# ةصاخلا ةيضارتفالا ةكبشلا) VPN نيوكت ةددعتم ةقداصملا عم ASA AnyConnect نم اللخ نم Microsoft Azure نم لماوعلا (نامألا ديكأت زيمرت

تايوتحملا <u>ةمدق ملا</u> <u>قيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>قىساسأ تامولعم</u> SAML تانوكم <u>ريفشتا او عيقوتا ا تايا معل تاداهش</u> <u>ةكېش لل ىطىطختال مس رال</u> <u>نىوكتلا</u> Microsoft تاقى بطت ضرعم نم Cisco AnyConnect قفاض <u>قيبطتلل Azure AD مدختسم نييعت</u> CLI ربع SAML ل ASA نىوكت <u>قحصلا نم ققحتلا</u> SAML ةقداصم مادختساب AnyConnect رابتخا <u>ةعئاش لا تالكش ملا</u> قباطتم ريغ نايكلا فرعم <u>تقولا قباطت مدع</u> <u>قحيحص ريغ IDp عيقوت ةداهش مادختسا مت</u> <u>جلاص ريغ ديكأتانا روممج</u> <u>كلەتسمارا قمدخ دېكأتال ئطاخ URL ناونع</u> <u>ذي فنت از يج لخدت ال يت SAML ني وكت تاري يغت</u> <u>اهحالصاو ءاطخألا فاشكتسا</u> <u>ةلص تاذ تامولعم</u>

### ةمدقملا

ىلع زيكرتلاا عم (SAML) نامألا ديكأت زييمت ةغل نيوكت ةيفيك دنتسملا اذه حضوي ASA ىلع زيكرتلا عم (AML) مال اذه حضوي AnyConnect لاللخ نم Microsoft Azure MFA.

ةىساسألا تابلطتملا

تابلطتملا

:ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- ميكترل لباقلا نامألا زاهج يلع RA VPN نيوكتب ةيساسأ ةفرعم (ASA).
- . Microsoft Azure و SAML ب ةيْساساً ةفرغم •
- اطقف VPN وأ AnyConnect (APEX صيخارت نيكمت مت ).

### ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- Microsoft Azure AD. كارتشا
- + Cisco ASA 9.7 و + AnyConnect 4.6
- AnyConnect VPN فيرعت فلم لمع •

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

# ةيساسأ تامولعم

تالاجم نيب ضيوفتلاو ةقداصملا تانايب لدابتل XML ىلإ دنتسي لمع راطإ وه SAML ةيوهلا دوزمو (SP) ةمدخلا دوزمو مدختسملا نيب ةقثلا نم ةرئاد ءاشنإ ىلع لمعي وهف .نامألا (IDp) جمد متي .تامدخ ةدعل ةدحاو ةرم لوخدلا ليجستب مدختسملل حمسي امم (IDp) Microsoft Azure جمد متي .تامدخ تواف الما يفاض لوخدلا ليجستب مدختسمل حمسي امم (VPN ASA حمسي الم وVPN قكبش لوخد ليجستل يفاض يفاض نامأ ريفوتل VPN ما يم يفال السب Cisco AnyConnect.

### SAML تانوكم

نيب ةنمآ ةلماعم نمضي يذلا وه XML ىلإ دنتسملا دنتسملا دنتسملا : تايقافتالا ىلع ضوافتلاب يجيتارتسالا قفرملاو فرعملل حمسي وهو .SP فرعمو P فرعم.

(IdP، SP) ةزەجألا ةطساوب ةموعدملا راودألا

لقح تحت .Dp و SP نم لكل ميق ىلع يوتحي دقو دحاو رود نم رثكأ زاهجلا معدي نأ نكمي لوخد ليجست فرعم صخت ةدراولا تامولعملا تناك اذإ ،IDPSSODescriptor نوكي IDPSSODescriptor نوكي EntityDescriptor اذهو .دحاو لوخد ليجستل SPSSODescriptor من تامولعملا تناك اذإ SPSSODescriptor ددحم وأ يداحأ .حاجنب SAML دادعإل ةبسانملا ماسقألاا نم ةحيحصلا ميقلا ذخأ بجي هنأل مهم

ةدع ىلع دحاولا زامجلا يوتحي نأ نكمي .IDp وأ SP ل ديرف فرعم وه لقحلا اذه :نايكلا فرعم ،لاثملا ليبس ىلع .اهنيب قيرفتلل ةفلتخم تانايك تافرعم مادختسإ هنكميو تامدخ اهتقداصم مزلي يتلا ةفلتخملا قفنلا تاعومجمل ةفلتخم نايك تافرعم ىلع ASA يوتحي نايك فرعم تالاذإ ىلع قفن ةعومجم لك ةقداصمب موقي يذلا ةيوهلا فرعم يوتحت منايك فرعم لكل قلصفن

اذإ .اەنيب زييمتلل فرعم لكل لصفنم نايك فرعم ەلو ةددعتم تافرعم ASA معدي نأ نكمي نمف ،اقبسم ەنيوكت مت نايك فرعم ىلع يوتحي ال زامج نم ةلاسر نيبناجلا نم يأ ىقلت فرعم ىلع روثعلا نكمي .SAML ةقداصم لشفتو ،ةلاسرلا ەذە زاەجلا طقسي نأ لمتحملا لقح لخاد نايكلا EntityDescriptor بناجب وأ SP ةطساوب اەريفوت متي يتلا SAML ةمدخل URL نيوانع ەذە فرعت :ةمدخلل URL نيوانع ةمدخو يداحألا جورخلا ليجست ةمدخ يە ةمدخلا ەذە نوكت ،(IdPs) ةمدخلا فرعمل ةبسنلاب . يە ةمدخلا ەذە نوكت ام ةداع ،ةيعامتجالا تامدخلا يدوزمل ةبسنلاب .يداحألا لوخدلا ليجست يداحألا جورخلا ليجست ةمدخو ةدكؤملا ءالمعل قمدخ.

تانايب يف هيلع روثعلا مت يذلا يداحألا لوخدلا ليجست ةمدخل URL ناونع SP مدختسي لكشب ةميقلا هذه نيوكت ةلاح يف .ةقداصملل IdP ىلإ مدختسملا هيجوت ةداعإل IdP فيرعت هتجلاعم هيلع رذعتي وأ SP ةطساوب لسرملا ةقداصملا بلط IdP ىقلاتي ال ،حيحص ريغ حاجنب.

تانايب يف ەيلع روثعلا مت يذلا ةيوەلا ديكأتل ءالمعلا ةمدخل URL ناونع مادختسإ متي لوح تامولعم ريفوتو SP ىلإ ىرخأ ةرم مدختسملا ەيجوت ةداعإل IDp ةطساوب SP فيرعت ديكأتلا SP ىقلتي ال ،حيحص ريغ لكشب اذه نيوكت ةلاح يف .مدختسملا ةقداصم ةلواحم .حاجنب ەتجلاعم رذعتي وأ (ةباجتسالا)

متيو .IDp و SP نم لك ىلع يداحألاا جورخلا ليجست ةمدخل URL ناونع ىلع روثعلاا نكمي امدنع .ASA ىلع يرايتخإ وهو SP نم SSO تامدخ عيمج نم جورخلا ليجست ليهستل همادختسإ مدختسملا موقي امدنع ،SP ىلع IdP فيرعت تانايب نم SLO ةمدخل URL ناونع نيوكت متي ليجستب IdP موقي نأ درجمب .IdP ىل SP لسري ،SP ىلع ةمدخلا نم جورخلا ليجستب مدختسيو SP ىلإ ىرخأ قرم مدختسمل اهيجوت ديعي هنإف ،حاجنب تامدخلا نم مدختسمل اونع ناونع URL نونع تال يورخ

لقنل SAML المردختسي يتلاا ةقيرطلا يه طباورلا :ةمدخلاب ةصاخلا URL نيوانعل SAML طباور HTTP و HTTP ميجوت ةداعإ كلذ نمضتيو .تامدخلل سكعلاب سكعلاو IdP ىل تامولعملا ةقيرط نيمضت متي .تانايبلا لقنل ةفلتخم ةقيرط ةقيرط ةقيرط لكلو .Artifact و POST تلاثملا ليبس ىلع .تامدخلا هذه فيرعت نمض ةمدخلا اهمعدت يتلا طبرلا SingleSignOnService Binding="urn:oasis:names:tc:saml:2.0:bindings:http-redirect" location <u>قمردخ</u> = HTTP ميجوت ةداعإ ققيرط امئاد ASA مدختسي .ASA معدي ال .< <u>SSO</u> تابلطل HTTP ميجوت ةداعإ ققيرط امئاد ASA مدختسي .ASA معدي ال .< <u>SSO</u> قداعإل HTTP ميجوت قداع قاري الكان الكان الكان .

ريفشتلاو عيقوتلا تايلمعل تاداهش

ىلع ةردقلا SAML نمضتي ،IDp و SP نيب ةلسرملا لئاسرلل ةەازنلاو ةيرسلا ريفوتل وأ/و تانايبلا ريفشتل ةمدختسملا ةداەشلا نيمضت نكمي .اەعيقوتو تانايبلا ريفشت ةلاسر نم ققحتلا ملتسي يذلا فرطلل نكمي ثيحب فيرعتلا تانايب نمض اەعيقوت مدختسملا تاداەشلا ىلع روثعلا نكمي .عقوتملا ردصملا نم يتأت اەنأ نم دكأتلاو SAML قمدختسملا تاداەشل يلع روثعلا نكمي .عقوتملا ردصملا مى يتأت اەنأ نم دكأتلاو KeyDescriptor use=signature لئاسر ريفشت ASA معدي ال .SogCertificate مث ،مارتحإ لكب ،Salu

ةكبشلل يطيطختلا مسرلا



نيوكتلا

#### Microsoft تاقيبطت ضرعم نم Cisco AnyConnect ةفاضإ

متخاو Azure لخدم ىلإ لوخدلا لجس .1 ةوطخلا Azure لخدم ىل



.تاسسؤملا تاقيبطت رتخأ ،ةروصلا هذه يف حضوم وه امك .2 ةوطخلا



ةروصلا هذه يف حضوم وه امك ،ديدج قيبطت رتخأ ،نآلاا .3 ةوطخلا.

Enterprise applications rchoga-azure-ad - Azure Active Directory	All applications		
	← New application == Colum	ns	
Overview	Try out the new Enterprise Apps se	earch preview! Click to enable the preview	v. $ ightarrow$
Overview     Diagnose and solve problems	Application Type	Applications status	Application visibility
Prograde and solve problems	Enterprise Applications	Any 🗸	Any 🗸

Cisco رتخاو ،ثحبلاً عبرم يف AnyConnect بتكا ،ضرعملاً نم ةفاضإلاً مسق يف .4 ةوطخلاً مث ،جئاتنلاً قحول نم AnyConnect



ةروصلا هذه يف حضوم وه امك ،يداحألا لوخدلا ليجست ةمئاق رصنع رتخأ .5 ةوطخلا.

AnyConnectVPN   Overvie	w		
*			
u Overview	Properties		
Deployment Plan	Name		
X Diagnose and solve problems	AnyConnectVPN		
Manage	Application ID ①		
Properties			
A Owners	Object ID 💿		
Users and groups			
Single sign-on	Getting Started		
Provisioning			
Application proxy	1. Assign users and groups	2. Set up single sign on	3. Provision User Accounts
Self-service	Provide specific users and groups access	Enable users to sign into their application	Automatically create and delete user
Security	Assign users and groups	Get started	Get started
Conditional Access			
Permissions			
Token encryption	4. Conditional Access	S. Self service	
Activity	Secure access to this application with a customizable access policy.	Enable users to request access to the application using their Azure AD	
Sign-ins	Create a policy	Get started	
🖬 Usage & insights (Preview)			

#### .ةروصلا يف حضوم وه امك ،SAML رتخأ .6 ةوطخلا

Cisco AnyConnect   Single     Enterprise Application	e sign-on		
<ul> <li>Werview</li> <li>Deployment Plan</li> <li>Diagnose and solve problems</li> </ul>	Select a single sign-on method	SAML Rich and secure authentication to applications using the SAMI (Security	Linked Link to an application in the Azure Active Directory Acress Panel and/or
III Properties		Assertion Markup Language) protocol.	Office 365 application launcher.
A Owners			
Users and groups			
Single sign-on			

ليصافتلا هذهب 1 مسقلا ريرحتب مق .7 ةوطخلا.

#### <#root>

```
a. Identifier (Entity ID) - https://<VPN URL>/saml/sp/metadata/<TUNNEL-GROUP NAME>
```

b. Reply URL (Assertion Consumer Service URL) - https://<VPN URL>/+CSCOE+/sam1/sp/acs?tgname=<TUNNEL-G

```
Example: vpn url called
```

#### asa.example.com

and tunnel-group called

AnyConnectVPN-1

Basic SAML Configuration		
Identifier (Entity ID)	Required	
Reply URL (Assertion Consumer Service URL)	Required	
Sign on URL	Optional	
Relay State	Optional	
Logout Url	Optional	

ىلع ەظفحو ،صيخرتلا فلم ليزنتل ليزنت رتخأ ،SAML عيقوت ةداەش مسق يف .8 ةوطخلا كبساح.

SAML Signing Certificate		Ø
Status	Active	
Thumbprint		
Expiration	5/1/2023, 4:04:04 PM	
Notification Email		
App Federation Metadata Url	https://l	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XMI	Download	

.ASA نيوكتل بولطم اذه .9 ةوطخلا

- Azure AD Identifier انب صاخلا VPN نيوكت يف SAML idp وه اذه.
- لوخد ليجست وه اذه لوخدلا ليجستل URL ناونع
- جورخ ليجست وه اذه جورخلا ليجستل URL ناونع

You'll need to configure the appli	cation to link with Azure AD.	
Login URL	https://	
Azure AD Identifier	https://	
Logout URL	https://	

#### قيبطتلل Azure AD مدختسم نييعت

كنأل ارظن ،Azure ل يداحألا لوخدلا ليجست مادختسال Test1 نيكمت متي ،مسقلا اذه يف قيبطت ىلإ لوصولا حنمت Cisco AnyConnect. ةفاضإ مث ،تاعومجملاو نومدختسملا رتخأ ،قيبطتلا ىلع ةماع ةرظن ةحفص يف .1 ةوطخلا مدختسم.

Cisco AnyConnect   User	rs and groups		
«	+ Add user 🖉 Edit 🗊 Remove 🖓	Update Credentials   🗮 Columns   🛇 Got feedback?	
Overview	The application will appear on the Access P	anel for assigned users. Set 'visible to users?' to no in properties to prevent this	<b>→</b>
Deployment Plan			
X Diagnose and solve problems	First 100 shown, to search all users & group	s, enter a display name.	
	Display Name	Object Type	Role assigned
Manage			
Manage	No application assignments found		
Manage III Properties & Owners	No application assignments found		
Manage III Properties Conners Users and groups	No application assignments found		

#### ةمەم ةفاضإ ةشاش يف تاعومجمو نيمدختسم رتخأ .2 ةوطخلا.

Add Assignment chogi-anire-ad		,⊅ βearch
Users and groups None Selected	>	
Select Role User	>	
		TE Test1

#### .نييعت رز رقنا ،ةمەم ةفاضإ ةشاش يف .3 ةوطخلا

elect Role	
lser	2

CLI ربع SAML ل ASA نيوكت

.كب ةصاخلا SAML ةداهش داريتساو TrustPoint ءاشنإب مق 1. ةوطخلا

config t

```
crypto ca trustpoint AzureAD-AC-SAML revocation-check none
```

```
no id-usage
enrollment terminal
no ca-check
crypto ca authenticate AzureAD-AC-SAML
-----BEGIN CERTIFICATE-----
...
PEM Certificate Text you downloaded goes here
...
-----END CERTIFICATE-----
quit
```

.كب صاخلا SAML فرعم رماوألا هذه رفوت .2 ةوطخلا

webvpn

```
saml idp https://xxx.windows.net/xxxxxxxxx/ - [Azure AD Identifier]
url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
url sign-out https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0 - Logout URL
trustpoint idp AzureAD-AC-SAML - [IdP Trustpoint]
trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
no force re-authentication
no signature
base-url https://asa.example.com
```

.VPN قفن نيوكت ىلع SAML ةقداصم قيبطت .3 ةوطخلا

```
tunnel-group AnyConnectVPN-1 webvpn-attributes
  saml identity-provider https://xxx.windows.net/xxxxxxxxxx/
  authentication saml
end
```

write memory

رفوم نيوكت ةلازا ىلا ةجاحب تنأف ،ldP نيوكت ىلع تارييغت ءارجاب تمق اذا :ةظحالم 🔌 .ةلاعف تارييغتلا حبصت يكل ەقيبطت ةداعاو ،قفنلا ةعومجم نم saml ةيوە

### ةحصلا نم ققحتلا

SAML ةقداصم مادختساب AnyConnect رابتخإ

ليصافت لخدأو (VPN) ةيرهاظلا ةصاخلا ةكبشلاب صاخلا URL ناونعب لصتا 1. ةوطخلا Azure AD. لوخدلا ليجست بلط ىلع ةقفاوملا. 2 ةوطخلا.

AnyConnect. ليصوت متي .3 ةوطخلا

• • •	Lisco AnyLonnect Login			
	Microsoft Sign in Enail address, phone number or Skype Cart access your account? Sign-in options			
		Terms of use	Privacy & cookies	



IPv4

ةعئاشلا تالكشملا

00:00:22

قباطتم ريغ نايكلا فرعم

:ءاطخألا حيحصت لاثم

[SAML] consumption\_confirmation: رفوم ليجستل لفورعم ريغ رفومل فرعم #LassoServer. رفوم ليجستل #LassoServer، وأ وأ ((asso\_server\_add\_provider) بيل اسأل امادختس إبجي (asso\_server\_add\_provider) الع يف lasso\_server\_add\_provider\_from\_buffer

رمألاا نأ ينعت ،ماع لكشب :ةلكشملا saml idp [entityID] ب صاخلا WebVPN نيوكت نمض ASA ب صاخلا فيرعت تانايب يف هيلع روثعلا مت يذلا IdP نايك فرعم عم قباطتي ال IdP.

رمألا رييغتب مقو IdP فيرعت تانايب فلمب صاخلا نايكلا فرعم نم ققحت :لحلا saml idp رمألا رييغتب مقو IdP فيرعت تانايب فلمب صاخلا. [entity id] رمألا اذه ةقباطمل.

تقولا قباطت مدع

:ءاطخألا حيحصت لاثم

[SAML] لبق تسيل:2017-09-05T23:59:01.896z NotOnOrAfter:2017-09-06T00:59:01.896Z قارەملا 0

حلاص ريغ وأ ةيحالصلا يەتنم ديكأتلا :SAML] Consumption\_Confirmation]

IdP. تقو عم ASA تقو ةنمازم متت مل .1 ةلكشملا

.ldP لبق نم مدختسماا هسفن NTP مداخ مادختساب ASA نيوكتب مق .1 لحلا

ددحملا تقولا نيب حلاص ريغ ديكأتلا. 2 ةلكشملا.

ASA. ىلع اەنيوكت مت يتلا ةلەملا ةميق ليدعتب مق .2 لحلا

### ةحيحص ريغ IDp عيقوت ةداەش مادختسإ مت

:ءاطخألا حيحصت لاثم

[Lasso] func=xmlSecOpenSSLEvpSignatureVerify:file=signatures.c:line=493:obj=rsasha1:subj=EVP\_VerifyFinal:error=18:data قباطتت ال

اىلع عيقوت نم ققحتلا فيرعتلا فلمل نكمي ال :SAML] Consumption\_Confirmation] ةلاسرلا

البق نم قق حتايا ASA ل عيقوت دجوي ال وأ IdP لبق نم ةعقومال الله المرال ان مق ق حتايا ASA يلع رذعت :ةلكشم ق حتال .

ەلاسرا متي امل اەتقباطم نم دكأتلل ASA ىلع ةتبثملا IdP عيقوت ةداەش نم ققحت :لحلا قطساوب SAML. قباجتسإ يف عيقوتلا نيمضت نم دكأتف ،كلذ ديكأت مت اذإ IdP قطساوب :ءاطخألا حيحصت لاثم

حلاص ريغ روهمجلا ديكأت :SAML] Consumption\_Confirmation]

.حيحصلا ريغ روەمجلا IdP فرعي :ةلكشملا

ASA. نايك فرعم قباطت نأ بجي .IDp ىلع روەمجلا نيوكت حيحصت :لحلا

#### كلەتسملا ةمدخ ديكأتل ئطاخ URL ناونع

يلوألاا ةقداصملا بلط لاسرا دعب ءاطخأ حيحصت يأ يقلت رذعتي :ءاطخألاا حيحصت لاثم. علام ميجوتلا ديعي ال IdP نكلو IdP يف دامتعالاا تانايب لاخدا مدختسملل نكمي ASA.

Confirmation Consumer Service. ل حيحص ريغ URL ناونعل IdP نيوكت مت :ةلكشملا

تانايب نم ققحت .هتحص نم دكأتو نيوكتلا يف يساسألا URL نم ققحت :(لولحلا) لحلا حفصت ،وه رابتخال .ديكأتلل كلهتسملا ةمدخ URL ةحص نم دكأتلل راهظإ عم ASA فيرعت .حيحص الك نوكي نإ ،وه

#### ذيفنتلا زيح لخدت ال يتلا SAML نيوكت تارييغت

ال SAML لازي ال ،SP ةداهش ،لوخدلا ليجستل يداحأ URL ناونع رييغت وأ ليدعت دعب :لاثم ةقباسلا تانيوكتلا لسريو لمعي.

رييغت كانه نوكي امدنع هب ةصاخلا فيرعتلا تانايب ءاشنإ ةداعإ ىلإ ASA جاتحي :ةلكشملا ايئاقلت كلذ لعفي ال وهو .هيلع رثؤي نيوكتلا يف.

قفنلا ةعومجم ىلع قبطنملا [entity-id] تلازإ رمأ تحت ،تارييغتلا ءارجإ دعب :لحلا مقيبطت ةداعإو ةرثأتملا.

## اهحالصإو ءاطخألا فاشكتسا

هيلع روثعلاا نكمي حيحص ريغ نيوكت اهحالصإو SAML ءاطخأ فاشكتسأ تاودأ مظعم نمضتت debug webVPN مادختسإ نكمي .ءاطخألا حيحصت ليغشت وأ .SAML نيوكت نم ققحتلا دنع saml 255 ال يتلا تاهويرانيسلا يف ،كلذ عمو ،اهحالصإو لكاشملا مظعم ءاطخأ فاشكتسال 255 حيحصت تاودأ نم ديزم ليغشت نكمي ،ةديفم تامولعم اذه ءاطخألا حيحصت اهيف رفوي :ءاطخألا

debug webvpn saml 255 debug webvpn 255 debug webvpn session 255 debug webvpn request 255

## ةلص تاذ تامولعم

قيبطتارا ليكو مادختساب قول حملا تاقيبطتال SAML وداحاً لوخد ليجست

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما