Configurar o portal do convidado do 2.1 ISE com PingFederate SAML SSO

Índice

Introdução

Este documento descreve como configurar a versão 2.1 do Cisco Identity Services Engine (ISE) a fim fornecer únicas capacidades de On(SSO) do sinal para usuários portais do convidado com o linguagem de marcação da afirmação da Segurança (SAML).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Serviços do convidado do Cisco Identity Services Engine.
- Conhecimento básico sobre SAML SSO.

Componentes Utilizados

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

- Versão 2.1 do Cisco Identity Services Engine
- Server de PingFederate 8.1.3.0 da identidade do sibilo como a identidade Provider(IdP) de SAML

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 sua rede está viva, certifique-se de que você compreende o impacto potencial de toda a configuração aplicada.

Vista geral do fluxo

SAML é um padrão com base em XML para trocar dados da authentication e autorização entre domínios de segurança.

A especificação de SAML define três papéis: o diretor (usuário convidado), o [IdP] do fornecedor da identidade (server confederado de IPing), e o [SP] do provedor de serviços (ISE).

Em um fluxo típico de SAML SSO, o SP pede e obtém uma afirmação da identidade do IdP. Baseado neste resultado, o ISE pode executar decisões de política enquanto o IdP pode incluir atributos configuráveis que o ISE pode se usar (isto é grupo e endereço email associados ao objeto AD).

Fluxo previsto para este caso do uso

1. O controlador do Wireless LAN (WLC) ou o switch de acesso são configurados para um fluxo central típico da autenticação da Web (CWA).

   Dica: Encontre os exemplos de configuração para fluxos CWA na seção Informação Relacionada na parte inferior do artigo.

2. O cliente conecta e a sessão obtém autenticada contra o ISE. O acesso de rede Device(NAD) aplica os pares do valor de atributos da reorientação (AVP) retornados pelo ISE (o URL-reorientar-ACL e URL-reorienta).

3. O cliente abre o navegador, gerencie o tráfego HTTP ou HTTPS, e obtém-no reorientado ao portal do convidado do ISE.

4. Uma vez no portal o cliente poderá incorporar credenciais previamente atribuídas do convidado (**patrocinador criado**) e auto-disposição uma conta nova do convidado ou usar suas credenciais AD para entrar (**início de uma sessão do empregado**) que fornecerão o único sinal em capacidades com SAML.

5. Uma vez que o usuário seleciona a opção do “do início de uma sessão empregado”, o ISE verifica se há uma afirmação ativa associada à sessão de navegador deste cliente contra o IdP. Se não há nenhuma sessão ativa, o IdP reforçará o login de usuário. Nesta etapa o usuário será alertado incorporar diretamente credenciais AD ao portal de IdP.

6. O IdP autentica o usuário através do LDAP e cria uma afirmação nova que fique viva por um tempo configurável.

   Nota: O sibilo confederado aplica à revelia um **timeout de sessão de** 60 minutos (este significa que se não há nenhuma solicitação de login SSO do ISE em 60 minutos após a autenticação inicial a sessão está suprimida) e um **intervalo máximo da sessão de** 480 minutos (mesmo se o IdP recebeu solicitações de login constantes SSO do ISE para este usuário que a sessão expirará em 8 horas).

Enquanto a sessão da afirmação é ainda ativa, o empregado experimentará o SSO quando usa o portal do convidado. Uma vez o tempo de sessão para fora, uma autenticação de novo usuário será reforçada pelo IdP.

Configurar

Esta seção discute as etapas de configuração para integrar o ISE com o sibilo confederado e como permitir o navegador SSO para o portal do convidado.

> Nota: Embora as várias opções e possibilidades existam quando você autentica usuários convidado, não todas as combinações estão descritas neste documento. Contudo, este exemplo fornece-o a informação necessária compreender como alterar o exemplo à configuração que precisa você quer conseguir.

Etapa 1. Prepare o ISE para usar um fornecedor externo da identidade de SAML

1. Em Cisco ISE, escolha a **administração > o Gerenciamento de identidades > fontes externos da identidade > identificação de SAML fornecedores**.
2. Clique em Add.
3. Sob a aba de **Genaral**, dê entrada com um **nome do fornecedor identificação**. Clique em Salvar. O resto da configuração nesta seção depende dos metadata que precisa de ser importada do IdP em umas etapas mais atrasadas.

Etapa 2. Configurar o portal do convidado para usar um fornecedor externo da identidade

1. Escolha **centros de trabalho > acesso do convidado > configuram > portais do convidado.**
2. Crie um portal novo e escolha o **portal Auto-registrado do convidado**.

> Nota: Este não será o portal principal esse a experiência do usuário mas um subportal que interaja com o IdP a fim verificar o estado da sessão. Este portal é chamado SSOSubPortal.

3. Expanda **ajustes portais** e escolha **PingFederate** para o **método de autenticação**.

4. **Da sequência da fonte da identidade,** escolha o defined(PingFederate) externo de SAML IdP previamente.

5. Expanda as seções das **composição da bandeira de Acceptable Use Policy(AUP)** e de Cargo-**início de uma sessão** e desabilite ambos.

O fluxo portal é:

6. Salve as alterações.

7. Vá para trás aos portais do convidado e crie um novo usando a opção Auto-**registrada do portal do convidado.**

Nota: Este será o visível portal preliminar ao cliente. O portal preliminar usará o SSOSubportal como uma relação entre o ISE e o IdP. Este portal é chamado PrimaryPortal.

8. Expanda as **composição do início de uma sessão** e escolha o **SSOSubPortal** criado previamente sob "**permitem que o seguinte portal do convidado do identidade-fornecedor seja usado para o início de uma sessão**".

9. Expanda as **composição da bandeira AUP e de Cargo-início de uma sessão da política de uso aceitável** e desmarcar-las.

Neste momento o fluxo portal deve olhar como este:

10. Escolha a **personalização portal > as páginas > o início de uma sessão**. Você deve agora ter a opção para personalizar as **opções alternativas do início de uma sessão** (ícone, texto, e assim por diante).

Nota: Observe isso no lado direito, sob a estreia portal, a opção adicional do início de uma sessão é visível.

11. Clique em Salvar.

Agora ambos os portais aparecem sob a lista do portal do convidado.

Etapa 3. Configurar PingFederate para atuar como um fornecedor da identidade para o portal do convidado ISE

1. No ISE, escolha a **administração > o Gerenciamento de identidades > fontes externos da identidade > identificação de SAML fornecedores > PingFederate** e clique a **informação do provedor de serviços.**
2. Sob a **informação do provedor de serviços da exportação,** clique a **exportação.**

3. Salvar e extraia o arquivo zip gerado. O arquivo XML contido aqui é usado para criar o perfil em PingFederate em umas etapas mais atrasadas.

Nota: A partir daqui, este capas de documento a configuração de PingFederate. Esta configuração é mesma para soluções múltiplas como o portal do patrocinador, o MyDevices, e os portais BYOD. (Aquelas soluções não são cobertas neste artigo).

4. Abra o portal de PingFederate admin (tipicamente https://ip:9999/pingfederate/app).

5. Sob o **guia de configuração de IdP > conexões que SP a** seção escolhe **crie novo**.

6. Sob o **tipo de conexão,** clique **em seguida.**

7. Sob **opções de conexão,** clique **em seguida.**

8. Sob **Metadata da importação**, clique o botão de rádio do **arquivo**, o clique **escolheu o arquivo** e escolhe o arquivo XML exportado previamente do ISE.

o sumário dos Metadata 9.Under, clica **em seguida**.

10.On a página da informação geral, sob o nome de conexão, dão entrada com um nome (tal como ISEGuestWebAuth) e clicam-no **em seguida**.

11. Sob o **navegador SSO, o** clique **configura o navegador SSO** e sob a verificação dos **perfis de SAML as** opções e clica-o **em seguida**.

clique da **vida da afirmação** 12.On **em seguida.**

o clique da **criação da afirmação** 13.On **configura a criação da afirmação.**

o mapeamento da identidade 14.Under escolhe o **padrão** e clica-o **em seguida.**

15. No contrato do atributo > estenda o contrato incorporam o **correio dos** atributos e o **memberOf** e o clique **adicionam**. Clique em Next.

A configuração desta opção permite que o fornecedor da identidade passe os atributos de **MemberOf** e de **email** fornecidos pelo diretório ativo ao ISE, que o ISE pode usar mais tarde como uma circunstância durante a decisão de política.

exemplo novo do adaptador do mapa do clique do **mapeamento da fonte da autenticação** 16.Under.

o exemplo do adaptador 17.On escolhe o **adaptador do formulário HTML**. Clique **em seguida**

18. Sob **métodos do mapeamento** escolha a segunda opção para baixo e clique-a **em seguida.**

19. Em fontes do atributo & em clique da **consulta do usuário adicionar a caixa da fonte do atributo.**

20. Sob a **loja dos dados** incorpore uma descrição, e escolha o exemplo da conexão ldap da **loja ativa dos dados** e defina que tipo de serviço de diretório este é. Se não há nenhuma **loja dos dados** configurada contudo o clique **controla lojas dos dados** a fim adicionar o novo cita como exemplo.

21. Sob a **busca do diretório LDAP** defina a **base DN** para a consulta do usuário LDAP no domínio e clique-a **em seguida**.

> Nota: Isto é importante porque definirá a base DN durante a consulta do usuário LDAP. Uma base incorretamente definida DN conduzirá ao objeto não encontrado no esquema LDAP.

o filtro 22.Under **LDAP** adiciona a corda **sAMAccountName=$ {username}** e clica-a **em seguida**.

23. Sob a **realização do contrato do atributo** escolha as opções dadas e clique-as **em seguida**.

24. Verifique a configuração na seção sumária e clique-a **feito**.

25. Suporte clique na **consulta das fontes & do usuário do atributo em seguida**.

26. Sob a **fonte à prova de falhas do atributo** clique **em seguida**.

27. Sob a **realização do contrato do atributo** escolha estas opções e clique-as **em seguida.**

28. Verifique a seção e o clique da configuração em resumo **feitos**.

29. Suporte no clique do **mapeamento da fonte da autenticação em seguida**.

30. Uma vez que a configuração foi verificada sob o clique da **página de sumário feito**.

31. Suporte no clique da **criação da afirmação em seguida**.

32. Sob **configurações de protocolo**, o clique **configura configurações de protocolo**. Neste momento deve haver duas entradas já povoadas. Clique em Next.

33. Sob SLO preste serviços de manutenção ao clique URL **em seguida.**

34. Em emperramentos permissíveis de SAML, desmarcar as opções PRODUTO MANUFATURADO e SABÃO e clique-as **em seguida.**

35. Sob a política da assinatura clique **em seguida**.

36. Sob a política de criptografia clique **em seguida**.

37. Reveja a configuração na página de sumário e clique-a **feito**.

38. Suporte no navegador SSO > clique das configurações de protocolo **em seguida**, valide a configuração, e clique-a **feito**.

39. A aba do navegador SSO aparece. Clique em Next.

40. Sob o clique das **credenciais configurar credenciais** e escolha o certificado de assinatura a ser usado durante IdP a uma comunicação ISE e verifique a opção **incluem o certificado na assinatura**. Em seguida, clique em Avançar.

> Nota: Se não há nenhum clique configurado Certificados **controle Certificados** e siga as alertas a fim gerar um **certificado auto-assinado** a ser usado para assinar IdP às comunicações ISE.

41. Valide a configuração sob a página de sumário e clique-a **feito**.

42. Suporte no clique da aba das **credenciais em seguida**.

43. Sob a **ativação & o sumário** escolha o **ACTIVE do status de conexão**, valide o resto da configuração, e clique-o **feito**.

Etapa 4. Importe Metadata de IdP no perfil externo do fornecedor ISE SAML IdP

1. Sob o console de gerenciamento de PingFederate, escolha a **configuração do servidor > as funções administrativas > a exportação dos Metadata.** Se o server esteve configurado para papéis múltiplos (IdP e SP), escolha a opção que **eu sou a identidade Provider(IdP).** Clique em Next.
2. Sob o modo dos **Metadata** seleto **"selecione a informação para incluir manualmente nos Metadata".** Clique em Next.

3. Sob o **protocolo** clique **em seguida**.

4. **No contrato do atributo** clique **em seguida**.

5. Sob a **chave de assinatura** escolha o certificado configurado previamente no perfil de conexão. Clique em Next.

6. Sob a **assinatura dos Metadata** escolha o certificado de assinatura e a verificação **inclui a chave pública deste certificado no elemento de informação chave.** Clique em Next.

7. Sob o clique do **certificado da criptografia XML em seguida**.

Nota: A opção para reforçar a criptografia aqui é até a rede Admin.

8. Sob a **exportação do** clique da **seção sumária**. Salvar os Metadata arquivam gerado e clicam então **feito**.

9. Sob o ISE, escolha à **administração > ao Gerenciamento de identidades > fontes externos da identidade > identificação de SAML fornecedores > PingFederate**.

10. **A configuração do fornecedor da identidade do** clique **> consulta** e continua importar os metadata salvar da operação da exportação dos Metadata de PingFederate.

11. Escolha a aba dos **grupos**, sob o **atributo da membrasia do clube** adicionar o **memberOf** e clique-o então **adicionam**

Sob o nome na **afirmação** adicionar o nome destacado que o **IdP** deve retornar quando o atributo do **memberOf** é autenticação recuperada do formulário LADP. O grupo configurado é ligado neste caso ao grupo do patrocinador de TOR e o DN para este grupo é como segue:

Uma vez que você adiciona o DN e o “nome **APROVAÇÃO do** clique da descrição ISE”.

12. Escolha a aba dos **atributos** e o clique **adiciona**.

Nesta etapa, adicionar o atributo “correio” que está contido no token de SAML passado do IdP que baseou na pergunta do sibilo sobre o LDAP, ele deve conter o atributo do email para esse objeto.

Nota: Etapas 11 e 12 asseguram-se de que o ISE receba o email do objeto AD e atributos de MemberOf com o IdP entre a ação.

Verificar

1. Lance o portal do convidado usando o teste portal URL ou seguindo o CWA flua. O usuário terá as opções para incorporar credenciais do convidado, cria sua própria conta, e início de uma sessão do empregado.

2. **Início de uma sessão do empregado do** clique. Desde que não há nenhuma sessão ativa o usuário será reorientado ao portal do início de uma sessão de IdP.

3. Incorpore credenciais AD e clique o **sinal sobre**.

4. A tela de logon de IdP reorientará o usuário à página portal do sucesso do convidado.

5. Neste momento, cada vez que o usuário vem para trás ao portal do convidado e escolhe do “o **início de uma sessão empregado**” estarão permitidos na rede enquanto a sessão é ainda ativa no IdP.

Troubleshooting

Toda a edição da autenticação de SAML será registrada sob ise-psc.log. Há um componente dedicado (SAML) sob a **administração > registrando > debuga a configuração do log > seleciona o nó na pergunta >** ajustou SAML componente ao **nível de debug**.

Você pode alcançar o ISE com o CLI e entrar na **cauda de ise-psc.log do aplicativo do** comando show logging e monitorar os eventos de SAML, ou você pode transferir ise-psc.log para a análise mais aprofundada sob **operações > pesquisa defeitos > logs da transferência > seleciona o nó ISE > debuga a aba dos logs > o clique ise-psc.log** para transferir os logs.

```
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAMLUtils::isOracle() - checking whether IDP URL
indicates that its OAM. IDP URL: https://14.36.147.1:9031/idp/sso.saml2
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SPProviderId for PingFederate is: http://CiscoISE
/5b4c0780-2da2-11e6-a5e2-005056a15f11
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- ResponseValidationContext:
        IdP URI: PingFederate
        SP URI: http://CiscoISE/5b4c0780-2da2-11e6-a5e2-005056a15f11
        Assertion Consumer URL: https://14.36.157.210:8443/portal/SSOLoginResponse.action
        Request Id: _5b4c0780-2da2-11e6-a5e2-005056a15f11_DELIMITERportalId_EQUALS5b4c0780-2da2-
11e6-a5e2-005056a15f11_SEMIportalSessionId_EQUALS309f733a-99d0-4c83-8
b99-2ef6b76c1d4b_SEMI_DELIMITER14.36.157.210
        Client Address: 14.0.25.62
        Load Balancer: null
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.BaseSignatureValidator -:::::- Determine the signing certificate
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.BaseSignatureValidator -:::::- Validate signature to SAML standard
with cert:CN=14.36.147.1, OU=TAC, O=Cisco, L=RTP, C=US serial:1465409531352
2016-06-27 16:15:39,367 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
org.opensaml.xml.signature.SignatureValidator -:::::- Creating XMLSignature object
2016-06-27 16:15:39,367 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
org.opensaml.xml.signature.SignatureValidator -:::::- Validating signature with signature
algorithm URI: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.SAMLSignatureValidator -:::::- Assertion signature validated
succesfully
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::::- Validating response
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::::- Validating assertion
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::::- Assertion issuer succesfully validated
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::::- Subject succesfully validated
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::::- Conditions succesfully validated
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
```

```
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAML Response: validation succeeded for guest
IDPResponse
:
        IdP ID: PingFederate
        Subject: guest
        SAML Status Code:urn:oasis:names:tc:SAML:2.0:status:Success
        SAML Success:true
        SAML Status Message:null
        SAML email:guest@rtpaaa.net
        SAML Exception:null
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- AuthenticatePortalUser - about to call
authenticateSAMLUser messageCode:null subject:guest
2016-06-27 16:15:39,375 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- Authenticate SAML User - result:PASSED
```

Informações Relacionadas

- Autenticação da Web central com Cisco WLC e exemplo de configuração ISE.
- Autenticação da Web central com um exemplo de configuração do interruptor e do Identity Services Engine.
- Release Note para o Cisco Identity Services Engine, 2.1 da liberação
- Guia do administrador do Cisco Identity Services Engine, 2.1 da liberação