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?

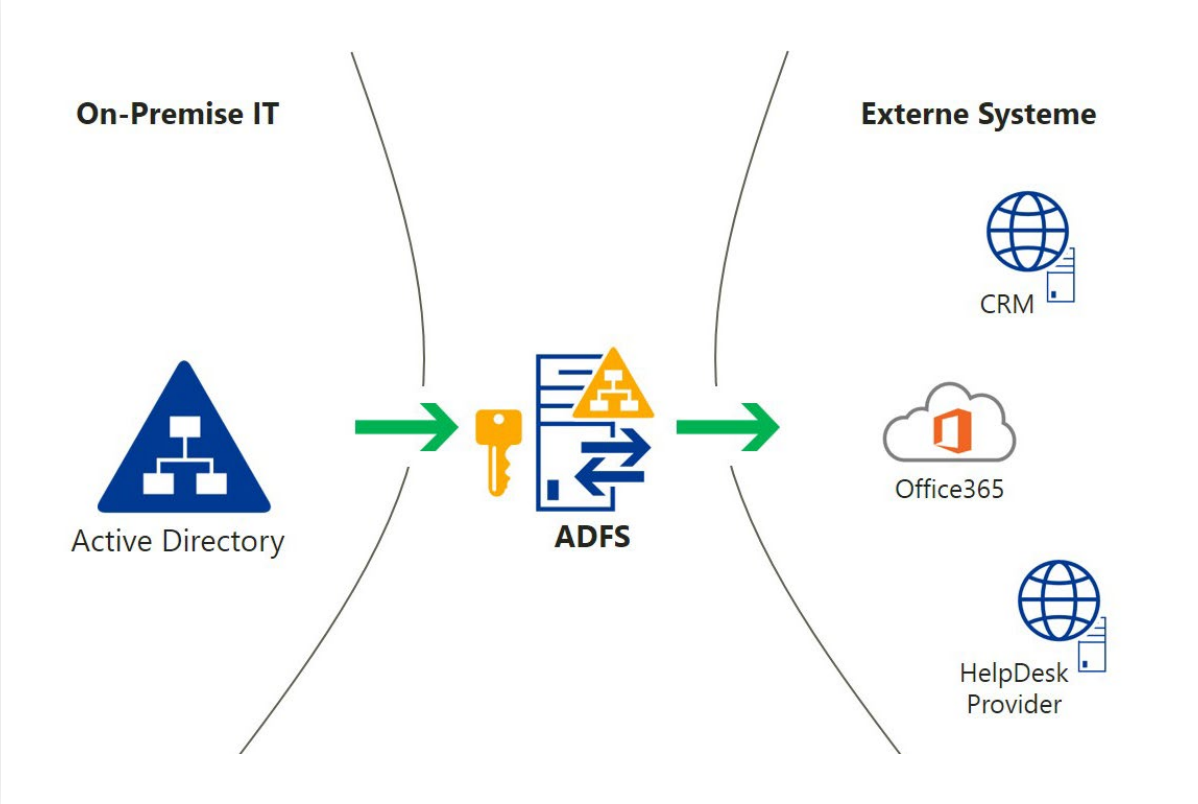
VMware vCenter® integration details and workflow

Setup Demo

Troubleshooting

What is AD FS?

What is Active Directory Federations Services (AD FS)?



- ADFS (Active Directory Federation Services) is a Microsoft service that enables secure authentication across organizational boundaries.
- It allows users to access resources in different domains using a single set of credentials.
- With ADFS, organizations can achieve greater security and flexibility in their authentication process.

AD FS Concepts

Elements in authentication flow

Sign-in Protocol

OpenID Connect/OAuth 2.0

Authentication Protocol

WIA, FBA, Azure MFA,
Device Auth, Certificates

Token Type

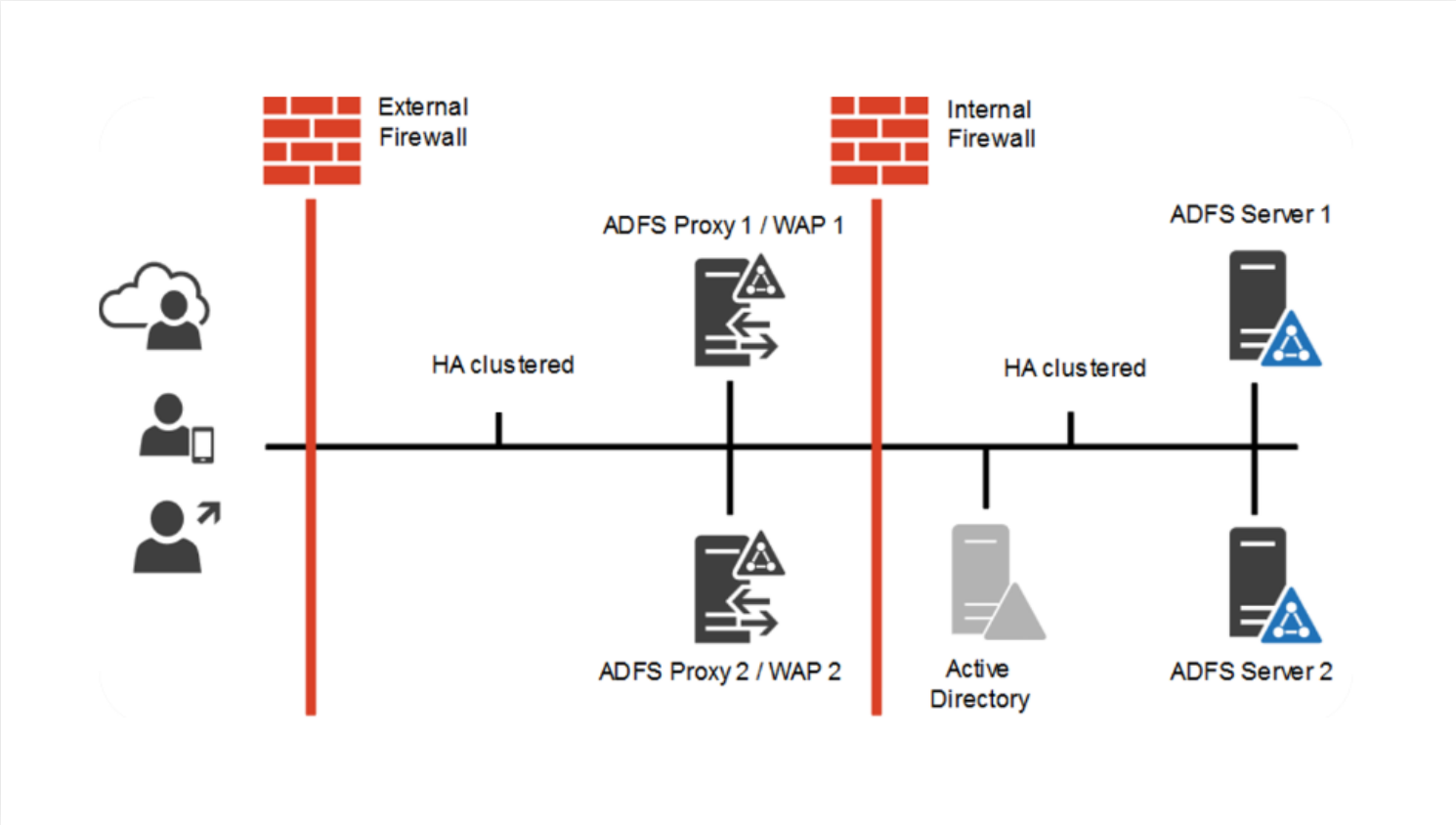
JavaScript Web Token (JWT)

- 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

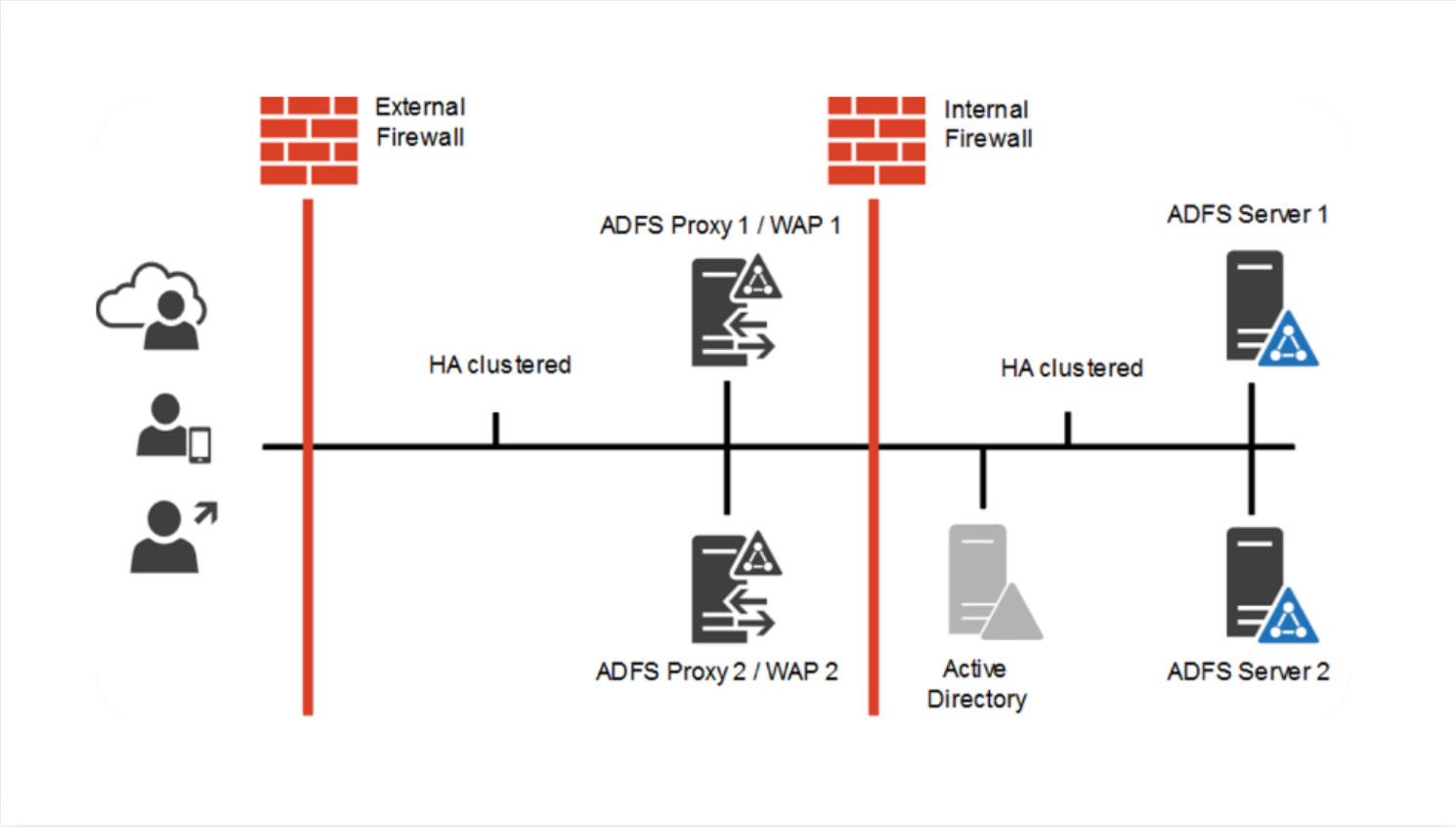
What are the Components of AD FS?



ACTIVE DIRECTORY:

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

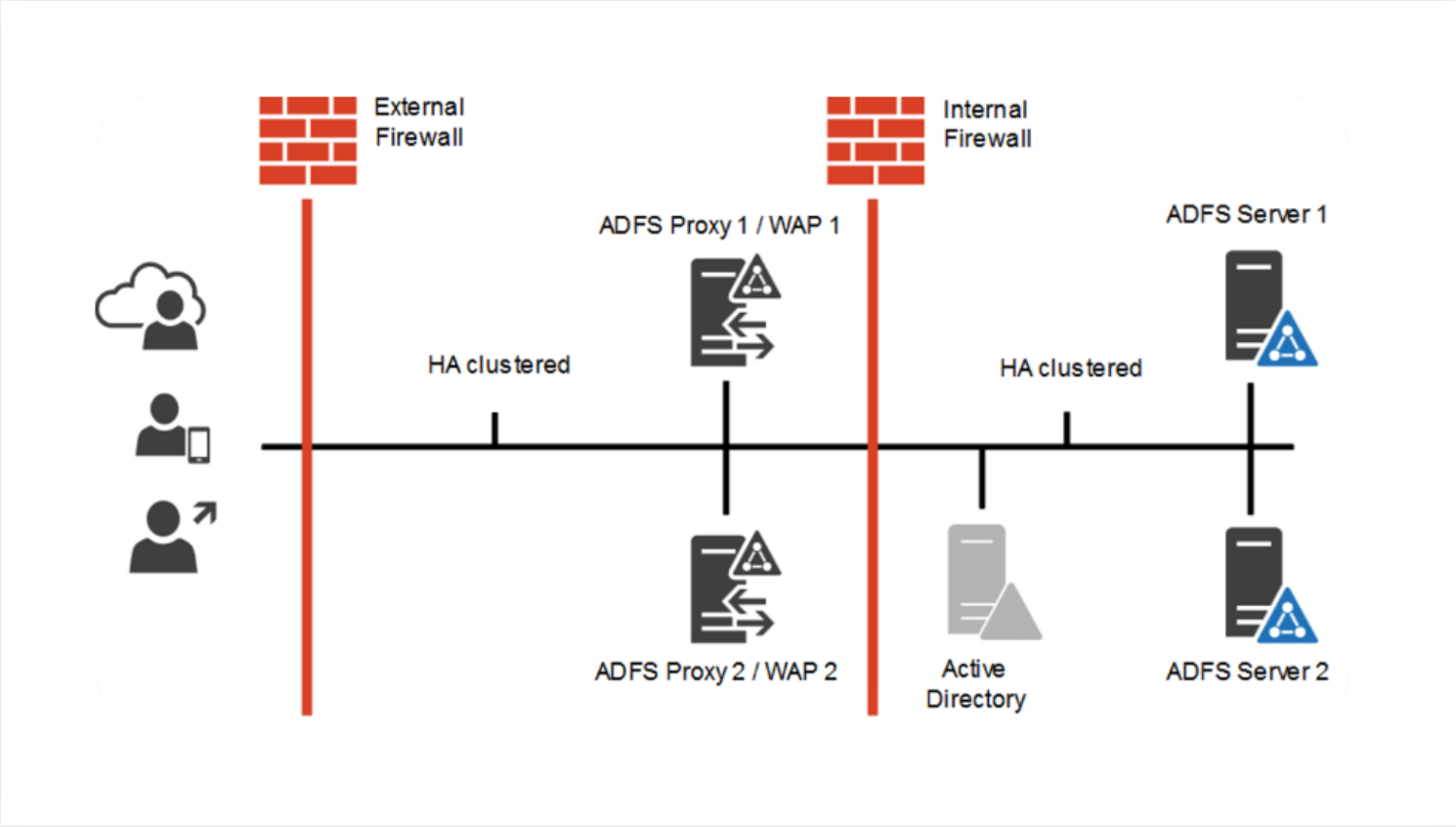
What are the Components of AD FS?



FEDERATION SERVER:

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

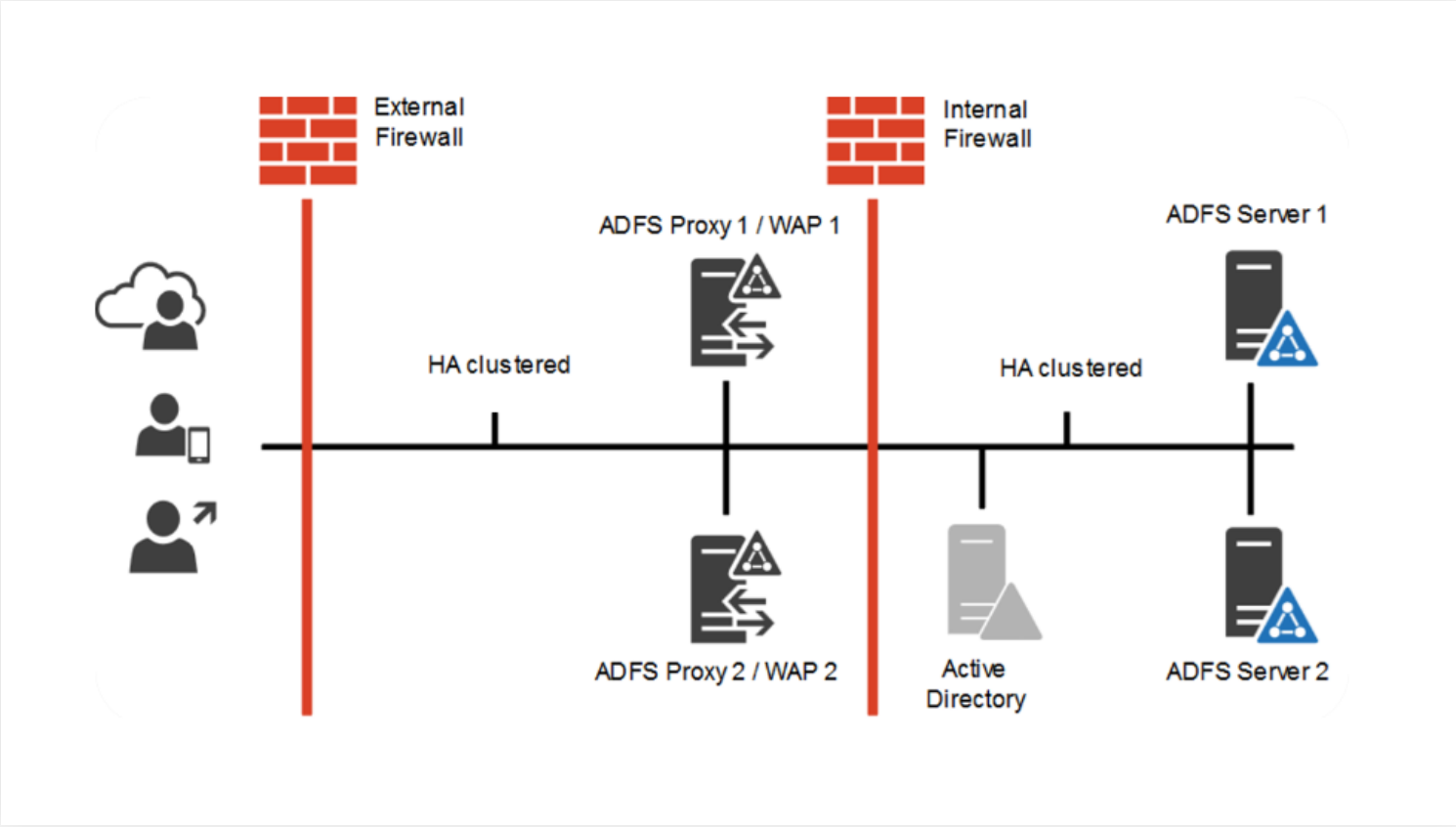
What are the Components of AD FS?



FEDERATION SERVER PROXY:

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

What are the Components of AD FS?



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.

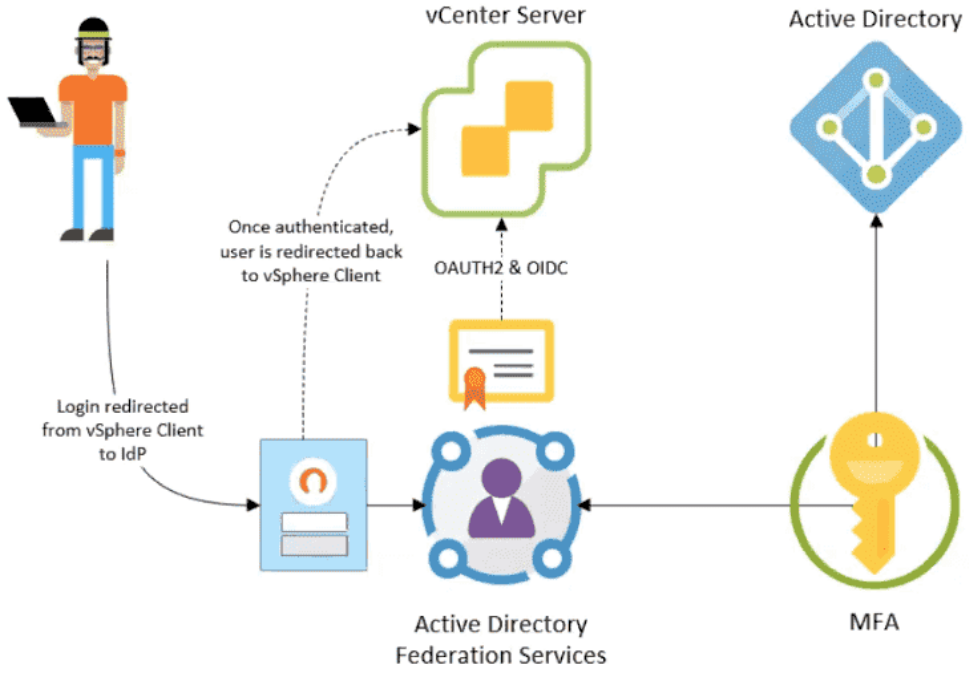
Single Sign-On with existing federated infrastructure and applications.

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 (http://example.com)
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 requirements

- 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

Prerequisites

Certificates requirement

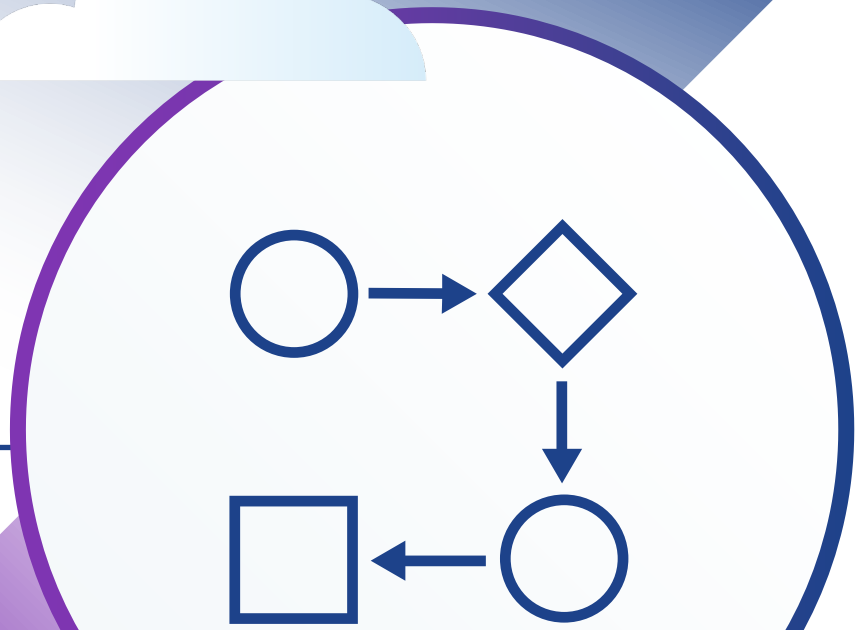
- AD FS server CA (Sub/Root) certificate to be added to the Trusted Root Certificates Store.
- Configuring LDAPs need to get the LDAP root certificate, add it to the Trusted Root Certificates within the configuration.
- How to get the AD certificate in case you will configure LDAPs.
- Run the following command in VC:
  openssl s_client -connect AD_FQDN:636

Prerequisites

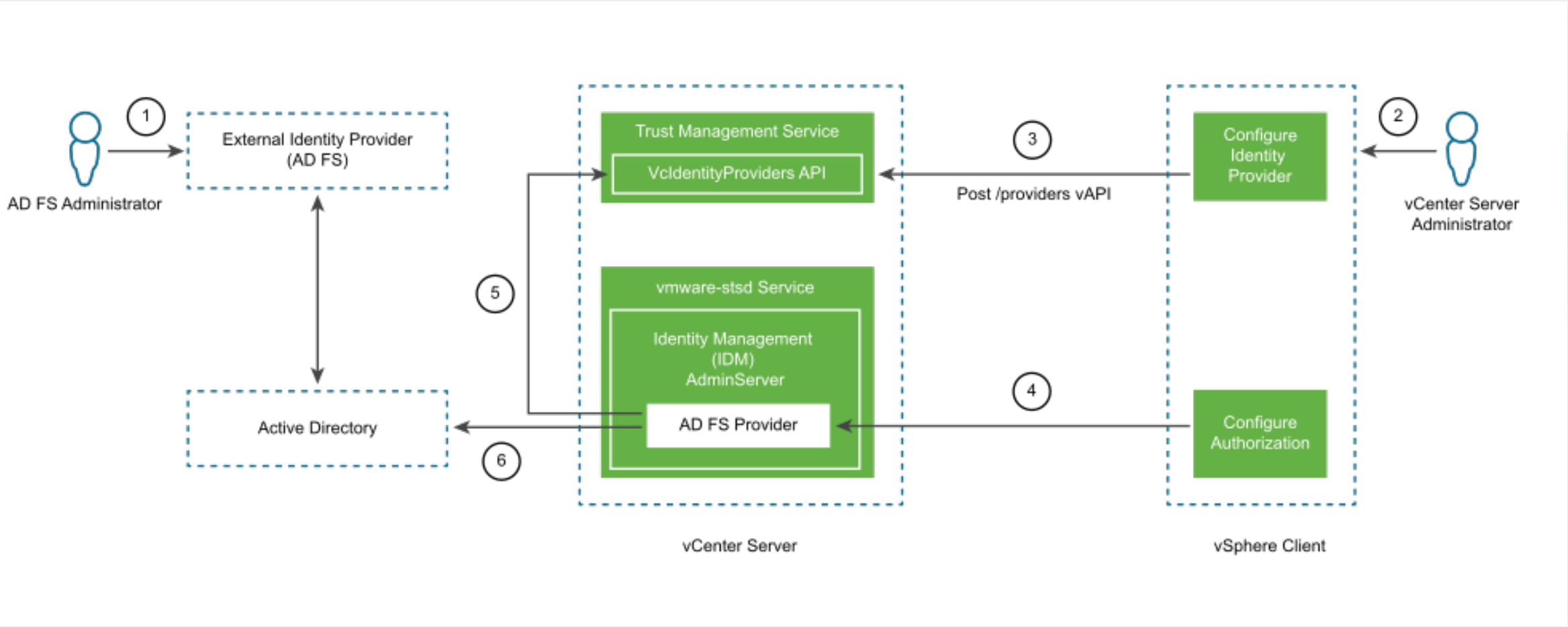
vCenter Server and other requirements

- 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

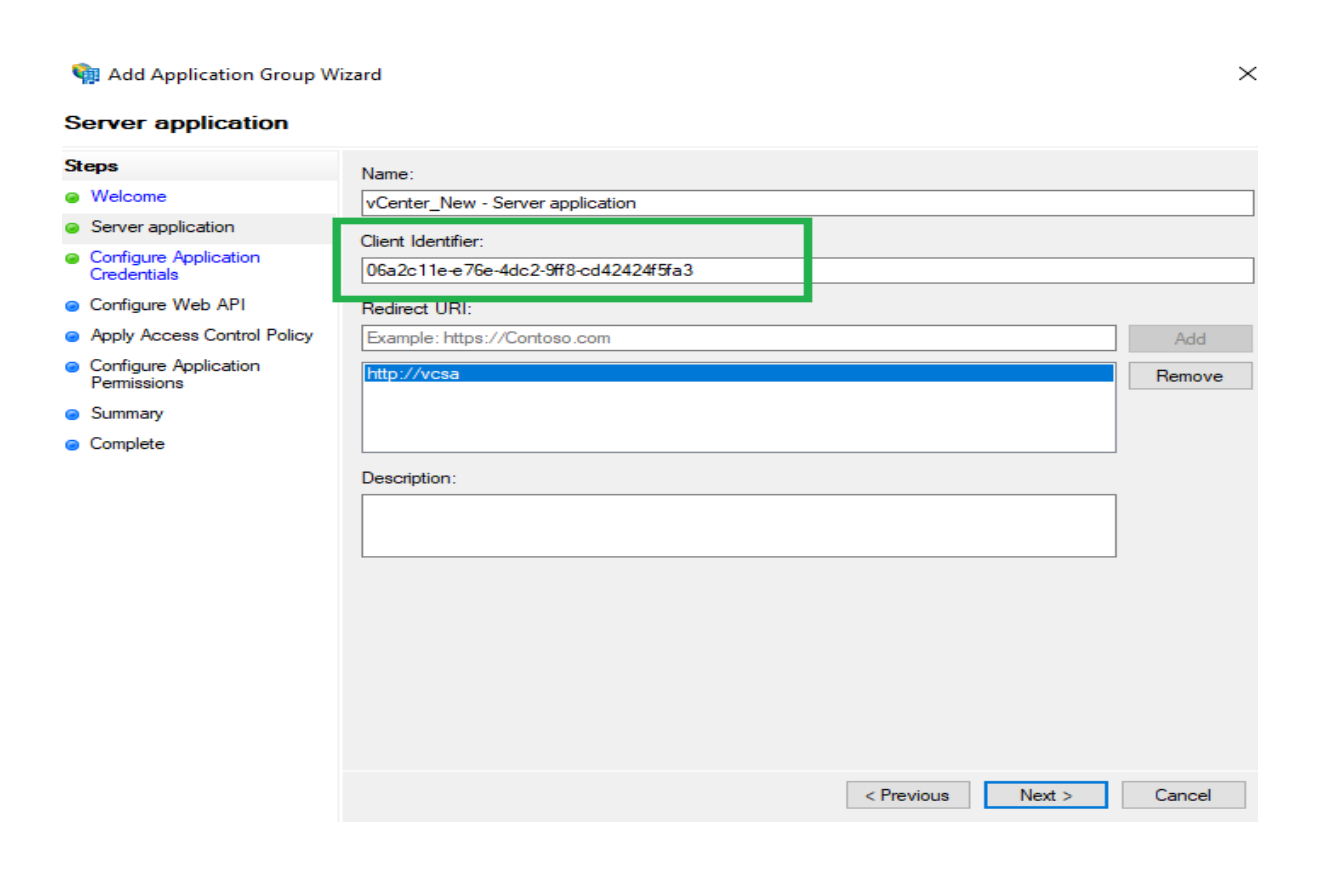


vCenter and AD FS Configuration Process Flow



Required Information

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

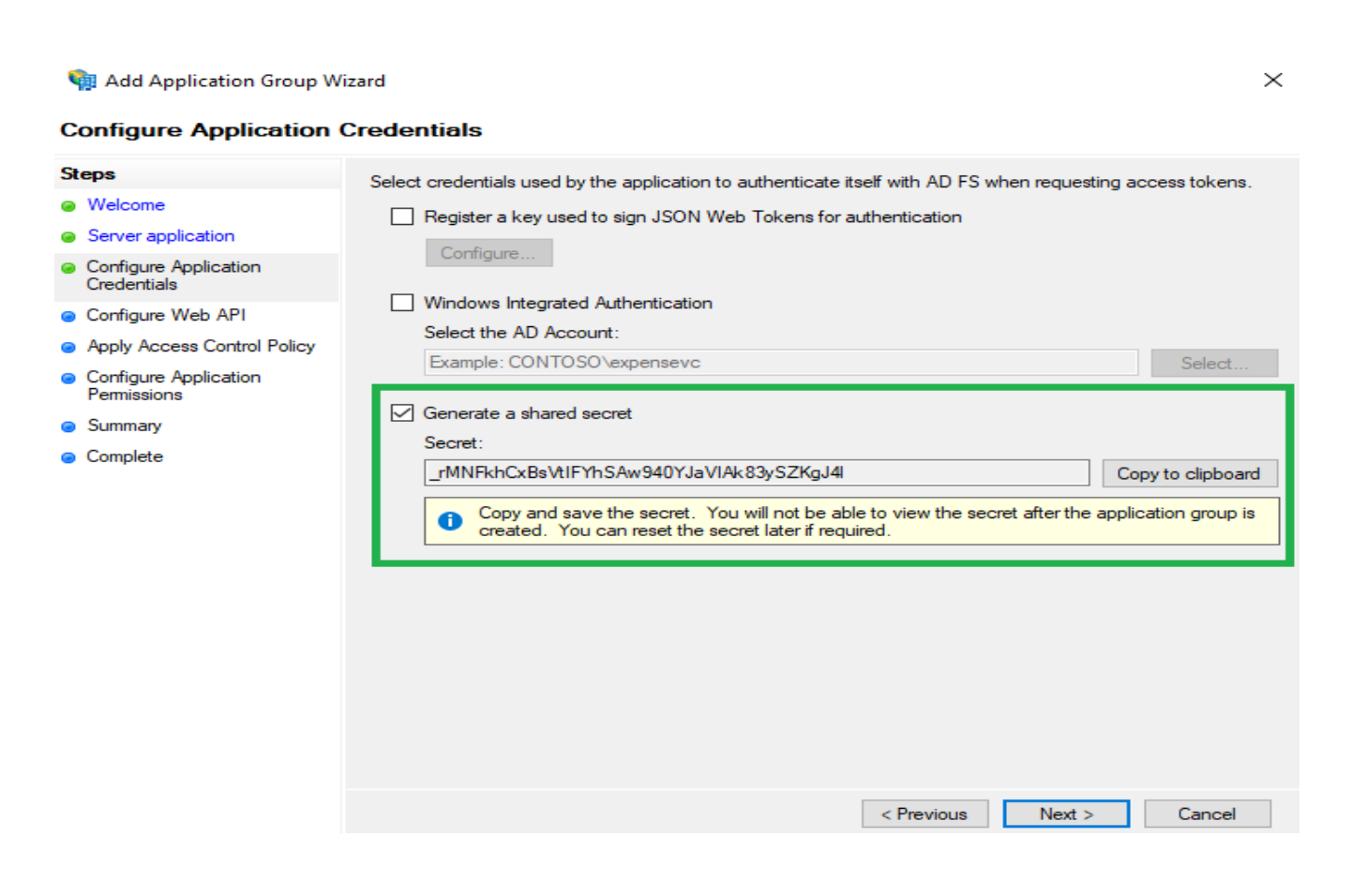


Client Identifier

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

Required Information

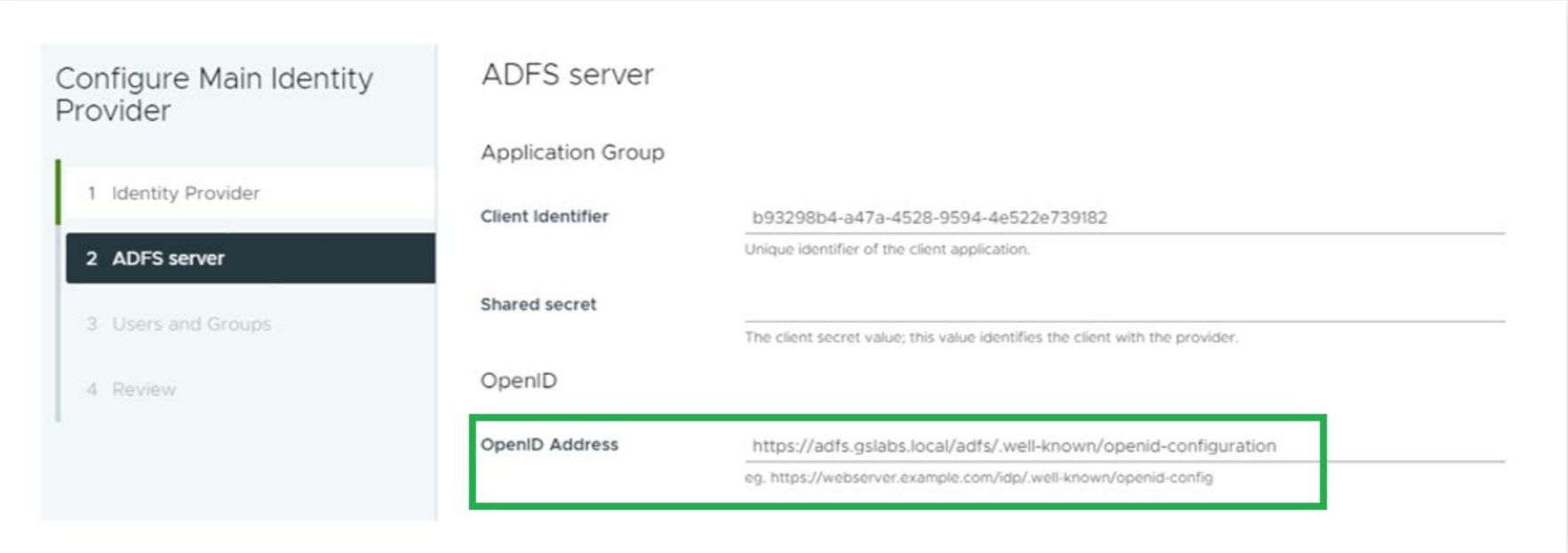
Shared Secret



- 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

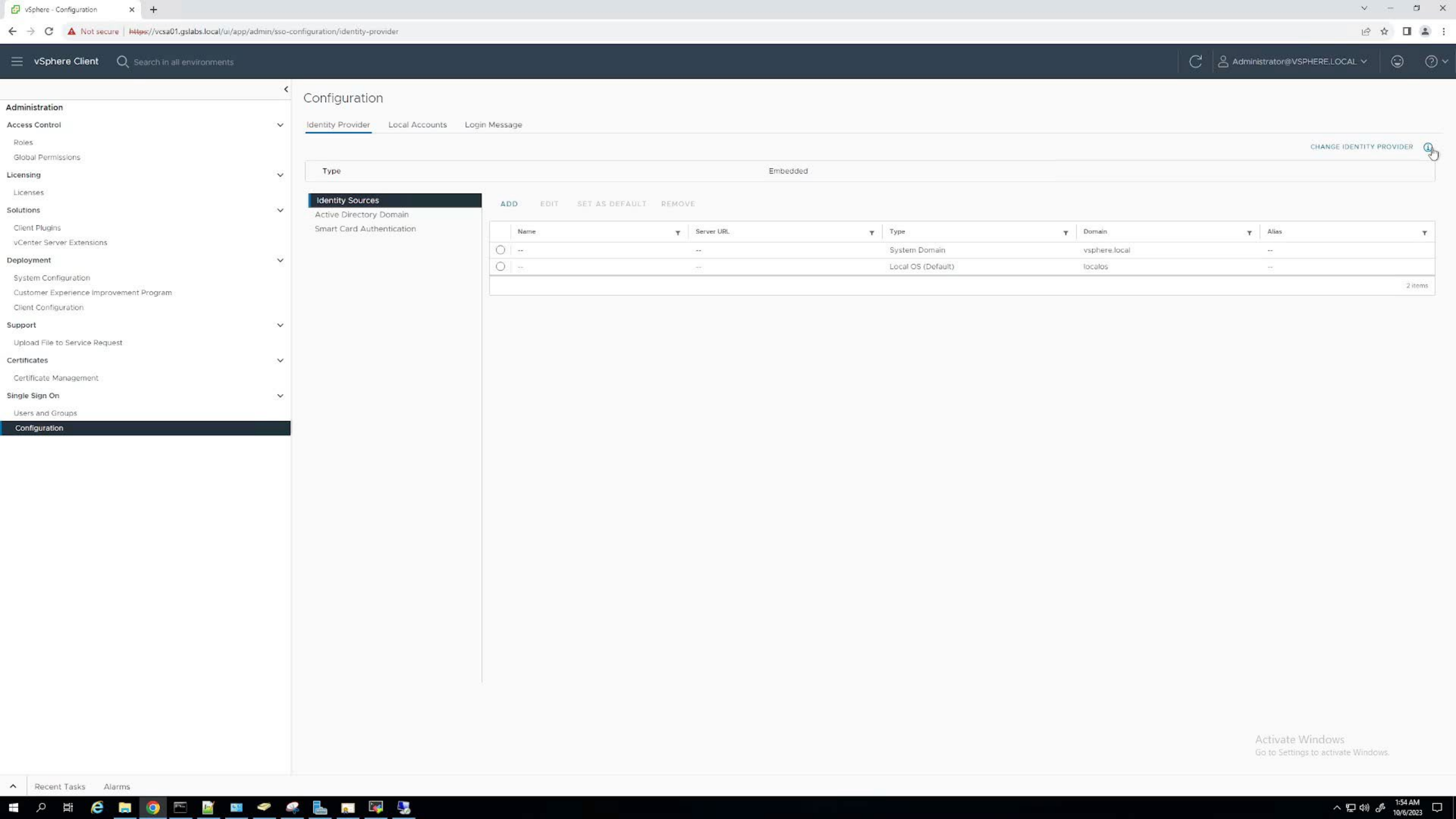
OpenID Address



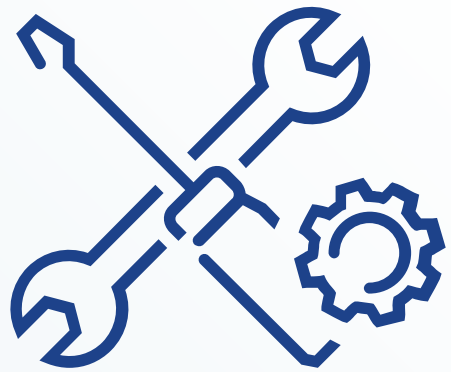
The OpenID Provider Discovery endpoint URL of the AD FS server, specifying a well-known address is typically the issuer endpoint concatenated with the path “/.well-known/openid-configuration”.

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

Setup Demo

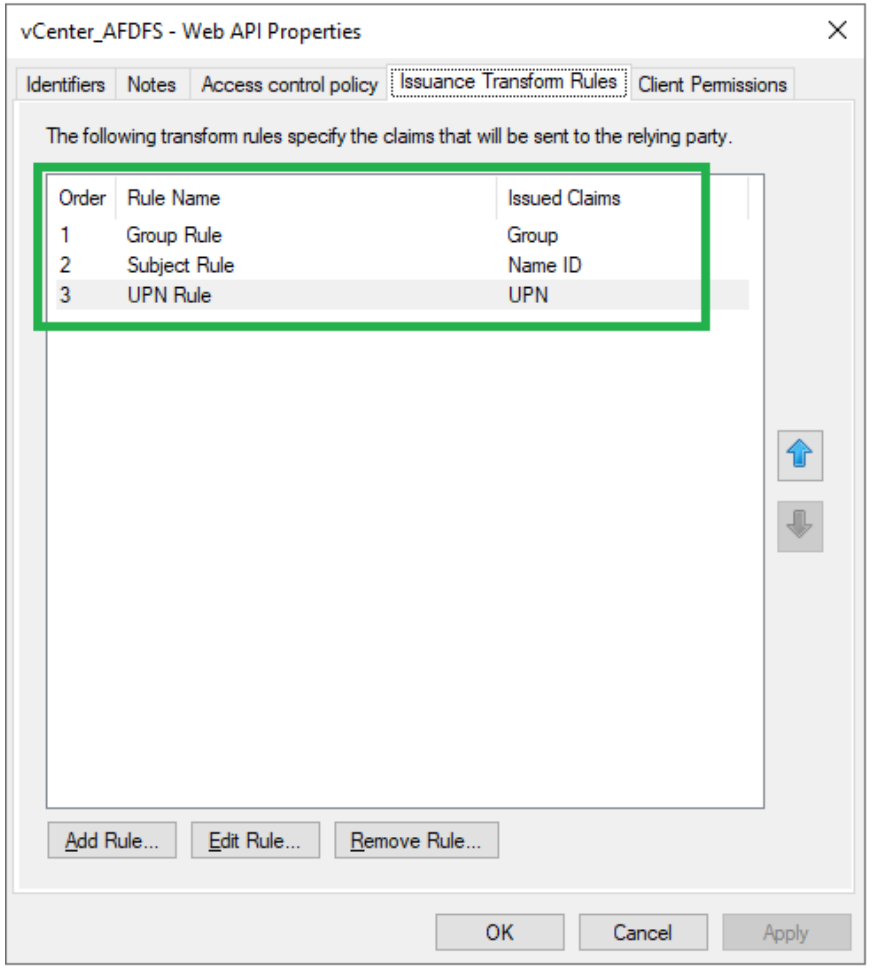

vSphere - Configuration
Not secure | https://vcsa01.gslabs.local/ui/app/admin/sso-configuration/identity-provider
vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
Administration
Access Control
Roles
Global Permissions
Licensing
Licenses
Solutions
Client Plugins
vCenter Server Extensions
Deployment
System Configuration
Customer Experience Improvement Program
Client Configuration
Support
Upload File to Service Request
Certificates
Certificate Management
Single Sign On
Users and Groups
Configuration
Configuration
Identity Provider
Local Accounts
Login Message
CHANGE IDENTITY PROVIDER
Type
Embedded
Identity Sources
Active Directory Domain
Smart Card Authentication
ADD
EDIT
SET AS DEFAULT
REMOVE
Name
Server URL
Type
Domain
Alias
-- -- System Domain vsphere.local --
-- -- Local OS (Default) localos --
2 items
Activate Windows
Go to Settings to activate Windows.
Recent Tasks
Alarms
1:54 AM
10/6/2023

Troubleshooting



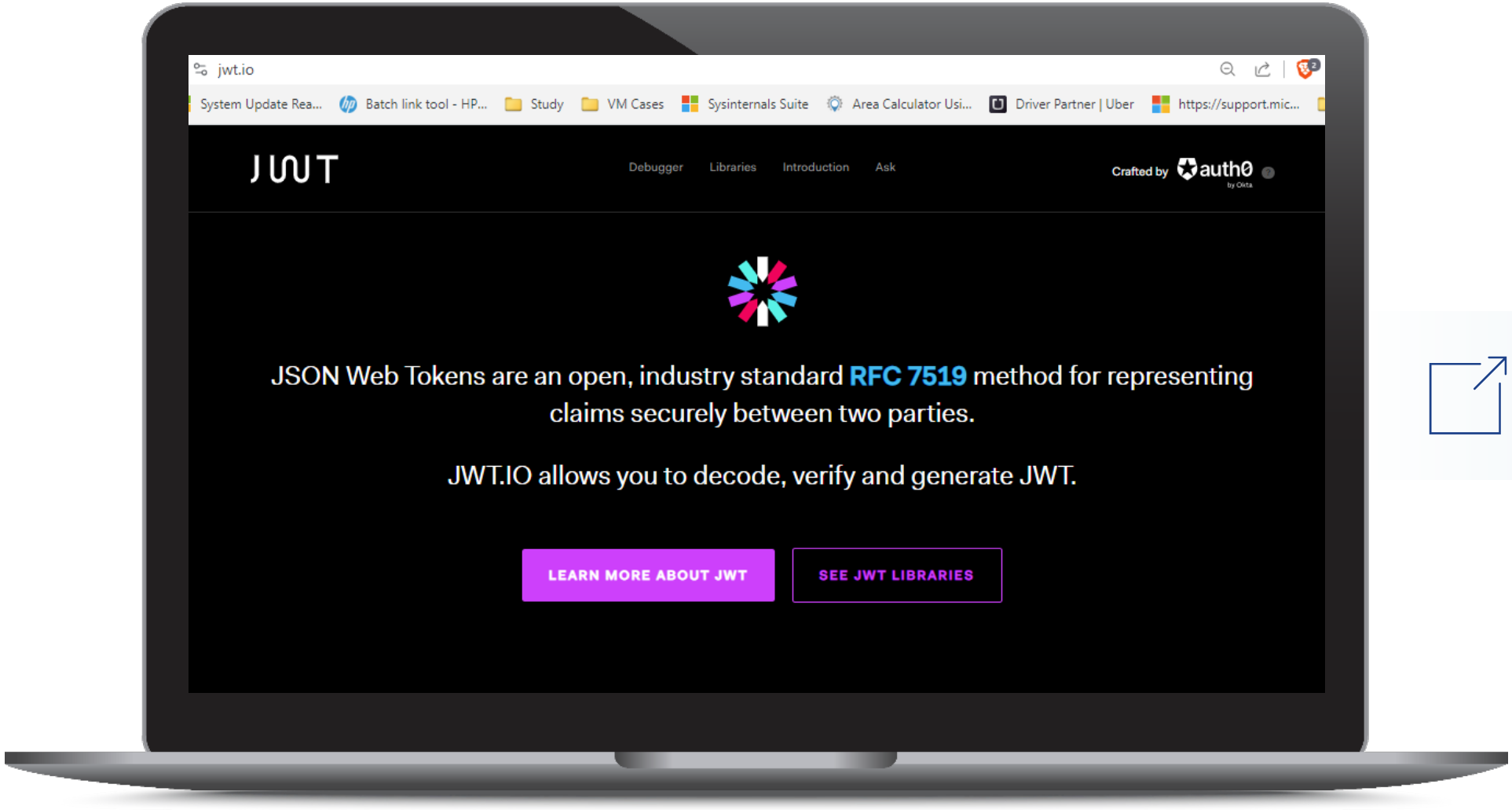
Troubleshooting

- Need to make sure you have the 3 required claims



Troubleshooting

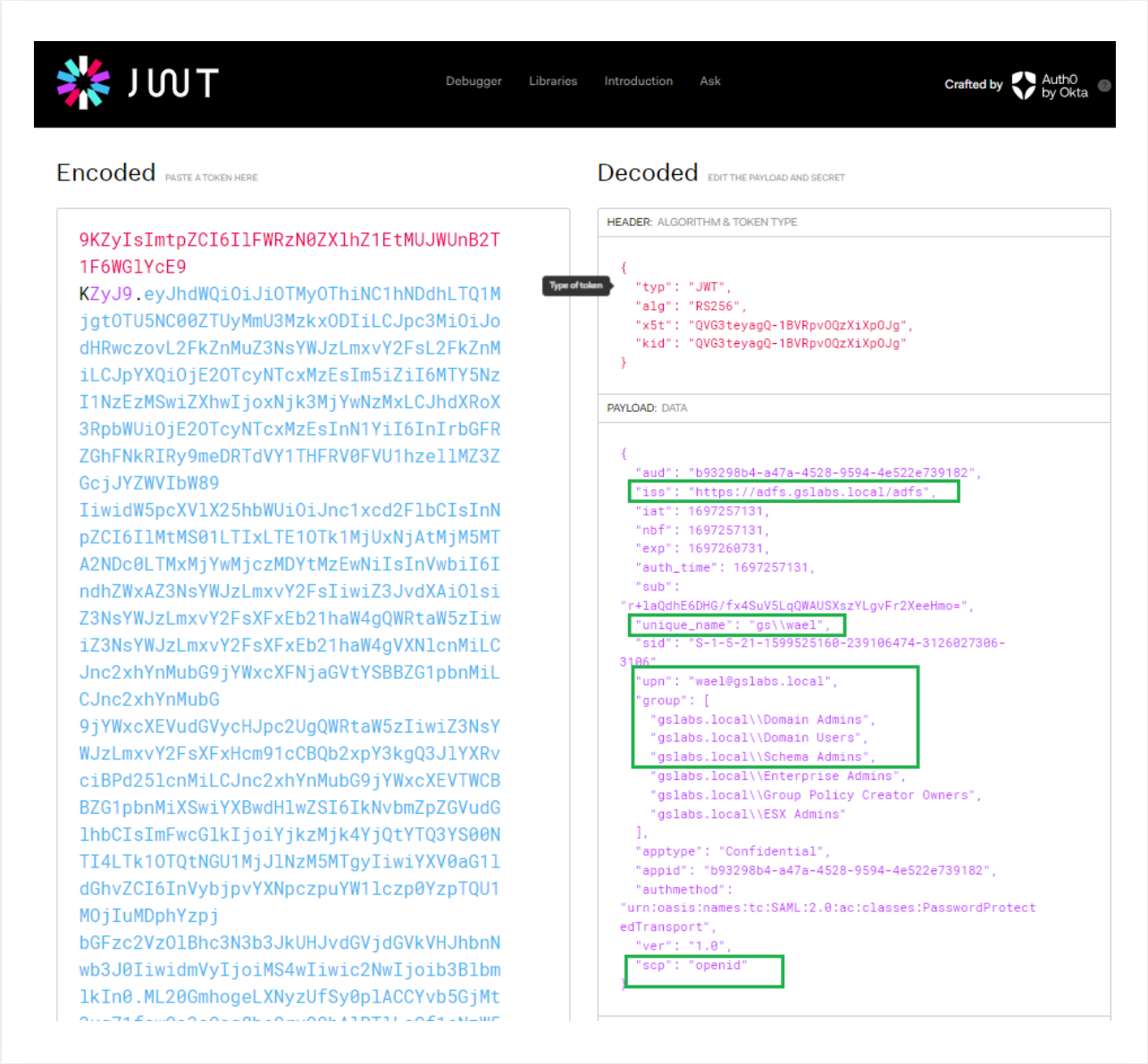
- How to translate the token by using token ID on the website



https://jwt.io/

Troubleshooting

- What should a good token look like?



Troubleshooting

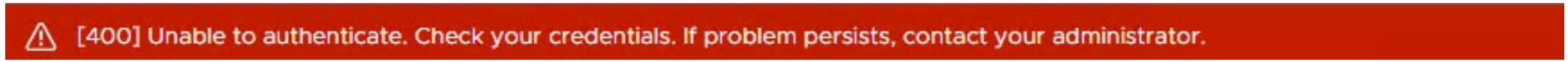
We need to enable debug logging on

- 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
```

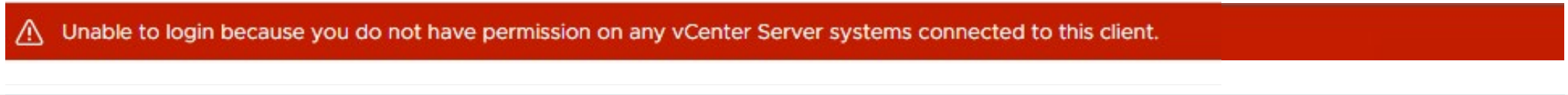
```
<root level="DEBUG">

    <!-- appender-ref ref="SIFTED_LOG_FILE" /-->
    <appender-ref ref="LOG_FILE" />
</root>
```

Troubleshooting



- 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

Troubleshooting



- 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] [CorId=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

Troubleshooting

⚠ 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)

idToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IlFWRzN0ZXlhZ1EtMUJWUnB2T1F6WGlYcE9KZyIsImtpZCI6IlFWRzN0ZXlhZ1EtMUJWUnB2T1F6WGlYcE9KZyJ9.eyJhdWQiOiI2NzFhMTdlZS1lM2E0LTRiNTgtOGRjYS0xM2RmZGU5ODM4NmYiLCJpc3MiOiJodHRwczovL2FkZnMuZ3NsYWJzLmxvY2FsL2FkZnMiLCJpYXQiOjE2ODkwMzM0NTcsIm5iZiI6MTY4OTAzMzQ1NywiZXhwIjoxNjg5MDM3MDU3LCJhdXRoX3RpbWUiOjE2ODkwMzM0NTcsInN1YiI6IkliV2FvbDNlZE5ITml3TFh2REtyTjJMRmQxVWZvMytmRE5taDNqYUFac3M9IiwidW5pcXVIX25hbWUiOiJnc1xcYWR1c2VyMS1tZWtyNTE2MC0yMzkxMDY0NzQtMzEyNjAyNzMwNi0zMTAyIiwidXBuIjoiYWR1c2VyMUBnc2xhYnMubG9jYWwiLCJncm91cCI6Imdzb2FicyI5sb2NhbFxcRG9tYWluIFVzZXJzIiwiYXBwdHlwZSI6IkNvbmZpZGVudGlhbCIsImFwcGlkIjoiNjcxYTE3ZWUtZTNhNC00YjU4LTkhY2EtMTNkZmRlOTgzODZmIiwiYXV0aG1ldGhvZCI6InVybjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDphYzpjbGFzc2VzOlBhc3N3b3JkUHJvdGVjdGVkYHJhbnNwb3J0IiwidmVyIjoiMS4wIiwic2NwIjoib3BlbmlkIn0.Vznt1529c1U11EyJzG6yS7X_D0vkso_pBNesxicDgG0ddvvyRDGddBff5a8YceFs1B64MmyE7TSeLpueHgi2fPLPhJnDMwTtf-zvJKhZ2DQwWMf_R0RPCXXScb2g508BiBePY_VHynFW91h04_kjQ_opRvpQbHKhl1IDbmnB7Ir4BjTDFuhNV_M15kSh6j6bZ5CN3W8no5yarN1bOo7JrPu9hFPnJ78c14tIYCSLxfd3adF3iQStX8T64m4uaOtLqVee4NFMwESsPeKfF37GPalTeYfV_oCb30THOKPK97AuwvxeKM8-rFZBrkvQuImLxAvXdLD4RvZ0LRdc0ECVnw, tokenType=bearer, expiresIn=3600, scope=null, jti=null)

- Paste on **https://jwt.io/**

Troubleshooting

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":
"JN7CMm1Jb4iGov5xZb5bl1INFu7ry+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"
}
```

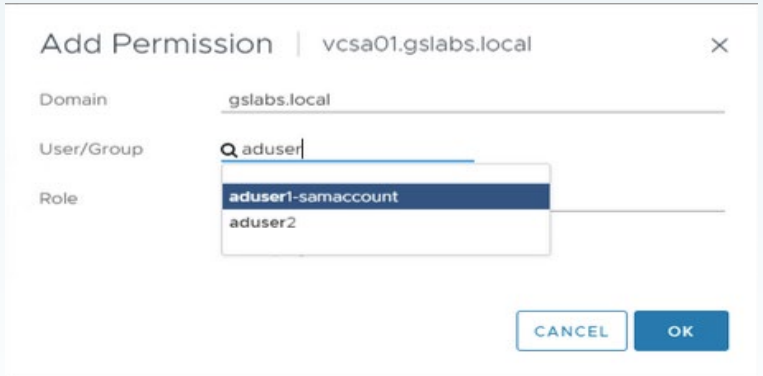
Troubleshooting

⚠ 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.

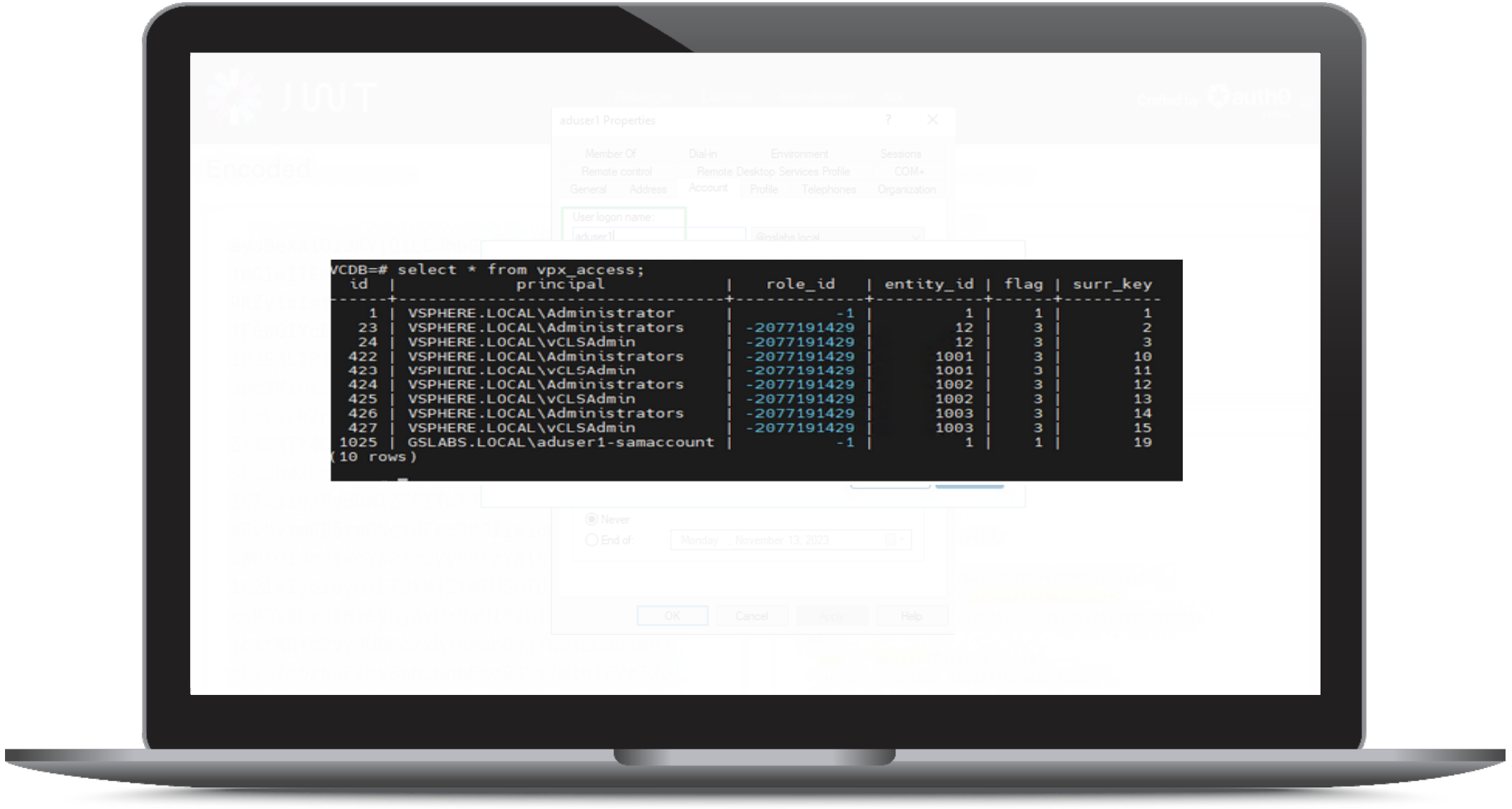
> This occurs because the logic in vCenter that searches for AD identities in the "Add Members" UI widget uses the sAM Account Name attribute when it is constructing the membership entry in the VC group.
> But during login, you get the UPN from the AD FS token and use that for comparison.



Workaround:

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

Troubleshooting



```
VCDB=# select * from vpx_access;
  id  |              principal              |   role_id   | entity_id | flag | surr_key
------+-------------------------------------+-------------+-----------+------+----------
    1 | VSPHERE.LOCAL\Administrator         |          -1 |         1 |    1 |        1
   23 | VSPHERE.LOCAL\Administrators        | -2077191429 |        12 |    3 |        2
   24 | VSPHERE.LOCAL\vCLSAdmin             | -2077191429 |        12 |    3 |        3
  422 | VSPHERE.LOCAL\Administrators        | -2077191429 |      1001 |    3 |       10
  423 | VSPHERE.LOCAL\vCLSAdmin             | -2077191429 |      1001 |    3 |       11
  424 | VSPHERE.LOCAL\Administrators        | -2077191429 |      1002 |    3 |       12
  425 | VSPHERE.LOCAL\vCLSAdmin             | -2077191429 |      1002 |    3 |       13
  426 | VSPHERE.LOCAL\Administrators        | -2077191429 |      1003 |    3 |       14
  427 | VSPHERE.LOCAL\vCLSAdmin             | -2077191429 |      1003 |    3 |       15
 1025 | GSLABS.LOCAL\aduser1-samaccount     |          -1 |         1 |    1 |       19
(10 rows)
```

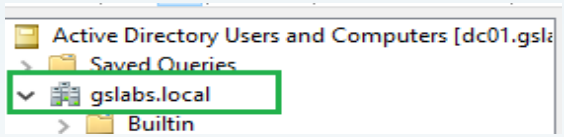
Troubleshooting

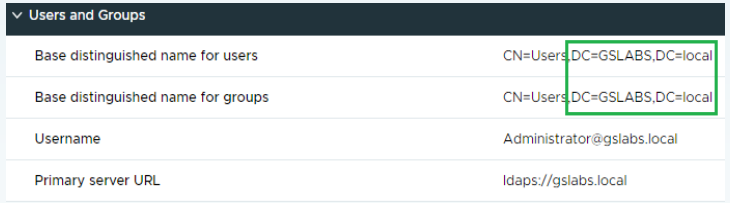
⚠ Unable to login because you do not have permission on any vCenter Server systems connected to this client.

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:

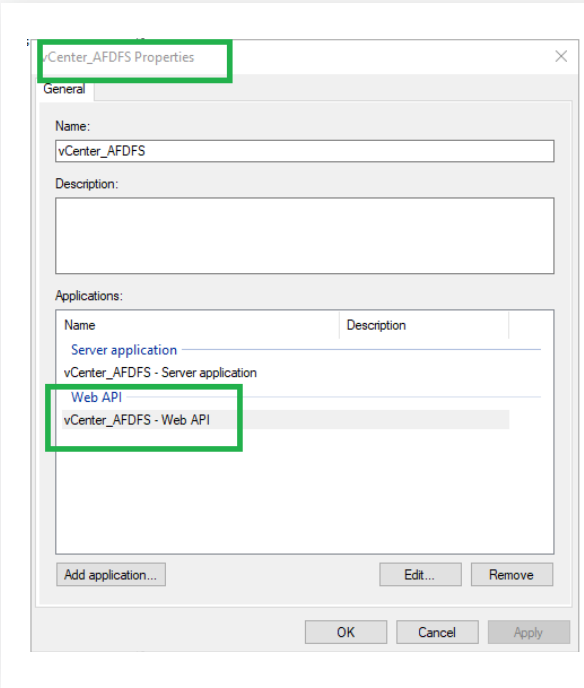
Add the user direct permission on the VC, instead of Group

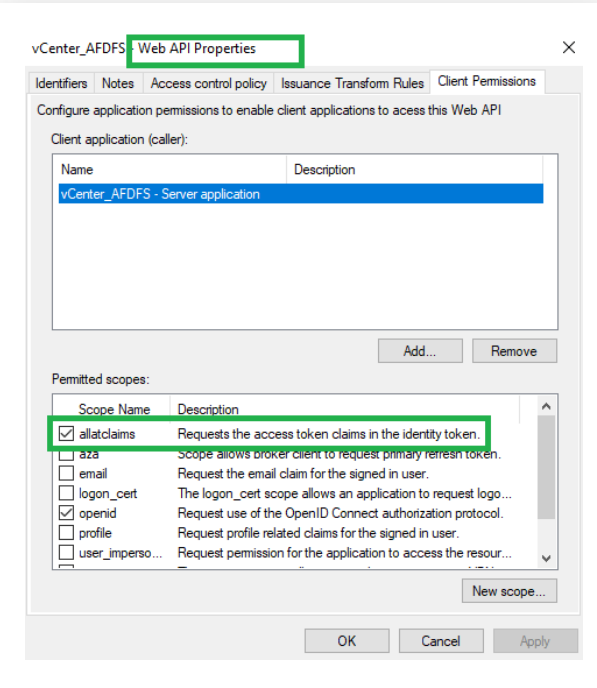
Troubleshooting

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.





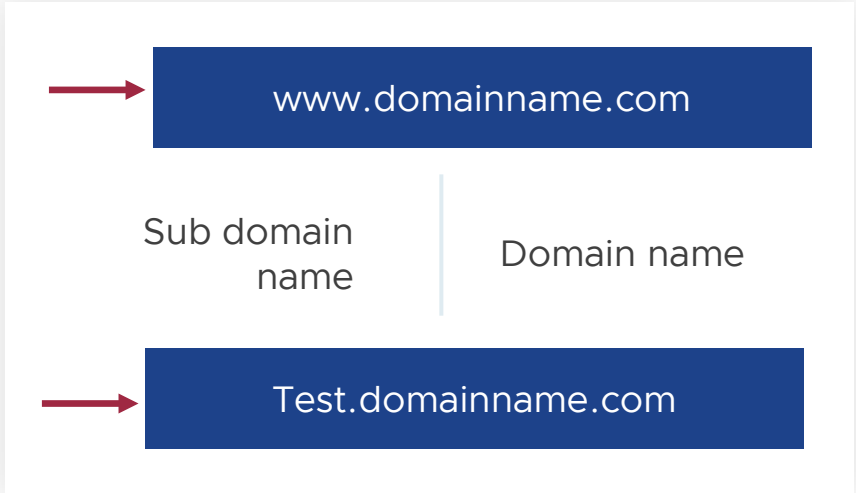
Troubleshooting

Issue: Users can't login while using sub-domains in the AD FS topology.

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

Workaround:

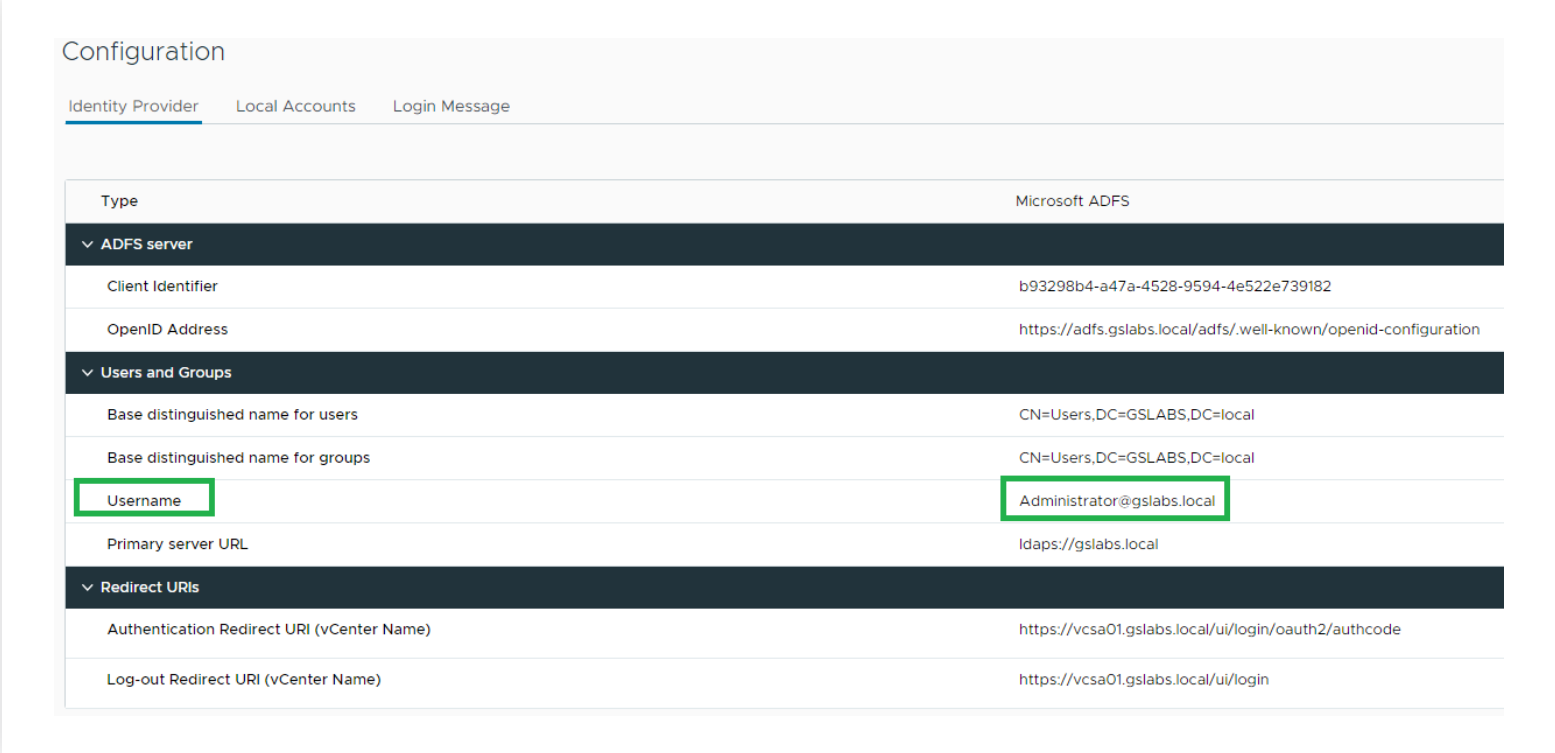
- Create a group in main domain and add the sub domains users
- Add that group to the vCenter
- By design vCenter doesn't support having multiple domains



Troubleshooting

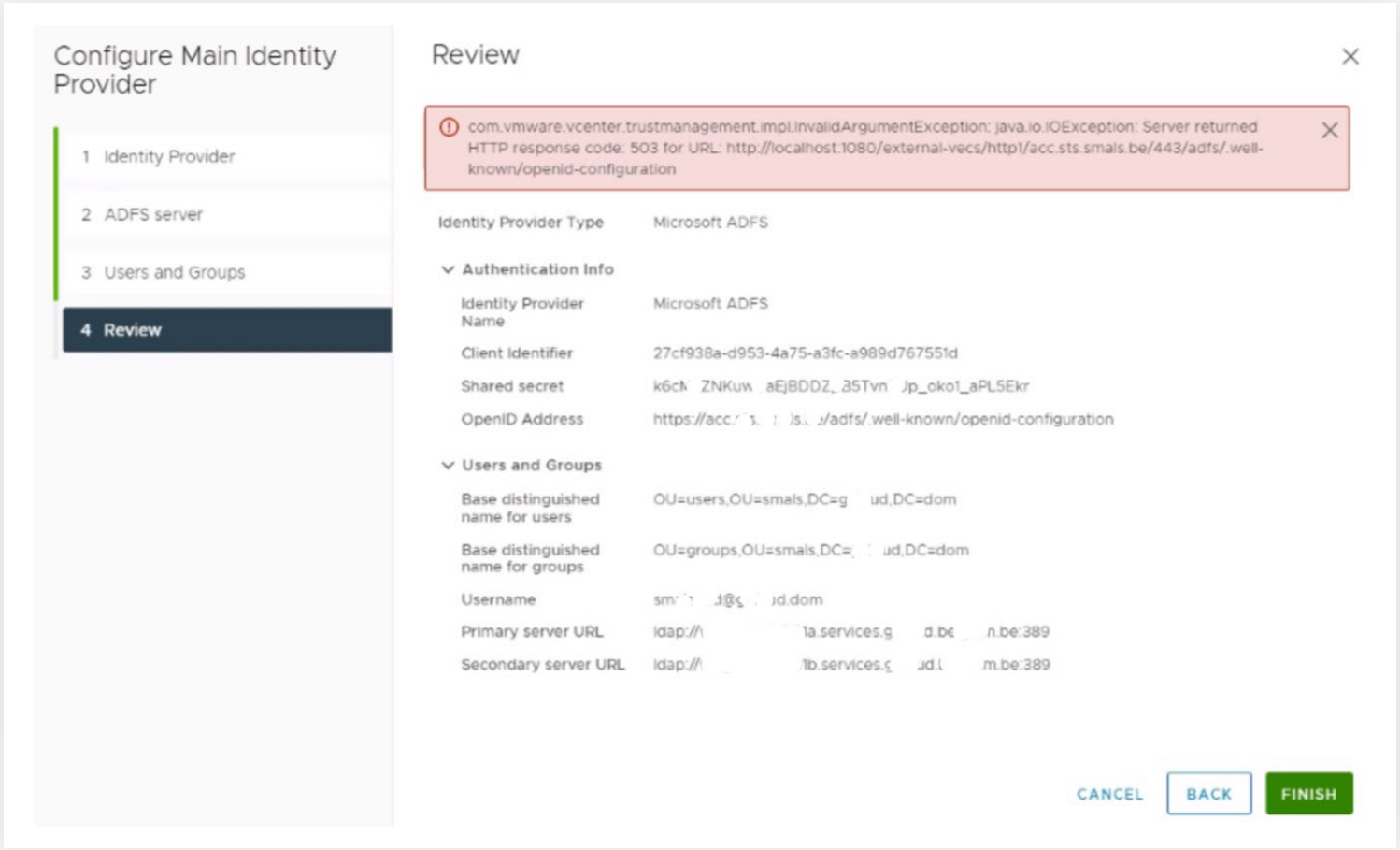
Issue: Can't add account or query from the AD FS Domain.

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



Troubleshooting

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



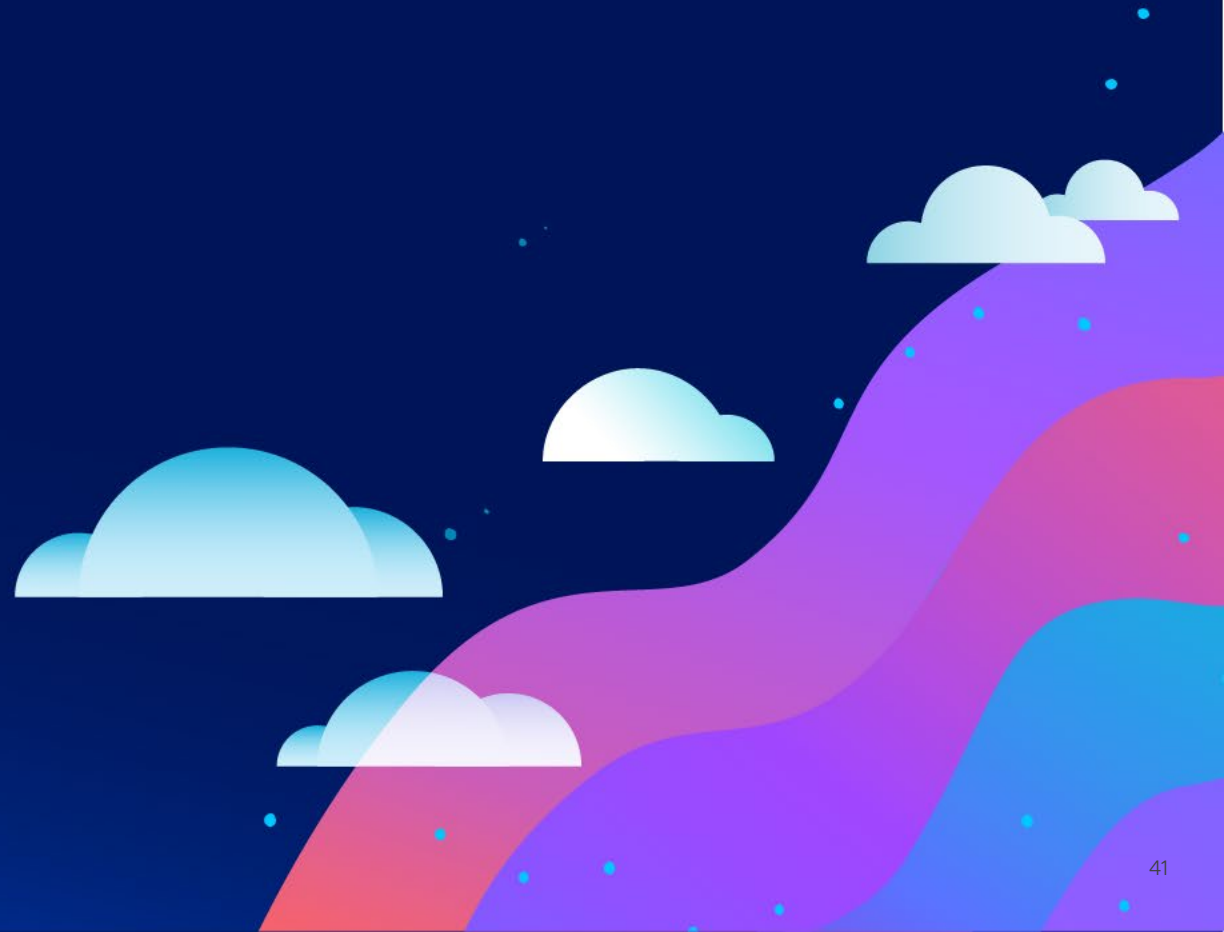
Troubleshooting

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