Gerenciando configurações de autenticação SAML

Active IQ Unified Manager 9.7

NetApp
October 22, 2024

Índice

Gerenciando configurações de autenticação SAML

Depois de configurar as configurações de autenticação remota, é possível ativar a autenticação SAML (Security Assertion Markup Language) para que os usuários remotos sejam autenticados por um provedor de identidade seguro (IDP) antes que eles possam acessar a IU da Web do Unified Manager.

Observe que somente usuários remotos terão acesso à interface gráfica do usuário do Unified Manager depois que a autenticação SAML for ativada. Os utilizadores locais e os utilizadores de manutenção não poderão aceder à IU. Essa configuração não afeta os usuários que acessam o console de manutenção.

Requisitos do provedor de identidade

Ao configurar o Unified Manager para usar um provedor de identidade (IDP) para executar a autenticação SAML para todos os usuários remotos, você precisa estar ciente de algumas configurações necessárias para que a conexão com o Unified Manager seja bem-sucedida.

É necessário inserir o URI e os metadados do Unified Manager no servidor IDP. Você pode copiar essas informações da página Autenticação do Unified ManagerSAML. O Unified Manager é considerado o provedor de serviços (SP) no padrão SAML (Security Assertion Markup Language).

Padrões de criptografia suportados

- AES (Advanced Encryption Standard): AES-128 e AES-256
- Algoritmo Hash seguro (SHA): SHA-1 e SHA-256

Provedores de identidade validados

- Shibboleth
- Serviços de Federação do ative Directory (ADFS)

Requisitos de configuração ADFS

- Você deve definir três regras de reivindicação na ordem a seguir, necessárias para que o Unified Manager analise respostas ADFS SAML para essa entrada confiável de parte confiável.

Regra de reclamação	Valor
Nome da conta SAM	ID do nome
Nome da conta SAM	urna:oid:0.9.2342.19200300.100.1.1
Grupos de token — Nome não qualificado	urna:oid:1.3.6.1.4.1.5923.1.5.1.1

- Você deve definir o método de autenticação como ""Autenticação de formulários""" ou os usuários podem

receber um erro ao fazer logout do Unified Manager . Siga estes passos:

a. Abra o Console de Gerenciamento ADFS.

b. Clique na pasta Authentication Policies (políticas de autenticação) no modo de exibição de árvore à esquerda.

c. Em ações à direita, clique em Editar política de autenticação primária global.

d. Defina o método de autenticação da Intranet como ""Autenticação de formulários"" em vez da "Autenticação do Windows" padrão.

- Em alguns casos, o login pelo IDP é rejeitado quando o certificado de segurança do Unified Manager é assinado pela CA. Existem duas soluções alternativas para resolver este problema:
  - Siga as instruções identificadas no link para desativar a verificação de revogação no servidor ADFS para a entidade dependente associada a cert AC encadeada:

    http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/

  - Peça que o servidor da CA resida no servidor ADFS para assinar a solicitação de cert do servidor do Unified Manager.

Outros requisitos de configuração

- O desvio do relógio do Unified Manager é definido para 5 minutos, portanto, a diferença de tempo entre o servidor IDP e o servidor do Unified Manager não pode ser superior a 5 minutos ou a autenticação falhará.

Habilitando a autenticação SAML

Você pode ativar a autenticação SAML (Security Assertion Markup Language) para que os usuários remotos sejam autenticados por um provedor de identidade seguro (IDP) antes que eles possam acessar a IU da Web do Unified Manager.

Antes de começar

- Você deve ter configurado a autenticação remota e verificado se ela foi bem-sucedida.
- Você deve ter criado pelo menos um Usuário remoto ou um Grupo remoto com a função Administrador do aplicativo.
- O provedor de identidade (IDP) deve ser suportado pelo Unified Manager e deve ser configurado.
- Você deve ter o URL e os metadados do IDP.
- Você deve ter acesso ao servidor IDP.

Sobre esta tarefa

Depois de ativar a autenticação SAML do Unified Manager, os usuários não poderão acessar a interface gráfica do usuário até que o IDP tenha sido configurado com as informações do host do servidor Unified Manager. Portanto, você deve estar preparado para concluir ambas as partes da conexão antes de iniciar o processo de configuração. O IDP pode ser configurado antes ou depois da configuração do Unified Manager.

Somente usuários remotos terão acesso à interface gráfica do usuário do Unified Manager após a autenticação SAML ser ativada. Os utilizadores locais e os utilizadores de manutenção não poderão aceder à IU. Essa configuração não afeta os usuários que acessam o console de manutenção, os comandos do Unified Manager ou ZAPIs.

O Unified Manager é reiniciado automaticamente após concluir a configuração SAML nesta página.

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação SAML**.
2. Marque a caixa de seleção **Enable SAML Authentication** (Ativar autenticação SAML*).

   São apresentados os campos necessários para configurar a ligação IDP.

3. Insira o URI de IDP e os metadados de IDP necessários para conetar o servidor do Unified Manager ao servidor de IDP.

   Se o servidor IDP estiver acessível diretamente a partir do servidor do Unified Manager, você poderá clicar no botão **obter metadados IDP** depois de inserir o URI IDP para preencher o campo metadados IDP automaticamente.

4. Copie o URI de metadados do host do Unified Manager ou salve os metadados do host em um arquivo de texto XML.

   Neste momento, você pode configurar o servidor IDP com essas informações.

5. Clique em **Salvar**.

   Uma caixa de mensagem é exibida para confirmar que você deseja concluir a configuração e reiniciar o Unified Manager.

6. Clique em **Confirm and Logout** (confirmar e terminar sessão) e o Unified Manager é reiniciado.

Resultados

Da próxima vez que os usuários remotos autorizados tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do IDP em vez da página de login do Unified Manager.

Depois de terminar

Se ainda não estiver concluído, acesse seu IDP e insira o URI e os metadados do servidor do Unified Manager para concluir a configuração.

Ao usar o ADFS como provedor de identidade, a GUI do Unified Manager não honra o tempo limite do ADFS e continuará funcionando até que o tempo limite da sessão do Unified Manager seja atingido. Quando o Unified Manager é implantado no Windows, Red Hat ou CentOS, é possível alterar o tempo limite da sessão da GUI usando o seguinte comando da CLI do Unified Manager: `um option set absolute.session.timeout=00:15:00`Este comando define o tempo limite da sessão da GUI do Unified Manager para 15 minutos.

Informações sobre direitos autorais

Informações sobre marcas comerciais