CXS1774BCN

vmware[®] **EXPLORE**

Active Directory Federation Services Integration & Troubleshooting the Most Recurring Issues

Wael Abdelhady Staff Technical Support Engineer

#vmwareexplore #CXS1774BCN



Required Disclaimer

- This presentation may contain product features or functionality that are currently under development.
- This overview of new technology represents no commitment from VMware to deliver these features in any generally available product.
- Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.
- Technical feasibility and market demand will affect final delivery.
- Pricing and packaging for any new features/functionality/technology discussed or presented, have not been determined.

Presenter



Wael Abdelhady

Staff Technical Support Engineer



Agenda What is AD FS?

VMware vCenter® integration details and workflow

Setup Demo

Troubleshooting

What is AD FS?

© 2023 VMware, Inc.

What is Active Directory Federations Services (AD FS)?



AD FS Concepts

Elements in authentication flow



- Federation is a concept where users from "company A" can authenticate to an application on "company B"
- But using their "company A" credentials.

It uses one of three federation protocols to do this:

- SAML 2.0
- WS-Federation
- OpenID Connect



ACTIVE DIRECTORY:

The Identity Information which is to be used by AD FS is stored on the Active Directory.





FEDERATION SERVER:

It contains the tools needed to manage federated trusts between business partners.



FEDERATION SERVER PROXY:

The Federation server is not exposed directly to the internet to prevent security risks.





AD FS WEB SERVER

It hosts the AD FS Web Agent.

AD FS Benefits

Integrating vCenter with ADFS can provide organizations with several benefits, including:



Improved security because VMware vCenter[®] never handles the user's credentials.



Single Sign-On with existing federated infrastructure and applications.



Support for multifactor authentication.



How Does AD FS Work?

The authentication process using the Active Directory Federation Service (AD FS)

- 1. The user navigates to a service, for example, a partner-company website (<u>http://example.com</u>)
- 2. The website requests an authentication token.
- 3. User requests token from the AD FS server.
- 4. AD FS server issues token containing user's set of claims.
- 5. User forwards token to the partner-company website.
- 6. The website grants authorization access to the user.



Prerequisites



AD FS for Windows Server 2016 or later must already be deployed



AD FS must be connected to Active Directory



An Application Group for vCenter must be created in AD FS as part of the configuration process.



Configuration KB https://kb.vmware.com/s/article/78029

AD FS requirements

Prerequisites



AD FS server CA (Sub/Root) certificate to be added to the Trusted Root Certificates Store.



Configuring LDAPs need to get the LDAP root certificate, add it to the Trusted Root Certificates within the configuration.



How to get the AD certificate in case you will configure LDAPs.



Run the following command in VC: openssl s_client -connect AD_FQDN:636

Certificates requirement

Prerequisites

vCenter Server and other requirements



VMware vSphere® 7.0 or later.



vCenter server must be able to connect to the AD FS discovery endpoint.



You need Administrator privilege or the "VcIdentityProviders.Manage" privilege.

VMware vCenter Integration Details and Workflow

© 2023 VMware, Inc.

vCenter and AD FS Configuration Process Flow



Required Information

The AD FS administrator must provide the following information to create the vCenter server identity provider configuration:

Steps	News	
• Welcome	Name:	
Server application		
Configure Application Credentials	Client Identifier: 06a2c11e-e76e-4dc2-9ff8-cd42424f5fa3	
Configure Web API	Redirect URI:	
Apply Access Control Policy	Example: https://Contoso.com	Add
 Configure Application Permissions 	http://vcsa	Remove
Summary		
Complete		
	Description:	

Client Identifier

The UUID string is generated by the AD FS Application Group Wizard, and it identifies the Application Group itself.

Required Information

Shared Secret

Add Application Group W Configure Application	izard ×
Steps Velcome Server application Configure Application Credentials Configure Web API Apply Access Control Policy Configure Application Permissions Complete	Select credentials used by the application to authenticate itself with AD FS when requesting access tokens. □ Register a key used to sign JSON Web Tokens for authentication □ Configure □ Windows Integrated Authentication Select the AD Account: Example: CONTOSO\expensevc Select Select Generate a shared secret Secret:

- It is generated by the AD FS Application Group Wizard and is used to authenticate vCenter server with AD FS.
- "Please note that, it appears only on the first-time configuration so note it down!"

Required Information

OpenID Address

onfigure Main Identity rovider	ADFS server	
	Application Group	
1 Identity Provider	Client Identifier	b93298b4-a47a-4528-9594-4e522e739182
2 ADFS server		Unique identifier of the client application.
	Shared secret	
3 Users and Groups		The client secret value; this value identifies the client with the provider.
4 Review	OpenID	
	OpenID Address	https://adfs.gslabs.local/adfs/.well-known/openid-configuration
		eg. https://webserver.example.com/idp/.well-known/openid-config

The OpenID Provider Discovery endpoint URL of the AD FS server, specifying a well-known address is typically the issuer endpoint concatenated with the path "/.well-known/openid-configuration".

For example: https://ADFS-webserver.example.com/AD FS/.well-known/openid-configuration.



Ŧ

≡ vSphere Client Q Search in all environments < Configuration Administration Identity Provider Local Accounts Login Message Access Control V Roles Global Permissions Туре Embedded Licensing V Licenses Identity Sources ADD EDIT SET AS DEFAULT REMOVE Solutions V Active Directory Domain **Client Plugins** Smart Card Authentication Name ¥ Server URL Type T Domain T Alias vCenter Server Extensions 0 --System Domain vsphere.local ----Deployment V 0 ---Local OS (Default) localos System Configuration 2 items Customer Experience Improvement Program Client Configuration Support V Upload File to Service Request Certificates V Certificate Management Single Sign On \sim Users and Groups Configuration



 Need to make sure you have the 3 required claims

The follo	Notes Access control p	policy Issuance Transform Rules Client Permissions
Order	Rule Name	
1	Group Bule	Group
2	Subject Rule	Name ID
3	UPN Rule	UPN

• How to translate the token by using token ID on the website



• What should a good token look like?

💥 រហក Crafted by Auth0 by Okta Debugger Libraries Introduction Ask Encoded PASTE A TOKEN HERE Decoded EDIT THE PAYLOAD AND SECRET HEADER: ALGORITHM & TOKEN TYPE 9KZyIsImtpZCI6I1FWRzN0ZX1hZ1EtMUJWUnB2T 1F6WG1YcE9 Type of token KZyJ9.eyJhdWQi0iJi0TMy0ThiNC1hNDdhLTQ1M "typ": "JWT" "alg": "RS256", jgt0TU5NC00ZTUyMmU3Mzkx0DIiLCJpc3Mi0iJo "x5t": "QVG3teyagQ-1BVRpv0QzXiXp0Jg", "kid": "QVG3teyagQ-1BVRpv0QzXiXp0Jg" dHRwczovL2FkZnMuZ3NsYWJzLmxvY2FsL2FkZnM iLCJpYXQi0jE20TcyNTcxMzEsIm5iZiI6MTY5Nz I1NzEzMSwiZXhwIjoxNjk3MjYwNzMxLCJhdXRoX PAYLOAD: DATA 3RpbWUi0jE20TcyNTcxMzEsInN1YiI6InIrbGFR ZGhFNkRIRy9meDRTdVY1THFRV0FVU1hzel1MZ3Z "aud": "b93298b4-a47a-4528-9594-4e522e739182" GcjJYZWVIbW89 "iss": "https://adfs.gslabs.local/adfs" IiwidW5pcXV1X25hbWUi0iJnc1xcd2FlbCIsInN "iat": 1697257131, "nbf": 1697257131, pZCI6I1MtMS01LTIxLTE10Tk1MjUxNjAtMjM5MT "exp": 1697260731, A2NDc0LTMxMjYwMjczMDYtMzEwNiIsInVwbiI6I "auth_time": 1697257131, "sub": ndhZWxAZ3NsYWJzLmxvY2FsIiwiZ3JvdXAiOlsi r+laQdhE6DHG/fx4SuV5LqQWAUSXszYLqvFr2XeeHmo=", Z3NsYWJzLmxvY2FsXFxEb21haW4gQWRtaW5zIiw "unique_name": "gs\\wael", "sid": "S-1-5-21-1599525160-239106474-3126027306iZ3NsYWJzLmxvY2FsXFxEb21haW4gVXNlcnMiLC Jnc2xhYnMubG9jYWxcXFNjaGVtYSBBZG1pbnMiL upn": "wael@gslabs.local". CJnc2xhYnMubG group": ["gslabs.local\\Domain Admins" 9jYWxcXEVudGVycHJpc2UgQWRtaW5zIiwiZ3NsY "gslabs.local\\Domain Users" WJzLmxvY2FsXFxHcm91cCBQb2xpY3kgQ3J1YXRv "gslabs.local\\Schema Admins" gslabs.local\\Enterprise Admins' ciBPd251cnMiLCJnc2xhYnMubG9jYWxcXEVTWCB "gslabs.local\\Group Policy Creator Owners", BZG1pbnMiXSwiYXBwdH1wZSI6IkNvbmZpZGVudG "gslabs.local\\ESX Admins" lhbCIsImFwcGlkIjoiYjkzMjk4YjQtYTQ3YS00N "apptype": "Confidential", TI4LTk10TQtNGU1MjJ1NzM5MTgyIiwiYXV0aG11 "appid": "b93298b4-a47a-4528-9594-4e522e739182", dGhvZCI6InVybjpvYXNpczpuYW1lczp0YzpTQU1 "authmethod": urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtect MOjIuMDphYzpj edTransport", bGFzc2Vz01Bhc3N3b3JkUHJvdGVjdGVkVHJhbnN "ver": "1.0" wb3J0IiwidmVyIjoiMS4wIiwic2NwIjoib3Blbm "scp": "openid" lkIn0.ML20GmhogeLXNyzUfSy0plACCYvb5GjMt 0....74 £-...0.0...0L.0....00L A1DT11 -0£4-N-W

We need to enable debug logging on

• STS & VMware vSphere[®] ui logs; to show the Token and the related AD FS errors.

UI Logs under: /usr/lib/vmware-vsphere-ui/server/conf/serviceability.xml

STS Logs under: vSphere 7.0: /usr/lib/vmware-sso/vmware-sts/webapps/ROOT/WEB-INF/classes/log4j2.xml vSphere 8.0: /var/lib/sso/webapps/ROOT/WEB-INF/classes/log4j2.xml

<root level="DEBUG">

[400] Unable to authenticate. Check your credentials. If problem persists, contact your administrator.

- Will be time issue related, between VC / AD FS / ESXi
- Need to check the time on the VC & make sure it is the same as the AD FS server

Δ Unable to login because you do not have permission on any vCenter Server systems connected to this client.

- Receives error message do not have permissions, while AD over LDAP permissions are successful.
- You can see in the **vmware-identity-sts**.log:

2023-09-23T18:12:53.880Z INFO sts[81:tomcat-http--42] [Corld=fe92fb2f-e0ac-4873-be1d-c088481a381d] [com.vmware.identity.saml.impl.AuthnOnlyTokenValidator] Token _3e9ede75-fe3a-40ca-8a3f-69e112ad8e24 for principal {Name: wael, Domain: gslabs.local} successfully validated

\Lambda Unable to login because you do not have permission on any vCenter Server systems connected to this client.

- Check the logs to see the token information /var/log/vmware/vsphere-ui/logs/vsphere_client_virgo.log
- Search for "idToken", copy everything after "idToken=" until ", tokenType"

(the part highlighted in yellow)

IToken= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUz11NilsIng1dCl6llFWRzN0ZXlhZ1EtMUJWUnB2T1F6WGIYcE9KZyIsImtpZCl6llFWRzN0ZXlhZ1EtMUJWUnB2T1F6WGIYcE9KZyJ9.eyJhdWQiOil2NzFhMTdlZS1lM2E0LTRiNTgtOGRjYS0xM2RmZGU50DM4NmYiLCJpc MiOiJodHRwczovL2FKZnMuZ3NsYWJzLmxvY2FsL2FkZnMiLCJpYXOiOjE20DkwMzM0NTcsIn5iZil6MTY4OTAzMzQiNywiZXhwIjoxNjg5MDM3MDU3LCJhdXROX3RpbWUiOjE20DkwMzM0NTcsInN1Yil6lkliV2FvbDNIZE5ITml3TFh2REtyTjJMRmQxVWZvMytmR StaDNqYUFac3M9liwidW5pcXVIX25hbWUiOjJnc1xcYWRlc2VyM51zYWhY2NvdW50liwic2lkljoiUy0xLTUtMjEtMTU5OTUyNTE2MC0yMzkxMDY0NzQtMzzUJzNyNj0xMXM00NTCsInN1Yil6lkliV2FvbDNIZE5ITml3TFh2REtyTjJMRmQxVWZvMytmR NhbFxcRG9tYWluIFVzZXJzliwiYXBwdHlwZSI6lkNvbmZpZGVudGihbClsImFwcGikljoiNjcxYTE3ZWUtZTNhNC00YjU4LThkY2EtMTNkZmRIOTgzODZmliwiYXV0aGildGhvZCl6lnVybjpvYXNpczpuYW1lczp0YzpTQU1MOjluMDphYzpjbGFzc2VzOiBhc3N3b3JkUHJ 3GVjGGVkVHJhbnNwb3J0liwidmVyljoIMS4wliwic2Nwijob3BlbmlkIn0.vznt1529c1U11EyJ2G6y57X_D0vkso_pBNesxicDgG0ddvyRDGddBff588YceFs1B64Mmye7TSeLpuEHgi2Fl2PLJnDMwTffzJKhZ2DQwWMf_R0RPCXX5cb2g508BiBePY_VHynFW91h04_kjQ_opRvpQbHKh11DbmnB7Ir4BjTDFuhNV_M15K5N6j6bZ5CN3W8no5yarN1b0o7JrPu9hFPnJ78c14tIYCSLxfd3adF3iQStX8T64m4uaOtLqVee4NFMwESsPeKfF37GPalTeYfv_oCb30THOKPK

AuwyzeKM8-rFZBrkvQuImLxAvXdLD4RvZ0LRdcOECVnw, tokenType=bearer, expiresIn=3600, scope=null, jti=null;

Paste on https://jwt.io/

Bad Token "missing Groups claim"

```
"aud": "671a17ee-e3a4-4b58-8dca-13dfde98386f",
  "iss": "https://adfs.gslabs.local/adfs",
  "iat": 1695492358,
  "nbf": 1695492358.
  "exp": 1695495958,
  "auth_time": 1695492358,
  "sub":
"JN7CMm1Jb4iGov5xZb5b11INFu7ry+MRLfZ1QYsWC4E=",
  "unique_name": "gs\\wael",
  "sid": "S-1-5-21-1599525160-239106474-3126027306-
3106",
  "upn": "wael@gslabs.local",
   apptype": "Confidential",
  "appid": "671a17ee-e3a4-4b58-8dca-13dfde98386f",
  "authmethod":
"urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtect
edTransport",
  "ver": "1.0",
  "scp": "openid"
```

Good Token

```
"aud": "b93298b4-a47a-4528-9594-4e522e739182",
  "iss": "https://adfs.gslabs.local/adfs",
  "iat": 1697257131,
  "nbf": 1697257131.
  "exp": 1697260731,
  "auth_time": 1697257131,
  "sub":
"r+laQdhE6DHG/fx4SuV5LqQWAUSXszYLgvFr2XeeHmo=",
  "unique_name": "gs\\wael",
  "sid": "S-1-5-21-1599525160-239106474-3126027306-
3106",
  "upn": "wael@gslabs.local",
  "group": [
    "gslabs.local\\Domain Admins",
    "gslabs.local\\Domain Users",
    "gslabs.local\\Schema Admins",
    "gslabs.local\\Enterprise Admins",
    "gslabs.local\\Group Policy Creator Owners",
    "gslabs.local\\ESX Admins"
  "apptype": "Confidential",
  "appid": "b93298b4-a47a-4528-9594-4e522e739182",
  "authmethod":
"urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtect
edTransport",
  "ver": "1.0",
  "scp": "openid"
```

▲ Unable to login because you do not have permission on any vCenter Server systems connected to this client.

Cause:

The UPN and sAMAccount Name doesn't match in the AD.

This occurs because the logic in vCenter that searches for AD identities in the "Add Members" UI widget uses the sAM Account Name attribute when it is constructing the membership entry in the VC group. But during login, you get the UPN from the AD FS token and use that for comparison.

omain	gslabs.local	
Jser/Group	Q aduser	
Role	aduser1-samaccount	
	aduser2	

Workaround:

Add the user to an AD group, then add that group to the required role.

Encoded							
evilexuloukvit							
VCDB=# id	select * from vp prin	x_access; cipal	role_id	entity_id	flag	surr_key	
1 23 24 422 423 424 425 426 427 1025 (10 rov	VSPHERE.LOCAL\A VSPHERE.LOCAL\A VSPHERE.LOCAL\A VSPHERE.LOCAL\A VSPHERE.LOCAL\A VSPHERE.LOCAL\A VSPHERE.LOCAL\A VSPHERE.LOCAL\A VSPHERE.LOCAL\A SSLABS.LOCAL\ad	dministrator dministrators CLSAdmin dministrators CLSAdmin dministrators CLSAdmin dministrators CLSAdmin user1-samaccount	-1 -2077191429 -2077191429 -2077191429 -2077191429 -2077191429 -2077191429 -2077191429 -2077191429 -2077191429 -1	1 12 1001 1001 1002 1002 1003 1003 1	1 3 3 3 3 3 3 1	1 2 3 10 11 12 13 14 15 19	

.

1 Unable to login because you do not have permission on any vCenter Server systems connected to this client.

Cause:

This issue can also occur if permissions are given to AD groups in the vCenter and the case of the domain name does not match the case of the configured domain in the Identity Source Base DN.

By design, domain filtering logic for groups in vCenter is case-sensitive.



Solution:

For example, if Active Directory is **gslabs.local**, then the identity source should have **dc=gslabs,dc=local** for the base distinguished name for **users** and **groups**.

Workaround:

Add the user direct permission on the VC, instead of Group

Issue: Login to vCenter server fails with NoPermission error, if the permission was added using a group from AD FS

Cause: Under Configure Application Permissions, "allatclaims" scope was unchecked for the specific vCenter (Server Application).

Solution:

Issue was resolved after checking the allatclaims.

and a second sec	~	Identifiers Notes Access control policy Issuance Transfor	m Rules Client Permission
		Configure application permissions to enable client applications	to acess this Web API
Center AFDES		Client application (caller):	
unities.		Name Description	
scription:		vCenter_AFDFS - Server application	
plications:			
Iamo	Department		
Conversionalization	Description		A LL D
Server application			Add Remov
Center_APDP3 - Server application		Permitted scopes:	
Web API		Scope Name Description	
Center_AFDFS - Web AP1		✓ allatclaims Requests the access token claims in	the identity token.
		aza Scope allows proker client to request	t primary refresh token.
		email Request the email claim for the signe	ed in user.
		logon_cert The logon_cert scope allows an app	lication to request logo
		openid Request use of the OpenID Connect	t authorization protocol.
		✓ openid Request use of the OpenID Connect □ profile Request profile related claims for the	t authorization protocol. signed in user.
		openid Request use of the OpenID Connect profile Request profile related claims for the user_imperso Request permission for the applicatio	t authorization protocol. signed in user. on to access the resour
dd application	Edit Remove	openid Request use of the OpenID Connect profile Request profile related claims for the user_imperso Request permission for the application	t authorization protocol. signed in user. on to access the resour New scop
dd application	Edit Remove	openid Request use of the OpenID Connect profile Request profile related claims for the user_imperso Request permission for the application	t authorization protocol. signed in user. on to access the resour New scop

Issue: Users can't login while using subdomains in the AD FS topology.

Environment: Main domain – vmware.com Sub domain – sub.vmware.com

Workaround:

- Create a group in main domain and add the sub domains users
- Add that group to the vCenter
- By design vCenter doesn't support having multiple domains



Issue: Can't add account or query from the AD FS Domain.

Cause: Password change for the service account, which was used for AD over LDAP/LDAPS broke the AD FS integration.

Configuration	
- Identity Provider Local Accounts Login Message	
Туре	Microsoft ADFS
✓ ADFS server	
Client Identifier	b93298b4-a47a-4528-9594-4e522e739182
OpenID Address	https://adfs.gslabs.local/adfs/.well-known/openid-configuration
✓ Users and Groups	
Base distinguished name for users	CN=Users,DC=GSLABS,DC=local
Base distinguished name for groups	CN=Users,DC=GSLABS,DC=local
Username	Administrator@gslabs.local
Primary server URL	ldaps://gslabs.local
✓ Redirect URIs	
Authentication Redirect URI (vCenter Name)	https://vcsa01.gslabs.local/ui/login/oauth2/authcode
Log-out Redirect URI (vCenter Name)	https://vcsa01.gslabs.local/ui/login

Connecting to AD FS is not supported when the vCenter system has a proxy configuration enabled.

Configure Main Identity Provider	Review		×
1 Identity Provider	Com.vmware.vcenter.tr HTTP response code: t known/openid-configu	rustmanagement.impl.invalidArgumentException: java.io.iOException: Server returned 503 for URL: http://localhost:1080/external-vecs/http1/acc.sts.smals.be/443/adfs/.well- ration	×
2 ADFS server	Identity Provider Type	Microsoft ADFS	
3 Users and Groups	✓ Authentication Info		
A Deview	ldentity Provider Name	Microsoft ADFS	
4 Review	Client Identifier	27cf938a-d953-4a75-a3fc-a989d767551d	
	Shared secret	k6cN ZNKuw aEjBDDZ, 25Tvn Jp_oko1_aPL5Ekr	
	OpenID Address	https://acc./~3,_1_3s2/adfs/.well-known/openid-configuration	
	✓ Users and Groups		
	Base distinguished name for users	OU=users,OU=smals,DC=g ud,DC=dom	
	Base distinguished name for groups	OU=groups,OU=smals,DC=(ud,DC=dom	
	Username	sm/ 1.9g	
	Primary server URL	Idap:/// 1a.services.g d.bc n.be:389	
	Secondary server URL	Idap:///	
		CANCEL BACK FI	NISH

Collecting Logs

Component	Log File(s)*	Potential Issues
H5C Client UI	(In /var/log/vmware/vsphere- ui/logs/): vsphere_client_virgo.log and apigw.log	 Can't connect to ADFS server due to no matching CA in JRE truststore OAuth protocol error, such as incorrect client ID/secret or invalid state parameter LDAP connection failure when searching users and groups in AuthZ config
ADFS Provider	ssoAdminServer.log vmware-identity-sts.log tokenservice.log vmware-identity-sts-default.log	 Can't connect to AD server when searching users and groups in AuthZ config Failure contacting VcIdentityProviders API or VMDIR for AD/ADFS metadata Can't connect to ADFS server for OAuth username/password login via CLI/SDK
Foreign Trust Provider	(Same as ADFS Provider)	Failure contacting Foreign Security Principals API to get JIT data
VcIdentityProviders API	/var/log/vmware/trustmanagement /trustmanagement-svcs.log	 Failure communicating with ADFS discovery endpoint, possibly due to no matching CA in JRE truststore, or ADFS discovery endpoint did not include all expected data Validation failed for input LDAP info: invalid DN formats, invalid or expired certs, etc Failure communicating with local VMDIR LDAP
Foreign Security Principals API	/var/log/vmware/trustmanagement /trustmanagement-svcs.log	Failure communicating with local VMDIR LDAP
Token Exchange Service	tokenservice.log	 Failure contacting VcIdentityProviders API or Foreign Security Principals API Can't contact ADFS discovery endpoint or JWKS URI to get JSON Web Key Set info Failed to verify ADFS JWT token signature with JWKS info Saved issuer data in VcIdentityProviders API does not match issuer in ADFS JWT token Validation failed for ADFS JWT token issue time, expiration time, or "not before" time Field names in ADFS JWT token don't match what's expected (i.e. "groups_claim" and "upn_claim" in the VcIdentityProviders API for example)

vmware[®] **EXPLORE**

Please take your survey.



vmware[®] **EXPLORE**

Thank You

