Feature Brief: vCenter Federated Login for VMware Cloud on AWS

VMware General

Table of contents

Feature Brief: vCenter Federated Login for VMware Cloud on AWS

Introduction

We introduced a new feature that enhances the user experience and simplifies identity management by providing a unified Single Sign-On (SSO) mechanism between VMware Cloud Services and the VMware Cloud on AWS SDDC vCenter Server. Using this functionality, users that have enabled Enterprise Federation with VMware Cloud Services can securely authenticate to their SDDC vCenter Server with the same credentials used to login to the VMware Cloud on AWS Console. This is accomplished by replacing AD over LDAP identity sources with the identity providers federated with the customer's VMware Cloud Services organization. This can improve the SDDC vCenter Server security by allowing a user to integrate with an identity provider that supports Multi-Factor Authentication (MFA) via a SAML 2.0-based provider.

Previously, despite the ability to federate corporate identities to the VMware Cloud console, users still had to independently configure their Active Directories (ADs) directly to the SDDC vCenter Server, resulting in separate logins to vCenter even if they accessed the VMware Cloud console using the same underlying identity provider. This setup became particularly cumbersome once one is managing several SDDC vCenter Servers, causing inconvenience and complexity. vCenter Federated Login addresses this problem for customers and as a result, improves the user experience, user productivity and enhances the security posture for our customers.

Prerequisites and Assumptions

To get started with this feature, the following pre-requisites must be met:

- The minimum SDDC version must be 1.22
- Enterprise Federation must be enabled for ALL domains that require SDDC vCenter Server Access. This means access to VMware Cloud services is authenticated through a corporate account. Contact VMware Support if you are unsure which domains are federated with your VMware Cloud Services organization.
- Your Identity Provider (IdP) must be linked to your VMware Cloud Services organization via the “Domains Linked to Identity Provider” Org setting.

Please note that we do not currently support the simultaneous use of SSO and AD/LDAP identity sources. If multiple domains are configured in your SDDC vCenter Server and they require continued access to SDDC vCenter Server post federation, then all domains that need access to SDDC vCenter Server must go through the Enterprise Federation process.

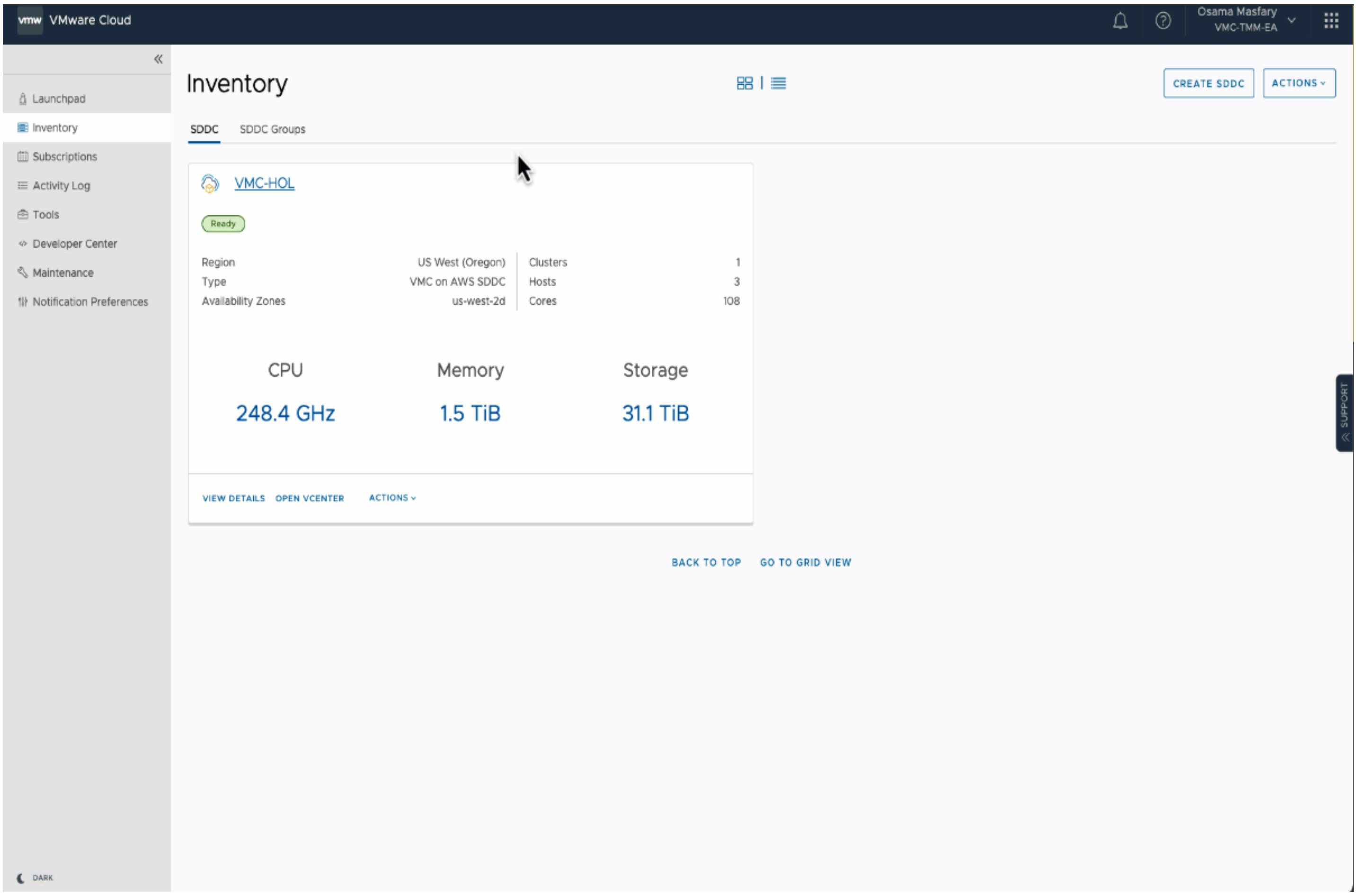
How it Works

Federated login to the SDDC vCenter Server utilizes VMware Cloud backend services and automated workflows to seamlessly transition the vCenter’s identity provider from using Native LDAP or AD-over-LDAP based identity sources to an SSO federation with your VMware Cloud Services organization. Once enabled, the customer’s SDDC vCenter Server based federation uses the industry standard protocol OAuth 2.0 to retrieve the necessary entities from VMware Cloud Services. This automates the entire identity provider configuration process in the SDDC vCenter Server such that the Admin only needs to make a one-step selection to either enable federation on the SDDC or not. Configuring SSO has never been easier!

However, before enabling the feature, it is important to carefully review the warnings once prompted. If you are uncertain whether all your domains, necessary for vCenter access, are properly configured for Enterprise Federation, it is advisable to cancel the prompt and seek assistance from VMware support. Furthermore, it is recommended to save the current Native LDAP or AD-over-LDAP identity source configuration information before enabling federation.

Enabling vCenter Federated Login

To enable the federated login functionality in your SDDC, begin by logging into the VMware Console with a VMware Cloud on AWS Administrator role. Select an SDDC from the Inventory, click on the SDDC Settings tab, and navigate to the vCenter Information section where you will find the Federated Login option. Simply click on Enable to deploy the feature.



Inventory

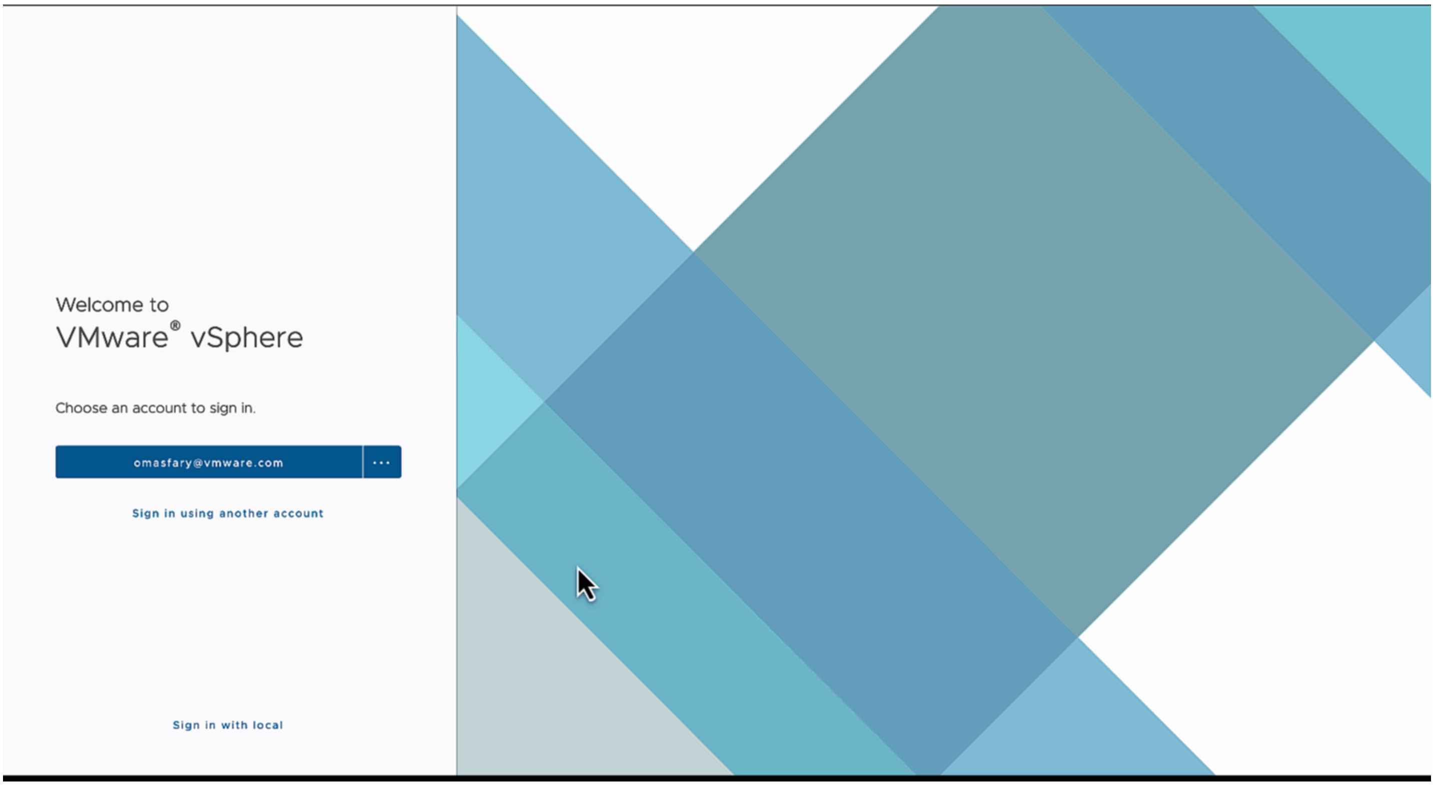
VMC-HOL

Region	US West (Oregon)	Clusters	1
Type	VMC on AWS SDDC	Hosts	3
Availability Zones	us-west-2d	Cores	108

CPU	Memory	Storage
248.4 GHz	1.5 TiB	31.1 TiB

Once the SDDC is enabled with Federated Login, the service will retrieve and push the necessary federation data such as IDP domains, the VMware Cloud Services OAuth2 endpoints, and VMware Cloud Services OAuth2 credentials to the deployed SDDC vCenter Server. All the SDDC vCenter Server external identity providers are then replaced with the identity providers federated with your VMware Cloud Services organization. Switching identity providers alters the authentication process (AuthN) while leaving the authorization (AuthZ) permissions such as global permissions and vCenter object-level permissions consistent across providers. This means that user's AD-based logins should continue to work and the transition to federation should be seamless. For example, if the identity source (acme.com) configured over AD over LDAP is replaced with an identity source (acme.com) configured over SSO, the permissions for users such as user1@acme.com remain unaffected and intact.

Additionally, it's worth noting that no new users or groups will be granted to your vCenter due to this change. Therefore, if a user or group lack the necessary permissions on any federated vCenter Server systems, attempting to access vCenter either directly or via the VMware Cloud console will result in the error message "Unable to login because you do not have permission on any vCenter Server systems connected to this client.". Additionally, this is also the type of error one would get if a user enables federation on an SDDC that has not been previously configured with an external identity source ("Greenfield SDDC").



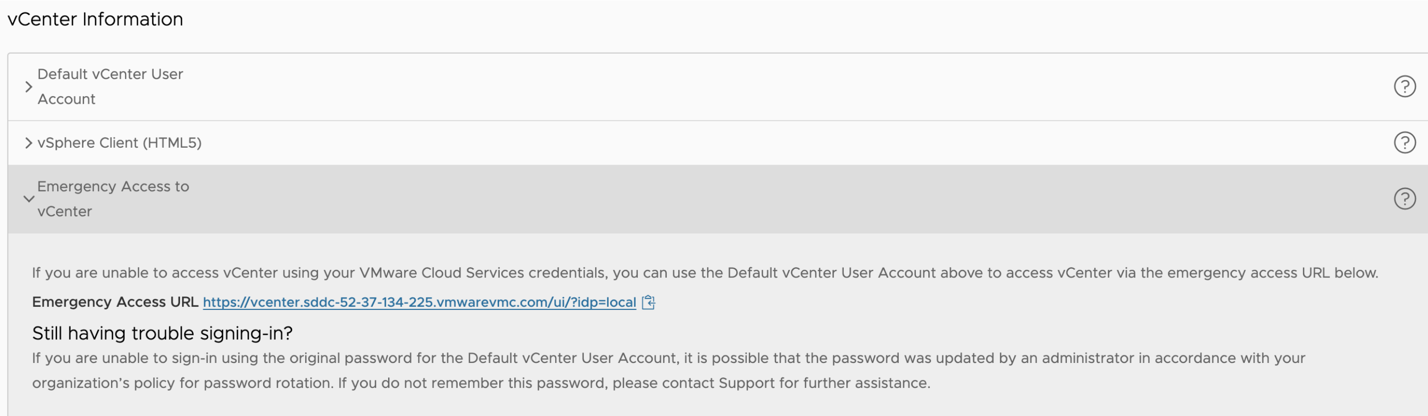
Welcome to
VMware® vSphere

Choose an account to sign in.

Emergency Access to vCenter

As a result of enabling federation, you will observe several UI changes within the Settings tab of the SDDC. The vCenter Information introduces the "Emergency Access to vCenter" URL, which acts as a break-glass procedure, allowing you to access vCenter via the cloudadmin@vmc.local.

This mechanism is intended to allow emergency access to cloud vCenters when the external identity source is inaccessible or unavailable (e.g., the AD servers go down). Nonetheless, this feature is best suited to address run-time environmental issues that occur temporarily and require immediate access to vCenter to perform a known action.



vCenter Information

If you are unable to access vCenter using your VMware Cloud Services credentials, you can use the Default vCenter User Account above to access vCenter via the emergency access URL below.

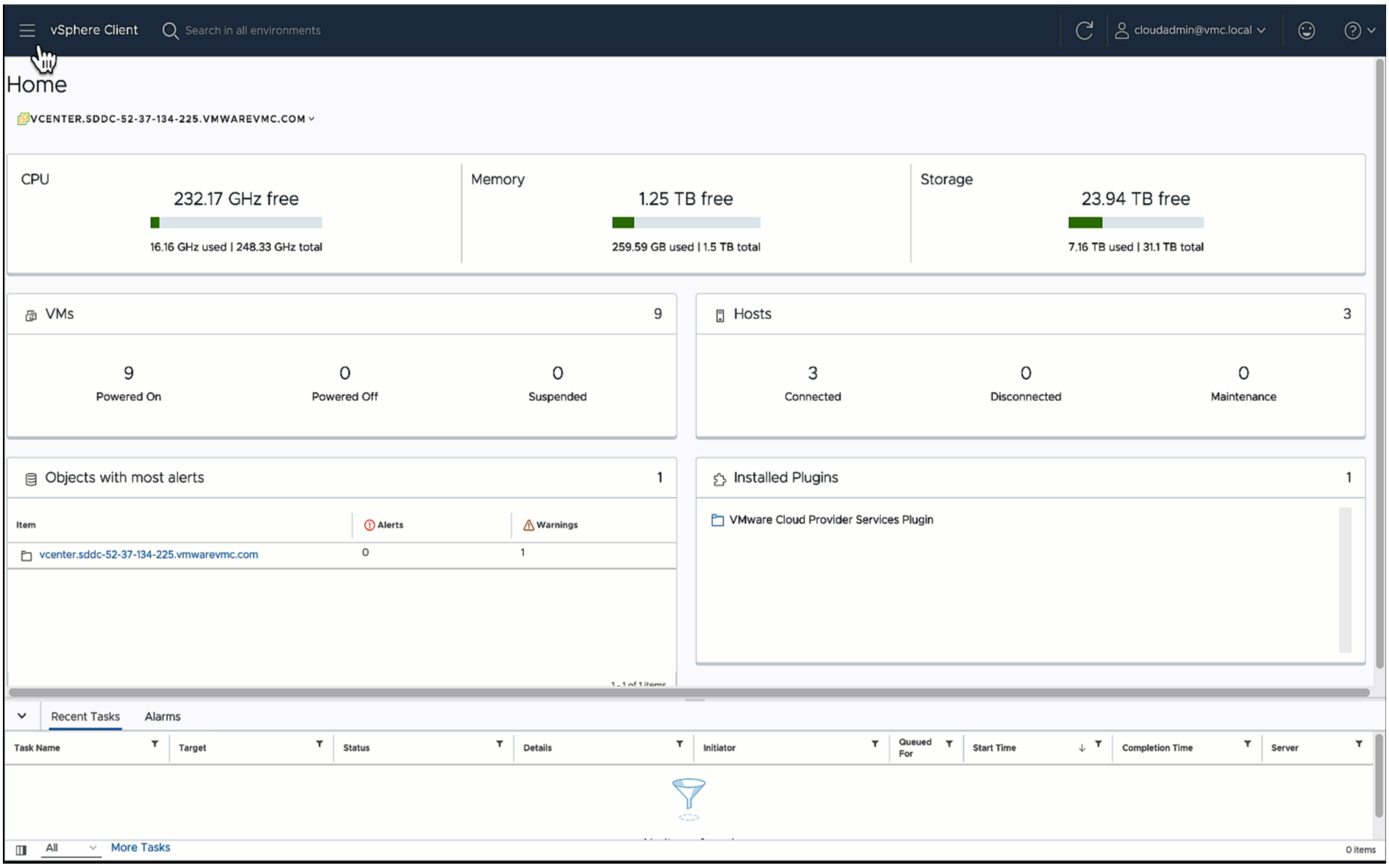
Emergency Access URL https://vcenter.sddc-52-37-134-225.vmwarevmc.com/ui/?idp=local

Still having trouble signing-in?

If you are unable to sign-in using the original password for the Default vCenter User Account, it is possible that the password was updated by an administrator in accordance with your organization's policy for password rotation. If you do not remember this password, please contact Support for further assistance.

The Federated Model

Once logged into the federated vCenter Server, the customer can now search in permissions dialogues for any users or groups in those federated trusted domains, assign roles and permissions to users/groups from the external IDP globally or at the object level for the same functionality as the user did with the previously configured LDAP identity sources.



Home

VCENTER.SDDC-52-37-134-225.VMWAREVMC.COM

CPU
232.17 GHz free
16.16 GHz used | 248.33 GHz total

Memory
1.25 TB free
259.59 GB used | 1.5 TB total

Storage
23.94 TB free
7.16 TB used | 31.1 TB total

VMs 9

9	0	0
Powered On	Powered Off	Suspended

Hosts 3

3	0	0
Connected	Disconnected	Maintenance

Objects with most alerts 1

Item	Alerts	Warnings
vcenter.sddc-52-37-134-225.vmwarevmc.com	0	1

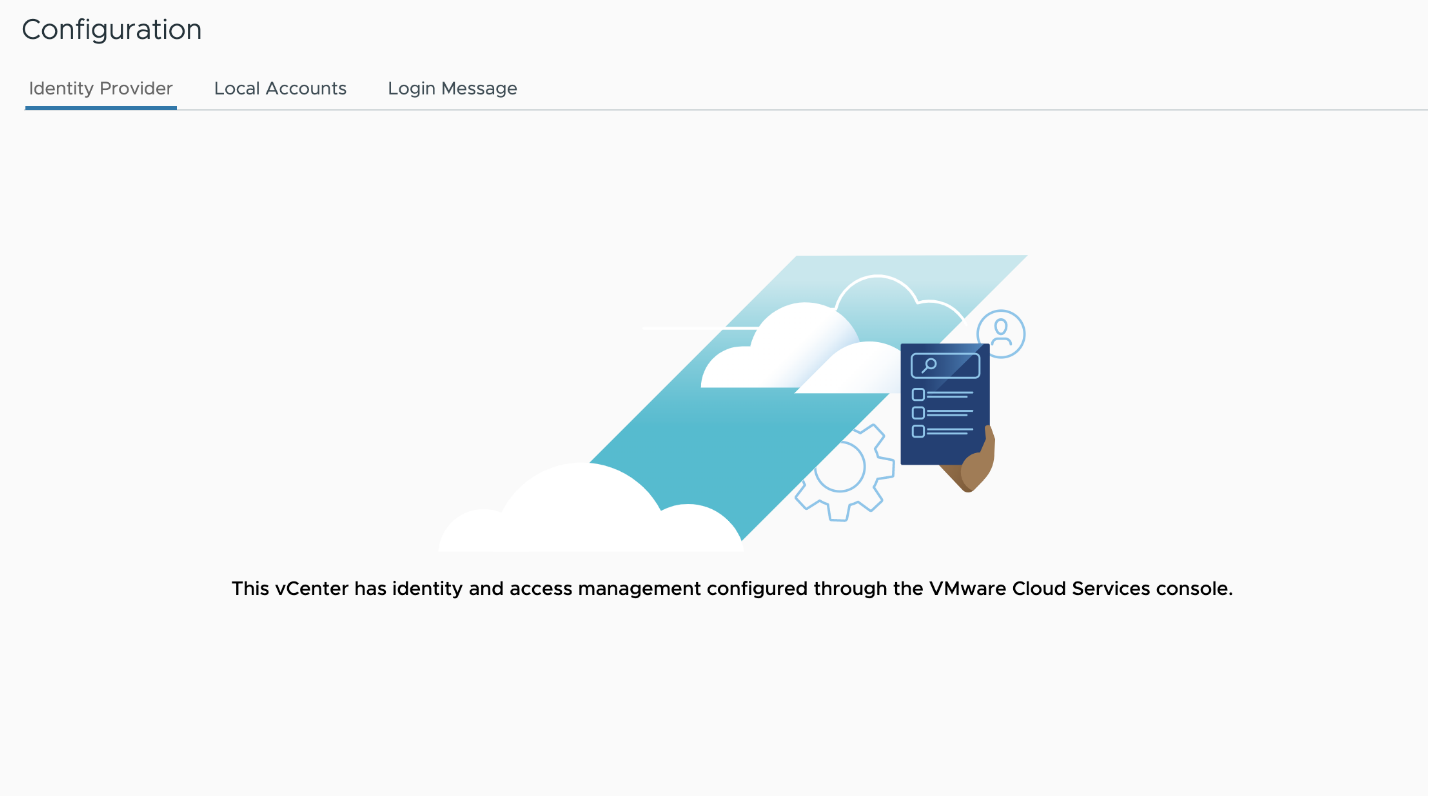
1 - 1 of 1 items

Installed Plugins 1

VMware Cloud Provider Services Plugin

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server

It’s important to note that once the SDDC vCenter moves to the federated model, users cannot change the vCenter Identity Provider configuration tab within vCenter. Here, you will encounter a notification declaring “This vCenter has identity and access management configured through the VMware Cloud Services console”. This indicates that, upon enabling the feature, vCenter's Single Sign-On (SSO) will be exclusively managed by VMware Cloud Services.



Configuration

This vCenter has identity and access management configured through the VMware Cloud Services console.

Disabling vCenter Federated Login

While we do not expect customers to disable vCenter Federated Login, there are a couple of scenarios where customers may need to disable federation. The first use-case is when a service account cannot be exempted from a SAML2.0 IDP’s 2FA or non-password-based authentication requirement. The second scenario is when users from another domain need to have federated access to vCenter. In this case, the customer would disable federation, set up Enterprise Federation for that new domain, and then re-enable federation. This process updates vCenter, allowing the new domain to be accepted.

To disable vCenter Federated login, navigate to the SDDC settings and select the federated login option, then click on "Disable." It's important to note that disabling federation will require users to set up their AD over LDAP again. We recommend saving the source configuration when enabling federation so that it can be easily added again if needed. The permissions, however, will be retained and do not need to be reset.