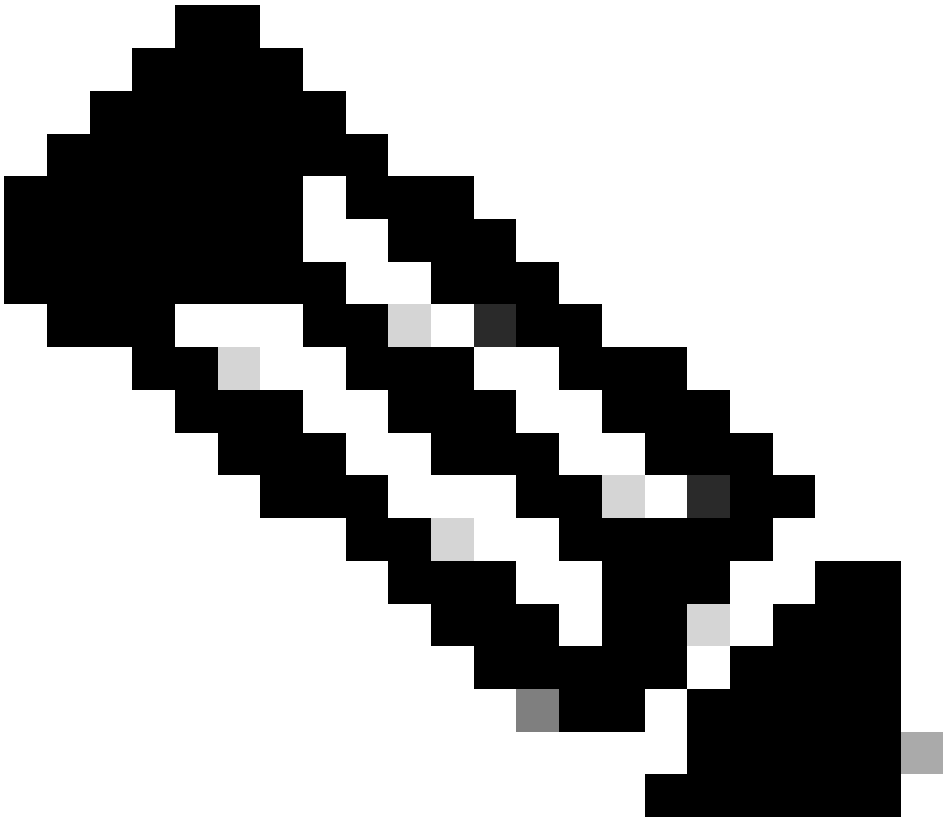


Note: O AppDynamics exibe o nome de usuário, email e nome de exibição de um usuário SAML. Por padrão, ele usa o atributo NameID da resposta SAML para criar um nome de usuário, que também é usado como displayName. Esse comportamento pode ser personalizado incluindo os atributos username, email e displayname na resposta SAML. Ao definir as configurações de IdP no AppDynamics, o usuário pode especificar esses nomes de atributo. Durante o logon, o AppDynamics verifica se o mapeamento de atributos está configurado. Se os mapeamentos estiverem configurados e atributos correspondentes estiverem presentes na resposta SAML, o AppDynamics usará esses valores de atributo para definir o nome de usuário, o email e o nome para exibição.

- Na seção Mapeamentos do grupo SAML, adicione esses detalhes.
  - Nome do Atributo do Grupo SAML: Informe o nome do atributo SAML que contém as

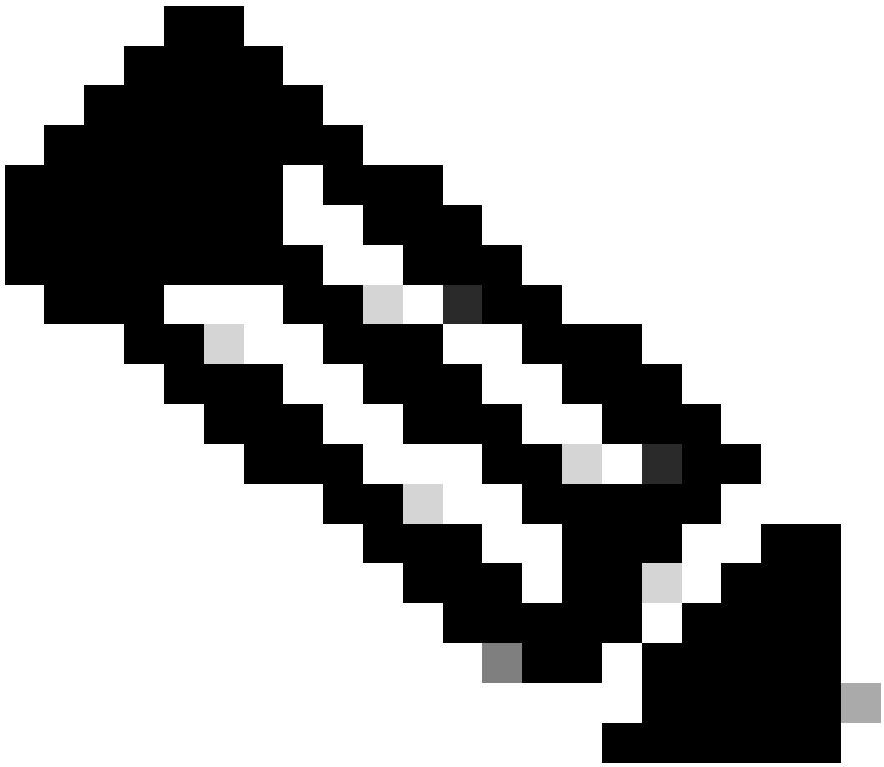
informações do grupo. Normalmente, são Grupos, ou grupo ou funções, ou Funções ou associação de grupo.

- Valor do Atributo do Grupo: Selecione o formato de valor apropriado para o atributo do grupo. As opções comuns incluem Vários Valores de Grupos Aninhados ou Valor Único, dependendo de como seu IdP estrutura as informações do grupo.

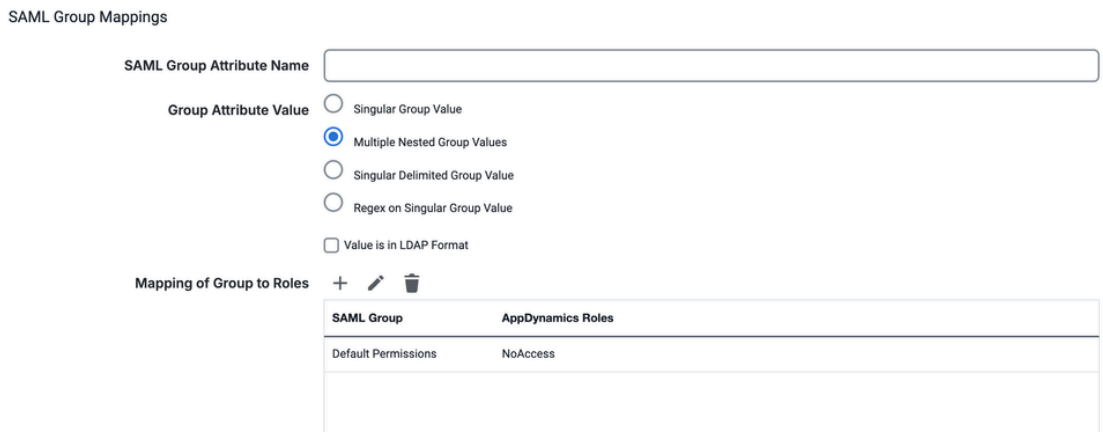


Note: Selecione O valor está no formato LDAP se as informações do grupo estiverem chegando no formato LDAP (Lightweight Diretory Access Protocol).

- Mapeamento de grupos para funções: clique no botão + para adicionar um novo mapeamento.
  - Grupo SAML: insira o nome do grupo SAML (conforme definido no seu IdP) que você deseja mapear para uma função do AppDynamics.
  - Função(ões): Selecione a(s) função(ões) AppDynamics correspondente(s) na lista disponível que você deseja atribuir aos usuários pertencentes ao grupo SAML.
  - Permissões Padrão: se o mapeamento de grupo SAML não estiver configurado ou se uma asserção SAML do usuário não incluir informações de grupo, o AppDynamics voltará a usar permissões padrão.



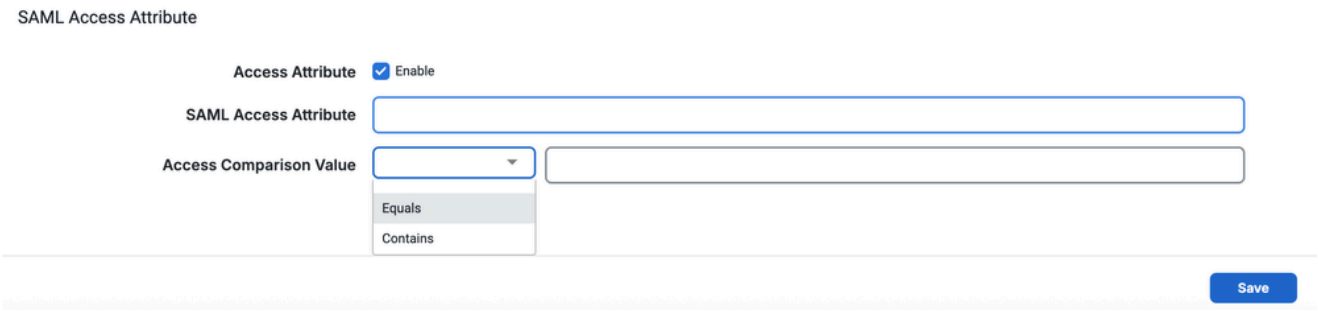
Note: É recomendável atribuir uma função com permissões mínimas às permissões padrão.



- Na seção Atributo de Acesso SAML, adicione estes detalhes (Opcional):
  - Atributo de acesso SAML: Digite o nome dos atributos da resposta SAML. Isso será usado para validação de acesso.

- Valor de Comparação de Acesso: Há duas opções disponíveis:
    1. Igual: O acesso será concedido somente se o valor do atributo na resposta SAML corresponder exatamente ao valor especificado na configuração.
    2. Contém: O acesso será concedido se o valor do atributo na resposta SAML contiver o valor especificado na configuração.
- Como funciona se estiver habilitado:
    1. O AppDynamics recupera o atributo especificado no campo Atributo de Acesso SAML da resposta SAML.
    2. Ele compara o valor do atributo com o Valor de comparação de acesso definido pelo usuário com base no método selecionado (Igual ou Contém).
    3. Se a comparação for bem-sucedida, o usuário receberá acesso.
    4. Se a comparação falhar, o log na tentativa será negado.

- Clique em Save (Salvar) (canto inferior direito) para salvar a configuração.



Verificar

- Abra um navegador e navegue até o AppDynamics Controller. A caixa de diálogo Logon do serviço IdP de terceiros é exibida.
- Clique em Login com Logon Único. O sistema o redireciona para o seu IdP.
- Insira e envie suas credenciais.
- Após a autenticação bem-sucedida, o IdP o redirecionará para o AppDynamics Controller.

Problemas e soluções comuns

400 Solicitação Incorreta

- Problema: os usuários encontram um erro de Solicitação Inválida 400 ao tentar fazer logon no AppDynamics Controller.
- Exemplo de erro:

```
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.
```

- Causas principais comuns:
    - Certificado SAML inválido
    - A Resposta SAML é maior que o comprimento máximo
    - ID da entidade ou URL do ACS inválida
- Solução:
    - Certificado SAML inválido
        - Verifique se o certificado fornecido pelo IdP (Provedor de Identidade) é válido e está atualizado.
        - Verifique a data de expiração do certificado IdP. Se tiver expirado, obtenha um novo certificado do IdP.
        - Se o certificado tiver sido atualizado no lado do IdP, verifique se o novo certificado foi carregado e configurado no AppDynamics.
        - Etapas para atualizar o certificado no AppDynamics:
            - Faça logon na interface do usuário do controlador como uma função de proprietário da conta ou uma função com permissão de Administração, Agentes, Assistente de Primeiros Passos.
            - Clique no Nome de usuário(canto superior direito)> Administração > Provedor de autenticação > Selecionar SAML.
            - Na seção SAML Configuration, localize o campo certificate e substitua o certificado antigo pelo novo fornecido pelo IdP.
            - Clique em Salvar para atualizar a configuração do SAML.

    - A Resposta SAML é maior que o comprimento máximo.
        - Esse problema ocorre quando a controladora é movida do GlassFish para o Jetty Server, começando com a versão da controladora 23.11 e posterior. No servidor Jetty, há uma propriedade chamada -Dorg.eclipse.jetty.server. Request.maxFormContentSize localizado na ...Arquivo /appserver/jetty/start.d/start.ini. Se o tamanho da resposta SAML exceder o valor definido para esta propriedade, o controlador rejeitará a carga e retornará uma solicitação 400 incorreta erro.
        - Causas de Respostas SAML Grandes:
            - Excesso de atributos: Muitos atributos incluídos na asserção SAML.
            - Respostas SAML assinadas ou criptografadas: Assinatura ou criptografia aumenta o tamanho da resposta.
            - Dados adicionais do usuário ou grupo: O IdP (Provedor de Identidade) tem dados de usuário ou grupo extras.

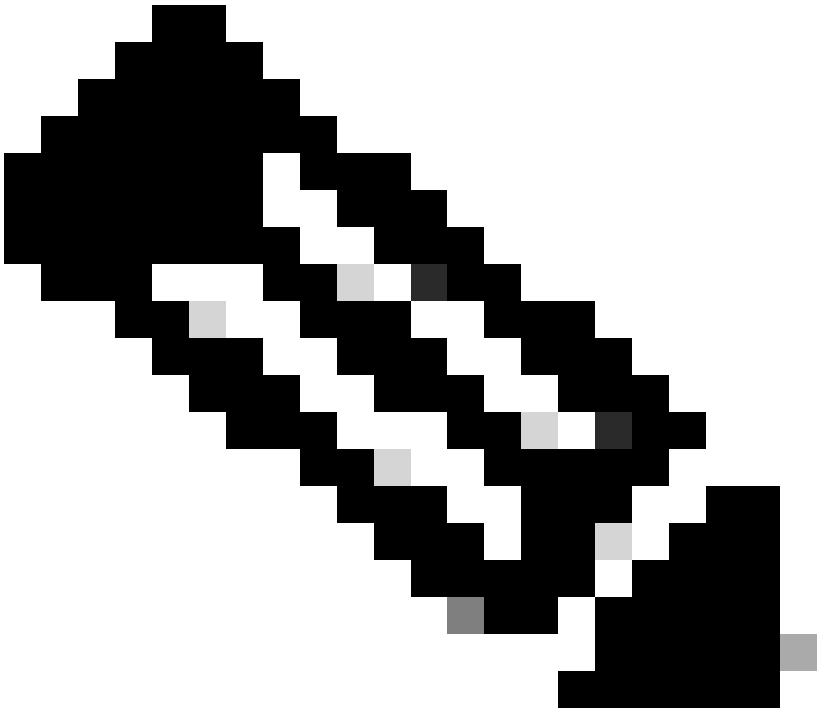
        - Há duas maneiras de resolver esse problema. Implementando uma ou ambas as soluções, você pode resolver o problema e evitar que o payload seja rejeitado.
            1. Aumente o valor de maxFormContentSize
                - Para controladores no local: Atualize a propriedade -Dorg.eclipse.jetty.server.Request.maxFormContentSize no .../appserver/jetty/start.d/start.ini com um valor maior e reinicie o controlador.
                - Para controladores SaaS: Registre um tíquete de suporte para que esse problema seja resolvido pela equipe de suporte.

2. Otimizar a Resposta SAML

   Trabalhe com o seu Provedor de Identidade (IdP) para reduzir o tamanho da resposta SAML, fazendo estes ajustes:

   - Excluir atributos desnecessários: Remova atributos não utilizados ou redundantes da asserção SAML por meio da configuração do IdP.
   - Desativar criptografia (se permitido): A criptografia aumenta o tamanho da resposta SAML. Se a conexão já estiver protegida por HTTPS, considere desativar a criptografia para reduzir o tamanho.

- ID da entidade ou URL do ACS inválida
  - No Idp:
    - Confirme se a ID da entidade é https://your_controller_domain/controller. Se a ID da entidade for diferente, atualize-a.
    - Confirme se a URL do ACS é https://your_controller_domain/controller/saml-auth?accountName=youraccountname. Se o URL do ACS for diferente, atualize-o de acordo.



Note: accountName deve corresponder ao nome da sua conta do AppDynamics. (por exemplo, cliente1)

- Permissões de Usuário Ausentes

- Problema: Você se conectou com êxito ao controlador. No entanto, você não recebeu as funções e permissões desejadas.
- Exemplo de configuração e resposta SAML:
  - No usuário SAML do atributo Grupo, o nome é Grupos com valores AppD_Admin e AppD_Power_User.

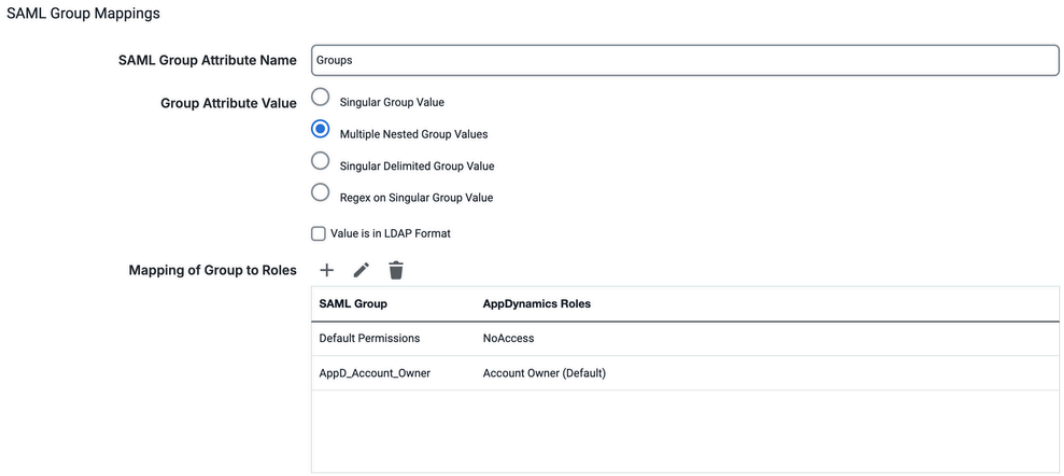
```
AppD_Admin
```

```
AppD_Power_User
```

  - No AppDynamics, na seção Mapeamentos de Grupo SAML, eles são configurados.
    - Nome do atributo do grupo SAML: Grupos
    - Valor do atributo do grupo: Vários valores de grupos aninhados
    - Mapeamento para funções de grupo:

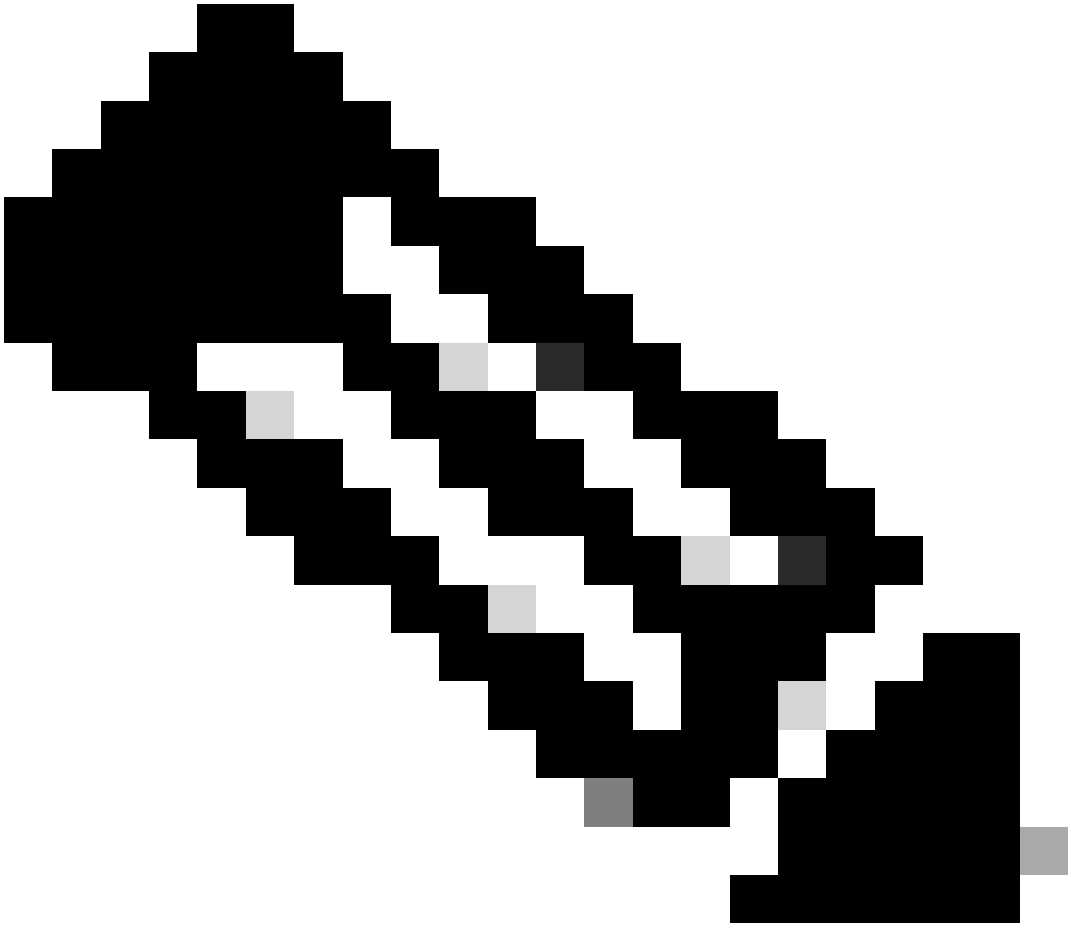
Grupo SAML	Funções do AppDynamics
AppD_Account_Owner	Proprietário da Conta (Padrão)
Permissões padrão	Sem acesso

      Sem acesso é uma função personalizada sem permissões.



- Problemas comuns e solução
  - Nenhum atributo de grupo encontrado na resposta SAML.
    - A resposta SAML do IdP não tem os atributos de grupo necessários ou o nome do atributo para grupos na resposta SAML está definido como Funções enquanto no AppDynamics, ele está configurado como Grupos.
    - Quando nenhum atributo de grupo é fornecido, as funções associadas às permissões padrão no AppDynamics são atribuídas automaticamente ao usuário.
    - Para resolver isso, verifique se o IdP está configurado para incluir os atributos de grupo corretos na resposta SAML e se o nome do atributo para grupos corresponde à configuração no AppDynamics.

  - Não há mapeamento de grupo SAML correspondente configurado no AppDynamics para os grupos de usuários fornecidos na resposta SAML.
    - Na resposta SAML, o atributo Grupos contém os valores AppD_Admin e AppD_Power_User. No entanto, no AppDynamics, os mapeamentos de grupo existem apenas para o grupo AppD_Account_Owner.
    - Como não há mapeamento correspondente para AppD_Admin ou AppD_Power_User, nenhuma função ou permissão foi atribuída ao usuário.
    - Para resolver isso, adicione os mapeamentos de grupo ausentes (por exemplo, AppD_Admin e AppD_Power_User) no AppDynamics para garantir a atribuição adequada de função e permissão.



Note: As permissões padrão só são aplicadas aos usuários SAML quando o Nome do atributo do grupo SAML configurado no AppDynamics não é o mesmo que os atributos Groups na resposta SAML.

- E-mail e/ou nome incorreto ou ausente para usuários SAML
  - Problema: Isso geralmente acontece quando a configuração de Atributo no AppDynamics não corresponde aos atributos que vêm na resposta SAML.
  - Exemplo de resposta SAML: Os atributos na resposta SAML são: User.email, User.fullName e Grupos

example@domain.com

FirstName LastName

AppD_Admin

AppD_Power_User

- Exemplo de mapeamentos de atributos SAML no AppDynamics
  - Atributo de nome de usuário: Nome.usuário
  - Atributo do nome de exibição: User.firstName ou vazio
  - Atributo de email: User.userPrincipal ou em branco

- Causa Raiz: os atributos de Nome para Exibição e Email configurados no

AppDynamics não correspondem a nenhum dos atributos fornecidos na resposta SAML.
    - Como resultado:
        - O email está definido como em branco.
        - O nome de exibição é padronizado para o nome de usuário.

- Solução: Verifique se os atributos de Nome para Exibição e Email configurados no AppDynamics correspondem aos atributos correspondentes na resposta SAML.
    - Por exemplo:
        - Atualize o atributo Display Name para User.fullName.
        - Atualize o atributo Email para User.email.

- Erro HTTP 404

- Problema: O usuário não consegue fazer login no controlador e obtém o erro 404 não encontrado.
- Exemplo de erro: Nos logs do controlador (somente para o controlador local) você vê este erro:

```
[#|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 Raiz: esse erro geralmente ocorre quando a URL do Controlador configurada no banco de dados do Controlador não corresponde à URL do Controlador usada para Fazer Logon ou à URL configurada no IdP
- Solução:
    - Para controladores no local:
        - Execute este comando para atualizar a URL da controladora (recomendado).

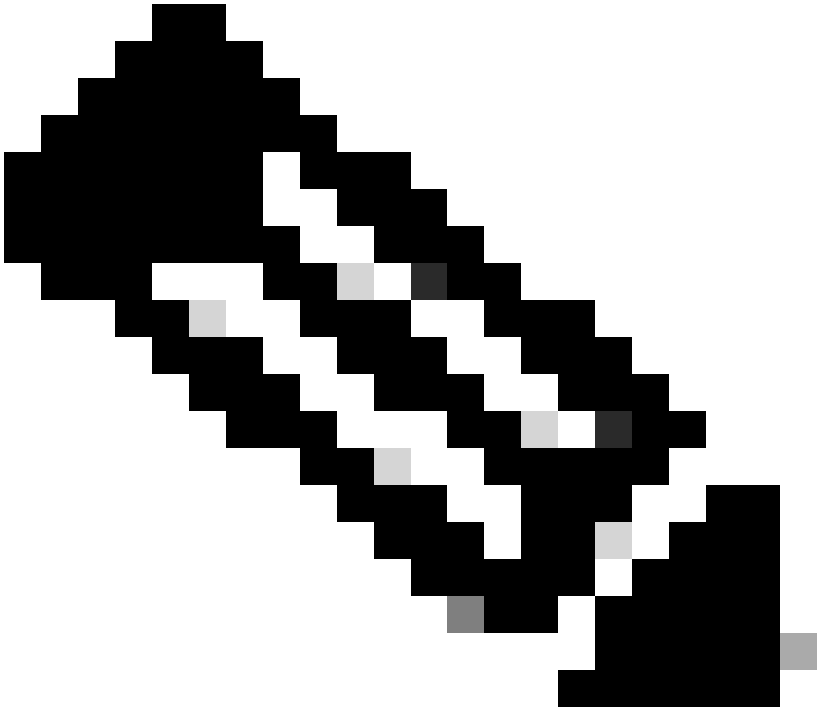
```
curl -k --basic --user root@system --header "Content-Type: application/json" --data '{

/controller" }' http://

/controller/rest/accounts/

/update-controller-url
```

- Como alternativa, você pode executar esses comandos no banco de dados do controlador para atualizar o URL do controlador.

```
UPDATE controller.account SET controller_url ='

            ' WHERE id=

             ;
UPDATE mds_auth.account SET controller_url='

              ' WHERE name='

               ';
```

  - Execute este comando para obter a <ACCOUNT_ID>.

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

                ';
```



Note: Execute curl -X POST -u root@system https://<domínio_controlador>/controller/api/controllermds/syncAll se ainda observar o mesmo problema.

- Substituir:
  - <NEW_CONTROLLER_URL> com o URL real do controlador que você está usando para acessar o controlador.
  - <controller_domain> com o domínio do controlador.
  - <youraccountname> com o nome da sua conta.

- Para controladores SaaS: Registre um tíquete de suporte para que esse problema seja resolvido pela equipe de suporte.

Precisa de mais assistência

Se você tiver uma dúvida ou estiver tendo problemas, crie um tíquete de suporte com estes detalhes:

- Detalhes do erro ou Captura de tela: forneça uma mensagem de erro específica ou uma captura de tela do problema.
- Resposta SAML: Coletar Rastreamento SAML e Arquivo HAR
- Controller Server.log (somente no local): Se aplicável, forneça os registros do servidor do controlador em <controller-install-dir>/logs/server.log

Informações Relacionadas

Documentação do AppDynamics

SAML para implantações de SaaS

Criptografar respostas SAML para implantações de SaaS

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.