Instalar arquivo de metadados no ADFS

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Configurar Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento descreve como instalar o arquivo de metadados no Microsoft Ative Diretory Federation Services (ADFS).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ADFS
- Integração do Security Assertion Markup Language (SAML) com o Security Management Appliance

Componentes Utilizados

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

- SMA 11.x.x
- SMA 12.x.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Antes de instalar o arquivo de metadados no ADFS, certifique-se de que estes requisitos sejam atendidos:

SAML habilitado no SMA

- Verifique se o provedor de identidade usado pela sua organização é compatível com o Cisco Content Security Management Appliance. Estes são os provedores de identidade suportados: Serviços de Federação do Microsoft Ative Diretory (ADFS) 2.0Ping Identity Ping Federate 7.2Cisco Web Security Appliance 9.1
- Obtenha os certificados necessários para proteger a comunicação entre seu dispositivo e o
 provedor de identidade:Se quiser que o aplicativo assine solicitações de autenticação SAML
 ou se quiser que o provedor de identidade criptografe asserções SAML, obtenha um
 certificado autoassinado ou um certificado de uma autoridade de certificação (CA) confiável e
 a chave privada associada.Se desejar que o provedor de identidade assine asserções SAML,
 obtenha o certificado do provedor de identidade. Seu aplicativo usa esse certificado para
 verificar as asserções SAML assinadas

Configurar

Etapa 1. Navegue até o SMA e selecione Administração do sistema > SAML > Fazer download de metadados, como mostrado na imagem.

Management Applianc	e Email Web				
Centralized Services	Network	System Administration			
SAML					
Service Provider					
Add Service Provider					
SP Profile Name	Entity ID	Assertion	n Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com	https://sm	a.mexesa.com:83/	Download Metadata	Ŵ
Add Identity Provider No Identity Provider Profile Copyright © 2008-2019 Cise	s have been defined. :o Systems, Inc. All rights	reserved. Privacy Sta	 bening MyLab_SAML_metadata.xr fou have chosen to open: MyLab_SAML_metadata.xm which is: XML file from: https://10.31.124.137 What should Firefox do with this Open with Notepad++ : a Save File Do this <u>a</u>utomatically for file 	file? file? free (GNU) source code editor (s like this from now on.	d V Cancel

Etapa 2. O perfil do provedor de identidade é preenchido automaticamente quando o cliente carrega seu arquivo de metadados ADFS. A Microsoft tem um URL padrão: https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml.

Etapa 3. Quando ambos os perfis estiverem configurados, os metadados do perfil SP devem ser editados, conforme o bug <u>CSCvh30183.</u>. O arquivo de metadados é exibido como mostrado na imagem.

1	xml version="1.0"?
2	<entitydescriptor <="" th="" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"></entitydescriptor>
3	<pre>xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"</pre>
4	<pre>xmlns:ds="http://www.w3.org/2000/09/xmldsig#"</pre>
5	entityID="sma.mexesa.com">
6	<spssodescriptor< th=""></spssodescriptor<>
7	AuthnRequestsSigned="false" WantAssertionsSigned="true"
8	protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
9	<pre><keydescriptor use="signing"></keydescriptor></pre>
10	<pre>ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"></pre>
11	<pre>ds:X509Data></pre>
12	<pre>ds:X509Certificate>Bag Attributes</pre>
13	localKeyID: D5 4F B4 DA BC 91 71 5C 53 94 4A 78 E0 4A C3 EF C4 BD 4C 8D
14	friendlyName: sma.mexesa.com
15	<pre>subject=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security</pre>
16	issuer=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security
17	BEGIN CERTIFICATE
18	MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
19	BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW
20	MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
21	SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjEwNTUxWjByMQsw
22	CQYDVQQGEwJNWDEXMBUGA1UEAwwOc21hLm11eGVzYS5jb20xDTALBgNVBAcMBENE
23	TVgxFjAUBgNVBAoMDVRpem9uY210byBJbmMxDTALBgNVBAgMBENETVgxFDASBgNV
24	BASMC01UIFN1Y3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
25	g7kzRmL114q9T1k1cTJzo8cmscu5nRXFW1ohFPcJgn/oHXEUKvUnWe+9cTJQ41X4
26	ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyv8Wtd+Io
21	MVOWJ9h9Kju/kSXuYHUIBYOXfPOLyzHHCbAVYKuPM4F1/y4jwj6rnO4jtvpZPj7B
28	cpwjawLixAIUHVyVrc661TD100exG+nZ+AIS3B01+61mTNjF3IcGcGS/TE0chETx
29	giscukulmiphPEtAZey/ebyh18EpH/WV1NwZkMUjINVmIFq3+LkF8As8B1Pm6YH1
30	Lokow4v0EjInjtmnC/EQIQIDAQABMAUGCSqGSID3DQEECWUAA4IBAQBy3vXNL/jD
31	emuthSkr4nyc01db9z2xGQCSe2EeynnkgH0z/r/TEV0NkOKOtF11200JbyGE0dWD
32	6+BVJ6WSBD/00LYBdCXgLy1+VK41/K2+1CVL3DYAXKDI0QSJVIDZOG/XSJKXZM/9
33	7Euptorm7purmp1/0oTKruykbyu220 TMUPurkbori2UthKKSFVqpKet/UTACH/
25	/Eubrogr/pvirbs/goincvikbau2sounvrxxacjAvj/2cianrBgSMxeo2//ECJq
35	DOIDC5M2WWF
30	END CERTIFICATE
38	
30	
22	N/ WO INVOLUTION

Etapa 4. Remova as informações realçadas, no final, o arquivo Metadados deve estar conforme mostrado na imagem.

1	<pre><?xml version="1.0"?></pre>	
2	<pre><entitydescriptor <="" th="" xmlns="urn:oasis:names:tc:SAML:2.</pre></th><th>0:metadata"></entitydescriptor></pre>	
3	<pre>xmlns:saml="urn:oasis:names:tc:SAML:2.0:asser</pre>	tion"
4	<pre>xmlns:ds="http://www.w3.org/2000/09/xmldsig#"</pre>	
5	<pre>entityID="sma.mexesa.com"></pre>	
6	<spssodescriptor< th=""><th></th></spssodescriptor<>	
7	AuthnRequestsSigned="false" WantAssertionsSi	gned="true"
8	<pre>protocolSupportEnumeration="urn:oasis:names:t</pre>	c:SAML:2.0:protocol">
9	<pre></pre>	
10	<pre>ds:KeyInfo xmlns:ds="http://www.w3.org/2000/</pre>	09/xmldsig#">
11	白 <ds:x509data></ds:x509data>	
12	<pre>ds:X509Certificate></pre>	
13	MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwU	AMHIxCzAJBgNV
14	BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1U	EBwwEQORNWDEW
15	MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDE	UMBIGA1UECwwL
16	SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjE	wNTUxWjByMQsw
17	CQYDVQQGEwJNWDEXMBUGA1UEAwwOc21hLm11eGVzYS5jb20xDTA	LBGNVBACMBENE
18	TVgxFjAUBgNVBAoMDVRpem9uY210byBJbmMxDTALBgNVBAgMBEN	ETVgxFDASBgNV
19	BAsMC01UIFN1Y3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8	AMIIBCgKCAQEA
20	g7kzRmL114q9T1k1cTJzo8cmscu5nRXFWlohFPcJgn/oHXEUKvU	nWe+9cTJQ41X4
21	ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsT	BGFNyv8Wtd+Io
22	MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6	rnO4jtvpZPj7B
23	cpWjawLlxAfUHVyvrc661Tblo0exG+hZ+AlS3B01+61mTNjF3Ic	GcGS/TE0chETx
24	glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+Lk	F8As8B1Pm6YHi
25	L6K8W4v0Ej1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4I	BAQBy3vxNL7jb
26	emMTKSRP4hycU1d69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFi	i2oOJ6yGEOdWD
27	6+Bvj6wSBp7UoLyBdCxglyi+vK4Y/R2+iCv13pyaXkbf0QSJvYp	zOg7xSjkxZm79
28	+ZIjQkekyCAM5N00f1ZRrJ9oGD5qoY1ZjhuD7NHmRBj7LKHRKsF	VqpKet/tTXCH7
29	7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/Zc1XnPB	GSMxeo277ECJq
30	ix5aXRSxOMRRtD/72FVRAsgT3x1mBYqu/HTyOBZonGM+isJHBhR	ZxSOMBL+45jFY
31	PO1jBG5MZuWE	
32	<pre>- </pre>	
33	-	
34	<pre>- </pre>	
35		
36	<pre></pre>	
37	<pre>ds:KeyInfo xmlns:ds="http://www.w3.org/2000/</pre>	09/xmldsig#">
38	<pre>ds:X509Data></pre>	
39	<pre>ds:X509Certificate></pre>	
40	MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwU	AMHIXCZAJBGNV
41	BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1U	EBwwEQORNWDEW
42	MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDE	UMBIGA1UECWWL
43	SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjE	wNTUxWjByMQsw

Etapa 5. Navegue até seu ADFS e importe o arquivo de metadados editados nas **Ferramentas ADFS > Gerenciamento do AD FS > Adicionar Confiança de terceira parte confiável**, como mostrado na imagem.

N	Add Relying Party Trust Wizard
Select Data Source	
 Steps Welcome Select Data Source Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish 	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network: Use this option to import the necessary data and certificates from a relying party organization that publishes is federation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app (*) Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: <u>Extends in metadata file location</u> (*) Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.
	< Previous Next > Cancel

Etapa 6. Depois de importar com êxito o arquivo de metadados, configure as regras de reivindicação para a confiança de terceira parte confiável recém-criada, selecione **Claim rule template > Send LDAP Attributes**, como mostrado na imagem.

9 1	Add Transform Claim Rule Wizard			
Select Rule Template				
Steps	Select the template for the claim rule that you want to create from the following list. The description provides			
Choose Rule Type	detais about each claim rue template.			
Configure Claim Rule	Claim rule template:			
	Send LDAP Attributes as Claims V			
	Claim rule template description:			
	Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.			

Passo 7. Nomeie o nome da regra de Reivindicação e selecione **Repositório de atributos > Ative Diretory**.

Etapa 8. Mapear atributos LDAP, como mostrado na imagem.

Atributo LDAP > Endereços de e-mail

• 1	Tipo de	solicitação	de saída	> Endered	o de e-mail
-----	---------	-------------	----------	-----------	-------------

\$ 0	Add Transform Claim Rule Wizard						
Configure Rule							
Steps Choose Rule Type Configure Claim Bule	You o which issued	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.					
Configure claim note	Claim	Claim rule name:					
	chare	la_sma					
	Rule t	emplate: Send LDAP Attributes as Claims &e store:	•				
	Activ	Active Directory V					
	Mapping of LDAP attributes to outgoing claim types:						
		LDAP Attribute (Select or type to add more)		Outgoing Claim Type (Select or type to add more)		
	•	E-Mail-Addresses	۷	E-Mail Address	~		
	*		~		~		
				< Previous Finish Cu	ancel		

Etapa 9. Crie uma nova regra de Reivindicação personalizada com essas informações, como mostrado na imagem.

Esta é a regra personalizada que precisa ser adicionada à regra de Reivindicação personalizada:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier
"] = "https://<smahostname>:83");
```

Edit Rule - charella_custom_rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

charella_custom_rule

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
    => issue(Type =
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
    Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,
    ValueType = c.ValueType, Properties
    ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format
"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
    Properties
    ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spname
    qualifier"] = "https://dh106-euql.r1.ces.cisco.com/");
```

 Modifique a URL realçada com o nome de host e a porta SMA (se você estiver em um ambiente CES, uma porta não será necessária, mas deve apontar para euq1.<alocação>.iphmx.com)

OK

Cancel

Etapa 10. Certifique-se de que o pedido da regra de Reivindicação seja: A regra de afirmação LDAP primeiro e a regra de solicitação personalizada em segundo lugar, como mostrado na imagem.

	Ec	dit Claim Rules for A	DFS_charella		-		
uance Tra	Insform Rules	Issuance Authorization Ru	es Delegation A	uthoriza	ation R	ules	
The follow	ing transform ru	les specify the claims that v	ill be sent to the re	elying p	arty.		
Order	ng transform ru Rule Name	les specify the claims that v	Issued Claims	elying p	arty.	1	
Order 1	ing transform ru Rule Name charella_sma	les specify the claims that v	Issued Claims E-Mail Address	elying p	earty.		
Order 1	Rule Name charella_sma	les specify the claims that v	Issued Claims E-Mail Address	elying p	enty.		

Etapa 11. Faça login no EUQ e redirecione para o host ADFS.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- CSCvh30183
- Suporte Técnico e Documentação Cisco Systems