Documentation for reported error where LDAP cannot be switched from Simple to Kerberos.

Requirements:

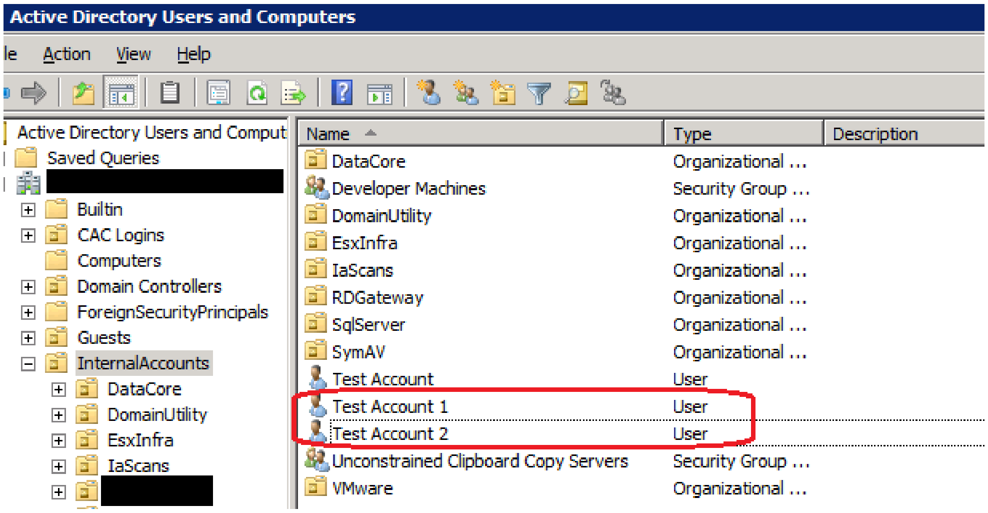
- vCD 5.1.2 (latest patches) with simple LDAP authentication and AD usersimported.
- Two brand-new test Active Directory users TestAccount1 and TestAccount2 that have *not* ever been entered into vCloud Director as owning any objects

Procedure:

- Set LDAP to Simple.
- Under Admin / Users: Import AD TestAccount1. Displays with sAMAccountName.
- Validate TestAccount1 login (using sAMAccountName).
- Change LDAP authentication from Simple to Kerberos.
- Under Admin / Users: Import AD TestAccount2. Displays with userPrincipalName.
- Validate TestAccount2 login (using userPrincipalName).
- Verify TestAccount1 login no longer works.
- Under Admin / Users: Disable and Delete AD TestAccount1.
- Under Admin / Users: Import AD TestAccount1 user again. Verify that – although Kerberos is in effect – user continues to display with sAMAccountName.
- Verify that TestAccount1 longer continues not to work.

Supporting Screenshots:

Two test AD accounts TestAccount1 and TestAccount2. These are brand-new accounts:

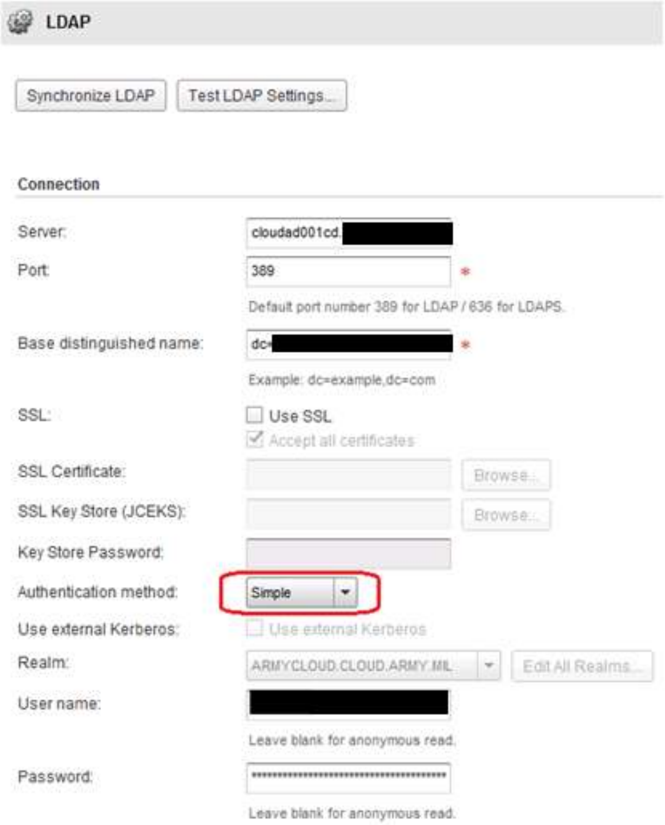


Active Directory Users and Computers

Active Directory Users and Comput
Saved Queries
[redacted]
Builtin
CAC Logins
Computers
Domain Controllers
ForeignSecurityPrincipals
Guests
InternalAccounts
DataCore
DomainUtility
EsxInfra
IaScans
[redacted]

Name	Type	Description
DataCore	Organizational ...	
Developer Machines	Security Group ...	
DomainUtility	Organizational ...	
EsxInfra	Organizational ...	
IaScans	Organizational ...	
RDGateway	Organizational ...	
SqlServer	Organizational ...	
SymAV	Organizational ...	
Test Account	User	
Test Account 1	User	
Test Account 2	User	
Unconstrained Clipboard Copy Servers	Security Group ...	
VMware	Organizational ...	

LDAP set to Simple as shown below:



Connection

Server: cloudad001cd.[redacted]

Port: 389 *

Default port number 389 for LDAP / 636 for LDAPS.

Base distinguished name: dc=[redacted] *

Example: dc=example,dc=com

SSL: ☐ Use SSL

☑ Accept all certificates

SSL Certificate: Browse...

SSL Key Store (JCEKS): Browse...

Key Store Password:

Authentication method: Simple

Use external Kerberos: ☐ Use external Kerberos

Realm: ARMYCLOUD.CLOUD.ARMY.MIL Edit All Realms...

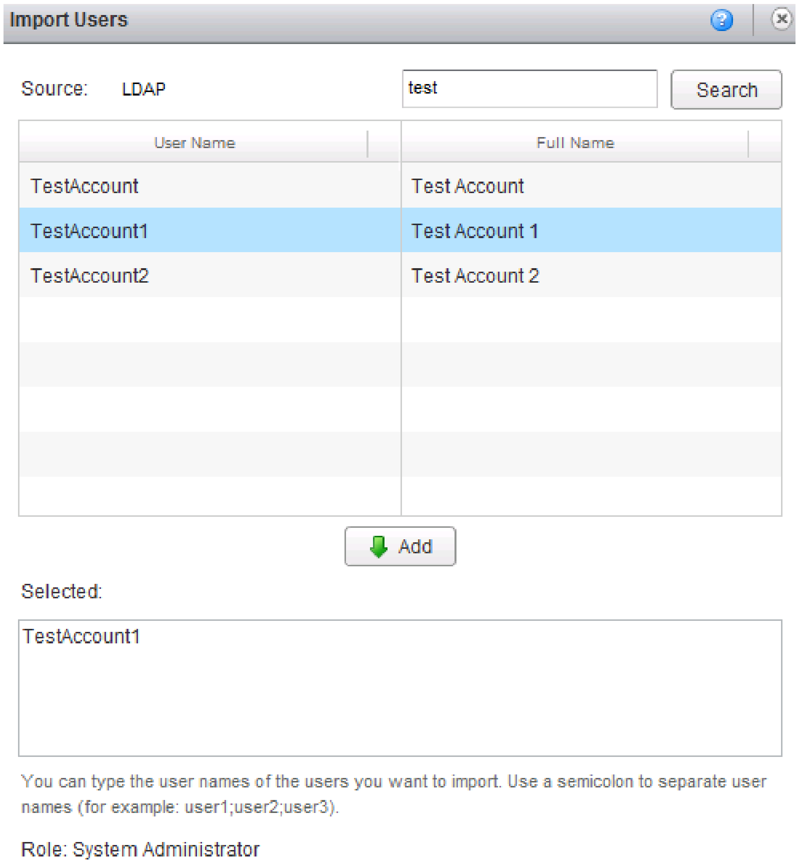
User name: [redacted]

Leave blank for anonymous read.

Password: **

Leave blank for anonymous read.

Import TestAccount1 into LDAP:



Import Users

Source: LDAP

test — Search

User Name	Full Name
TestAccount	Test Account
TestAccount1	Test Account 1
TestAccount2	Test Account 2

Add

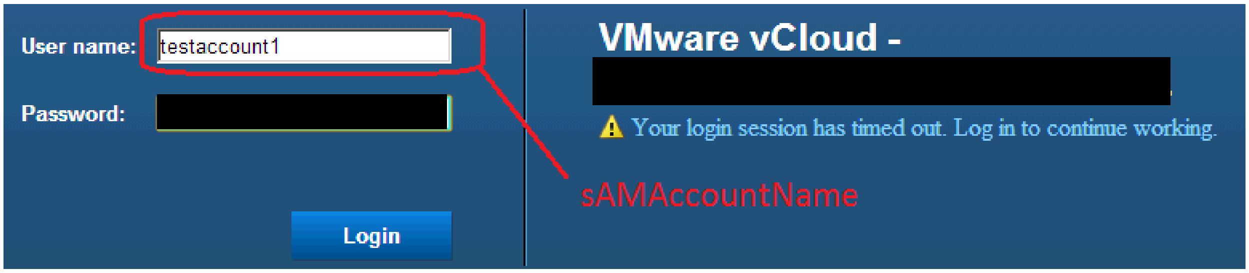
Selected:

TestAccount1

You can type the user names of the users you want to import. Use a semicolon to separate user names (for example: user1;user2;user3).

Role: System Administrator

Verify login from second browser:



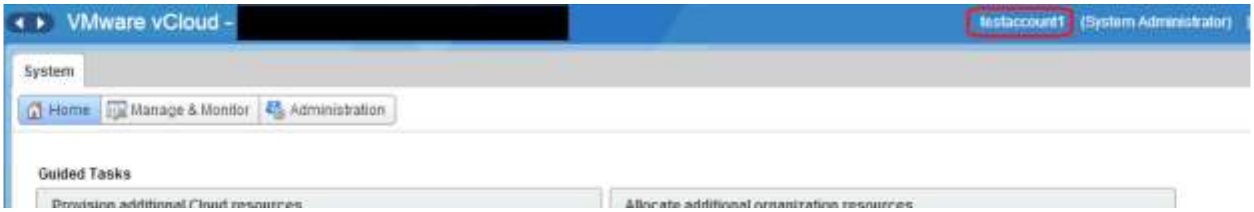
User name: testaccount1

Password: [redacted]

Login

VMware vCloud - [redacted]

⚠ Your login session has timed out. Log in to continue working.



VMware vCloud - [redacted]

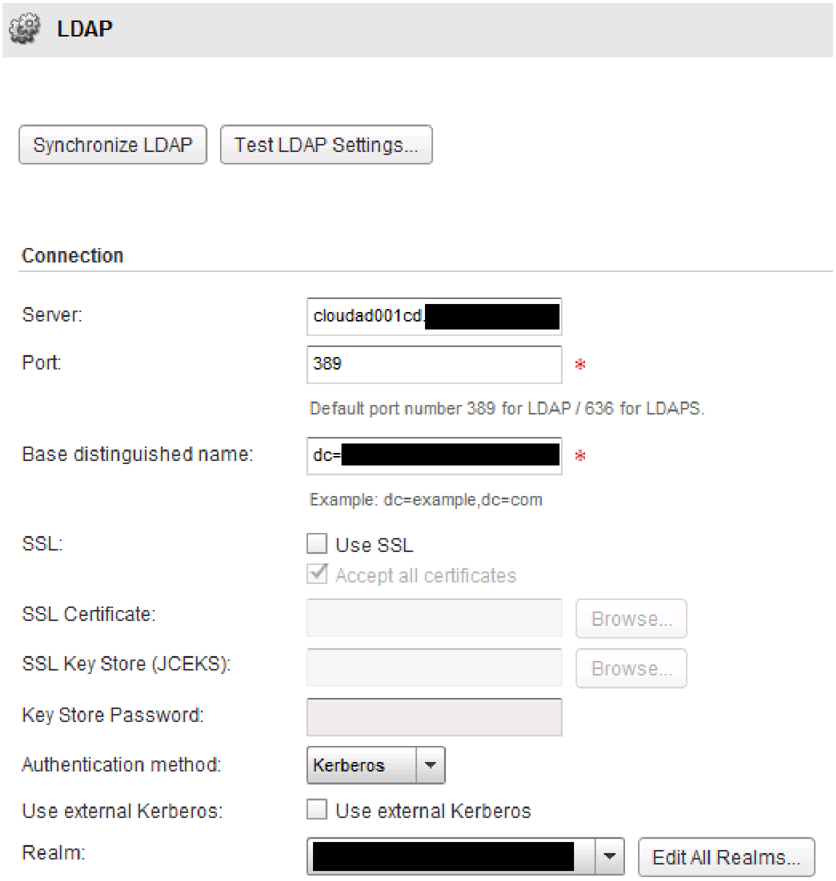
testaccount1 (System Administrator)

Guided Tasks

Provision additional Cloud resources

Allocate additional organization resources

Set LDAP to Kerberos:

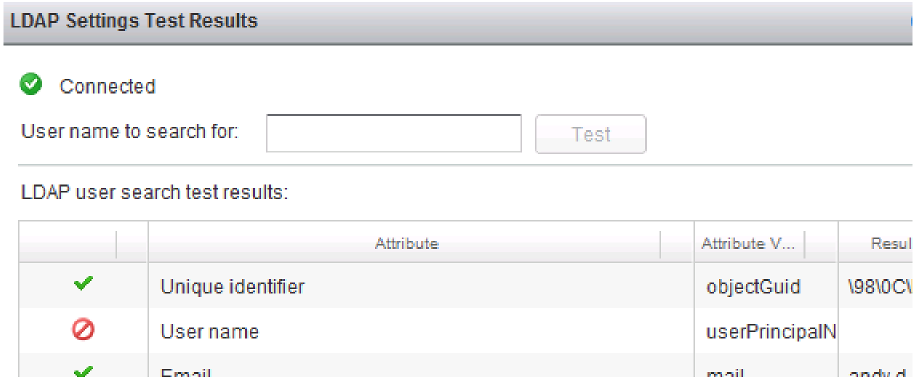


LDAP

Connection

Server:	cloudad001cd.[redacted]
Port:	389 *
	Default port number 389 for LDAP / 636 for LDAPS.
Base distinguished name:	dc=[redacted] *
	Example: dc=example,dc=com
SSL:	□ Use SSL ☑ Accept all certificates
SSL Certificate:	Browse...
SSL Key Store (JCEKS):	Browse...
Key Store Password:	
Authentication method:	Kerberos
Use external Kerberos:	□ Use external Kerberos
Realm:	[redacted] Edit All Realms...

Verify that LDAP connectivity works:



LDAP Settings Test Results

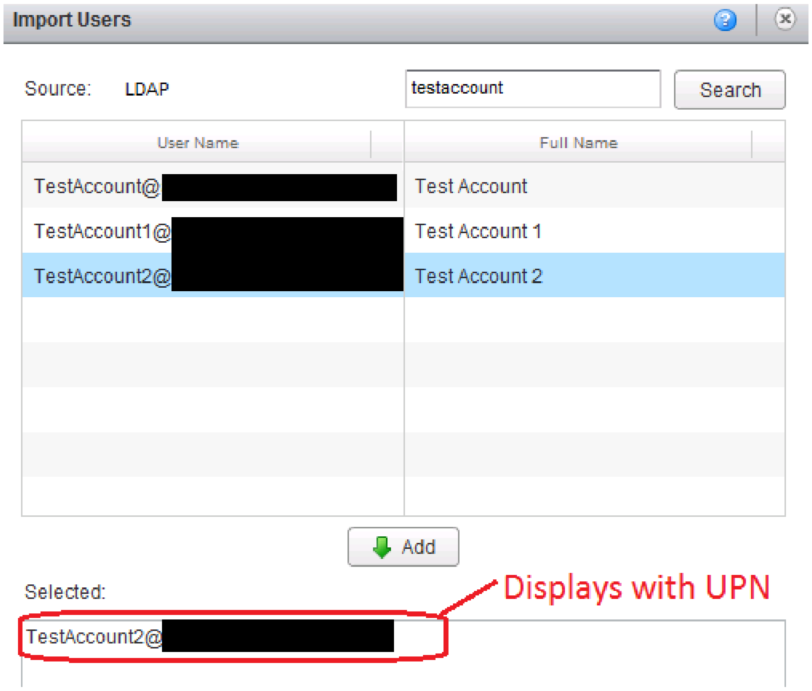
✓ Connected

User name to search for: Test

LDAP user search test results:

	Attribute	Attribute V...	Resul
✓	Unique identifier	objectGuid	\98\0C\
⊘	User name	userPrincipalN	
✓	Email	mail	andy.d

Import TestAccount2 user:



Import Users

Source: LDAP

testaccount

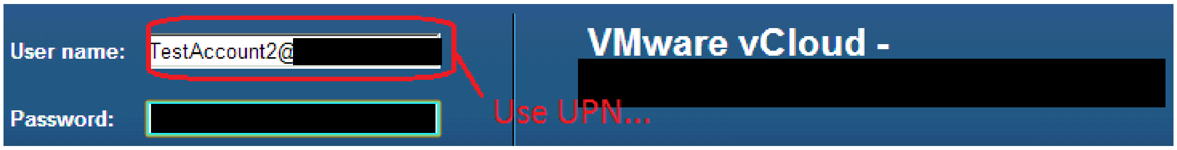
User Name	Full Name
TestAccount@[redacted]	Test Account
TestAccount1@[redacted]	Test Account 1
TestAccount2@[redacted]	Test Account 2

Selected:

TestAccount2@[redacted]

Displays with UPN

Verify that TestAccount2 works (with UPN):

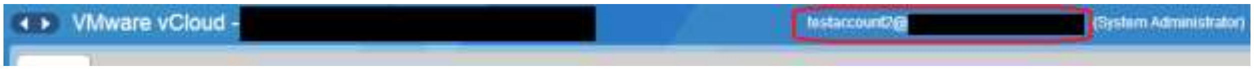


User name: TestAccount2@[redacted]

Password: [redacted]

Use UPN…

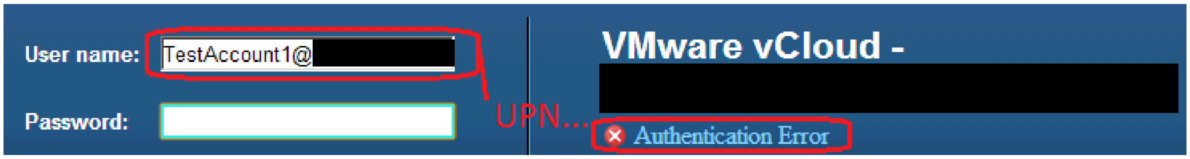
VMware vCloud - [redacted]



VMware vCloud - [redacted]

testaccount2@[redacted] (System Administrator)

Verify that TestAccount1 does *not* work either with UPN or with sAMAccountName:



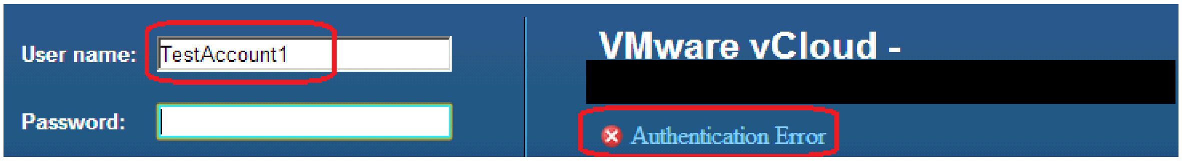
User name: TestAccount1@[redacted]

Password:

UPN…

VMware vCloud - [redacted]

Authentication Error



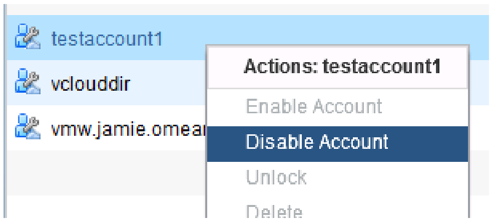
User name: TestAccount1

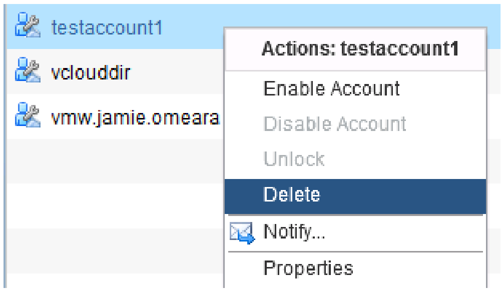
Password:

VMware vCloud - [redacted]

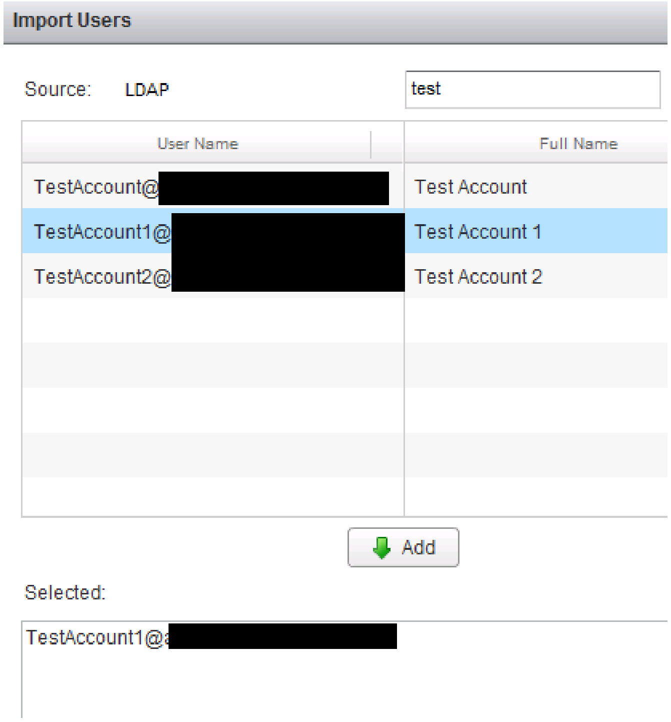
Authentication Error

Disable and delete the TestAccount1:





Add TestAccount1 back in – Kerberos is still active:



Source: LDAP

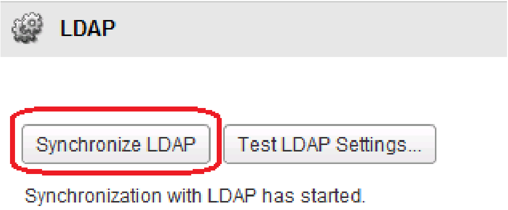
test

User Name	Full Name
TestAccount@[redacted]	Test Account
TestAccount1@[redacted]	Test Account 1
TestAccount2@[redacted]	Test Account 2

Selected:

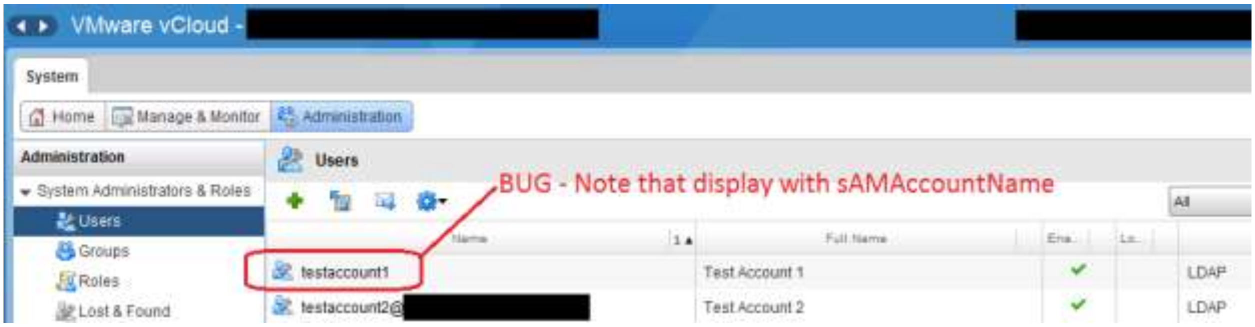
TestAccount1@[redacted]

Resync LDAP:



Synchronization with LDAP has started.

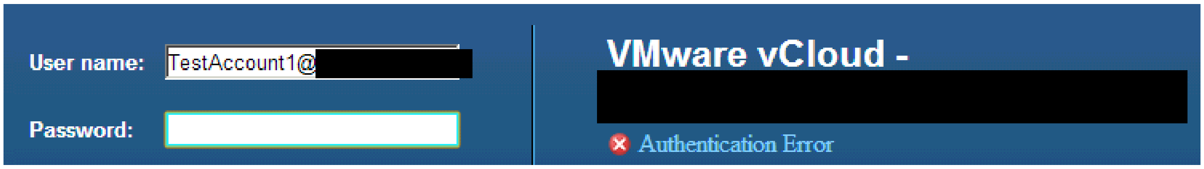
Note that TestAccount1 still displays with sAMAccountName:



BUG - Note that display with sAMAccountName

Name	1 ▲	Full Name	Ena...	Lo...	
testaccount1		Test Account 1	✓		LDAP
testaccount2@[redacted]		Test Account 2	✓		LDAP

TestAccount1 cannot login with UPN:

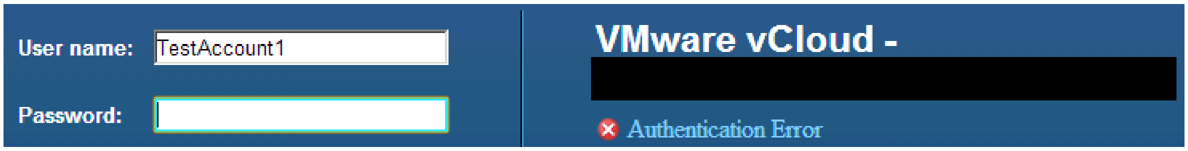


User name:	TestAccount1@[redacted]
Password:	

VMware vCloud - [redacted]

Authentication Error

Nor with sAMAccountName:



User name:	TestAccount1
Password:	

VMware vCloud - [redacted]

Authentication Error