Installieren der Metadatendatei auf dem ADFS

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

Dieses Dokument beschreibt, wie die Metadatendatei auf Microsoft Active Directory Federation Services (ADFS) installiert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ADFS
- Integration von Security Assertion Markup Language (SAML) in Security Management Appliance

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Bevor die Metadatendatei im ADFS installiert wird, stellen Sie sicher, dass diese Anforderungen erfüllt sind:

- SAML aktiviert in SMA
- Überprüfen Sie, ob der von Ihrem Unternehmen verwendete Identitätsanbieter von der Cisco Content Security Management Appliance unterstützt wird. Dies sind die unterstützten Identitätsanbieter: Microsoft Active Directory Federation Services (ADFS) 2.0Ping Identity Ping Federate 7.2Cisco Web Security Appliance 9.1
- Rufen Sie die folgenden Zertifikate ab, die zum Sichern der Kommunikation zwischen Ihrer Appliance und dem Identitätsanbieter erforderlich sind:Wenn die Appliance SAML-Authentifizierungsanforderungen signieren soll oder wenn der Identitätsanbieter SAML-Assertionen verschlüsseln soll, erhalten Sie ein selbstsigniertes Zertifikat oder ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) und dem zugehörigen privaten Schlüssel.Wenn der Identitätsanbieter SAML-Assertionen signieren soll, rufen Sie das Zertifikat des Identitätsanbieters ab. Die Appliance überprüft mithilfe dieses Zertifikats die signierten SAML-Assertionen.

Konfigurieren

Schritt 1: Navigieren Sie zu Ihrem SMA, und wählen Sie **Systemverwaltung > SAML > Metadaten** herunterladen aus, wie im Bild gezeigt.

Management Applianc	e Email Web				
Centralized Services	Network	System Administration			
SAML					
Service Provider					
Add Service Provider					
SP Profile Name	Entity ID	Asserti	on Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com	https://sr	na.mexesa.com:83/	Download Metadata	Ŵ
Identity Provider Add Identity Provider Profiles have been defined. No Identity Provider Profiles have been defined. Copyright © 2008-2019 Cisco Systems, Inc. All rights reserved. Privacy States S		reserved. Privacy Sta	Opening MyLab_SAML_metadata.xml × You have chosen to open: ✓ ✓ MyLab_SAML_metadata.xml ✓ which is: XML file ✓ from: https://10.31.124.137 ✓ Sta What should Firefox do with this file? ✓ Open with Notepad++ : a free (GNU) source code editor (d ✓ Sta Open with Notepad++ : a free (GNU) source code editor (d ✓ Sta Do this automatically for files like this from now on. OK Cancel		

Schritt 2: Das Identitätsanbieter-Profil wird automatisch ausgefüllt, wenn der Kunde seine ADFS-Metadatendatei hochlädt. Microsoft hat eine Standard-URL: https://<ADFShost>/FederationMetadata/2007-06/FederationMetadata.xml.

Schritt 3: Nach dem Einrichten beider Profile muss die SP Profile Metadata entsprechend dem Fehler <u>CSCvh30183</u> bearbeitet werden. Metadatendatei sieht wie im Bild gezeigt aus.

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

Schritt 4: Entfernen Sie die hervorgehobenen Informationen, am Ende muss die Metadatendatei wie im Bild gezeigt sein.

1	<pre><?xml version="1.0"?></pre>
2	<entitydescriptor <="" td="" 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	<pre>entityID="sma.mexesa.com"></pre>
6	<spssodescriptor< th=""></spssodescriptor<>
7	AuthnRequestsSigned="false" WantAssertionsSigned="true"
8	protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
9	<pre></pre>
10	<pre>ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"></pre>
11	白 <ds:x509data></ds:x509data>
12	<pre>ds:X509Certificate></pre>
13	MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
14	BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW
15	MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
16	SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjEwNTUxWjByMQsw
17	CQYDVQQGEwJNWDEXMBUGA1UEAwwOc21hLm11eGVzYS5jb20xDTALBgNVBAcMBENE
18	TVgxFjAUBgNVBAoMDVRpem9uY210byBJbmMxDTALBgNVBAgMBENETVgxFDASBgNV
19	BAsMC01UIFN1Y3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
20	g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUKvUnWe+9cTJQ41X4
21	ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyv8Wtd+Io
22	MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rnO4jtvpZPj7B
23	cpWjawLlxAfUHVyvrc661Tblo0exG+hZ+AlS3B01+61mTNjF3IcGcGS/TE0chETx
24	glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
25	L6K8W4vOEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBy3vxNL7jb
26	emMTKSRP4hycU1d69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
27	6+Bvj6wSBp7UoLyBdCxglyi+vK4Y/R2+iCv13pyaXkbf0QSJvYpzOg7xSjkxZm79
28	+ZIjQkekyCAM5N00f1ZRrJ9oGD5qoY1ZjhuD7NHmRBj7LKHRKsFVqpKet/tTXCH7
29	7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/Zc1XnPBGSMxeo277ECJq
30	ix5aXRSxOMRRtD/72FVRAsgT3x1mBYqu/HTyOBZonGM+isJHBhRZxSOMBL+45jFY
31	PO1jBG5MZuWE
32	<pre>- </pre>
33	-
34	<pre>- </pre>
35	<pre>- </pre>
36	<pre></pre>
37	<pre>ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"></pre>
38	白 <ds:x509data></ds:x509data>
39	<pre>ds:X509Certificate></pre>
40	MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
41	BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW
42	MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
43	SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjEwNTUxWjByMQsw

Schritt 5: Navigieren Sie zu Ihrem ADFS, und importieren Sie die bearbeitete Metadatendatei in ADFS Tools > AD FS Management > Add Relying Party Trust, wie im Bild gezeigt.

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. Bet 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 optioned to import the necessary data and certificates from a relying party organization that has optioned to import the necessary data and certificates from a relying party organization that has optioned to import the necessary data and certificates from a relying party organization that has optioned to import the necessary data and certificates from a relying party organization that has optioned to import the necessary data and certificates from a relying party organization that has opticate in metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Extended to import the necessary data and certificates from a relying party organization that has opticate in metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Extended to import the necessary data about this relying party organization. Browse.
	< Previous Next > Cancel

Schritt 6: Nachdem Sie die Metadatendatei erfolgreich importiert haben, konfigurieren Sie die Anspruchsregeln für die neu erstellte Vertrauenswürdigkeit der Partei. Wählen Sie **Anspruchsregelvorlage > LDAP-Attribute senden aus**, wie im Bild gezeigt.

9 1	Add Transform Claim Rule Wizard	x		
Select Rule Template				
Steps Choose Rule Type	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.	ı		
 Configure Claim Rule 	Caim rule template: Send LDAP Attributes as Claims Caim 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.			

Schritt 7: Nennen Sie den Namen der Anspruchsregel, und wählen Sie Attributspeicher > Active Directory aus.

Schritt 8: Zuordnen von LDAP-Attributen, wie im Bild gezeigt.

LDAP-Attribut > E-Mail-Adressen

Ausgehender An	spruchst	yp > E-Mail-Adress	e			
S		Add Transform	Claim Rule \	Wizard		×
Configure Rule						
Steps	You o	an configure this rule to send	the values of LD	AP attributes as claims	s. Select an attribut	e store from
Choose Rule Type	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 Rule	Claim rule name:					
	charela_sma					
	Rule t Attribu	emplate: Send LDAP Attribute te store:	es as Claims			
	Active	Directory		~		
	Марр	ing of LDAP attributes to outg	oing claim types:			
		LDAP Attribute (Select or add more)	type to	Outgoing Claim Type (Select or type to ad	id more)
	•	E-Mail-Addresses	×	E-Mail Address		¥
	*		×			Ý
				< Previous	Finish	Cancel

Schritt 9: Erstellen Sie eine neue benutzerdefinierte Anspruchsregel mit diesen Informationen, wie im Bild gezeigt.

Dies ist die benutzerdefinierte Regel, die der benutzerdefinierten Anspruchsregel hinzugefügt werden muss:

```
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.rl.ces.cisco.com/");
```

 Ändern Sie die hervorgehobene URL mit dem SMA-Hostnamen und -Port (wenn Sie sich in einer CES-Umgebung befinden, ist kein Port erforderlich, aber er muss auf euq1 verweisen.<allocation>.iphmx.com.

OK

Cancel

Schritt 10: Stellen Sie sicher, dass die Reihenfolge der Anspruchsregel folgendermaßen lautet: Die LDAP-Anspruchsregel wird zuerst und die benutzerdefinierte Anspruchsregel die zweite ausgeführt, wie im Bild gezeigt.

\$ 1	E	dit Claim Rules for ADI	FS_charella –	• X
Issuance	Transform Rules	Issuance Authorization Rules	Delegation Authorization Ru	ules
The fol	owing transform n	les specify the claims that will b	e sent to the relying party.	
Order	Rule Name	h	equad Claime	
1	charella_sma	E	E-Mail Address	
2	charella_custor	n_rule <	See claim rule>	

Schritt 11: Melden Sie sich beim EUQ an, muss dieser zum ADFS-Host umgeleitet werden.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- CSCvh30183
- <u>Technischer Support und Dokumentation Cisco Systems</u>