Stale AD Object Cleanup

When workload VMs in a DJI Frame account are created (due to a publish or an increase in the max capacity of a test or production pool), the test or production workload VMs are added to the specified Windows Active Directory as computer objects. Each time there is a publish (for non-persistent DJI Frame accounts) or if the max capacity of a test or production pool is reduced, workload VMs are terminated. However, the corresponding AD computer objects are not automatically removed from the Windows domain. Administrators have the following options to clean up stale computer objects in their Active Directory environment.

Manual

Domain administrators can periodically run the following PowerShell scripts to identify and remove stale computer objects in their domain, where stale computer objects are defined as computer objects that have not been logged in for a defined period of time. These scripts must be run with a Windows domain user with the proper Windows domain privileges to query the domain controller for the first PowerShell script and to delete computer objects from the domain for the second PowerShell script.

If the script detects any computers belonging to the Windows domain OU specified in `$OU` that have not logged into the domain for "x" days as defined by the variable `$DaysInactive`, the computer object will be listed.

```
#Set OU and inactive days interval to match your organization requirements
$DaysInactive = 60
$OU = "OU=FRAME-AWS-QA-TEST-2,OU=VDI,OU=Computers,OU=Frame,DC=frame,DC=demo"

#Search for inactive computer objects and show results in a powershell table
$Time = (Get-Date).Adddays(-($DaysInactive))
Get-ADComputer -Filter {LastLogonTimeStamp -lt $time} -Properties LastLogonDate -SearchBase
$OU | Ft Name,DistinguishedName,LastLogonDate -AutoSize
```

To find the computers belonging to the Windows domain OU specified in `$OU` that have not logged into the domain for "x" days as defined by the variable `$DaysInactive` and remove them from the Windows domain, the Windows administrator can execute (or setup a scheduled task to execute):

```
#Set OU and inactive days interval to match your organization requirements
$DaysInactive = 60
$OU = "OU=FRAME-AWS-QA-TEST-2,OU=VDI,OU=Computers,OU=Frame,DC=frame,DC=demo"

#Search for inactive computer objects and delete them (confirmation needed)
$Time = (Get-Date).Adddays(-($DaysInactive))
Get-ADComputer -Filter {LastLogonTimeStamp -lt $time} -Properties LastLogonDate -SearchBase
$OU | Remove-ADComputer -confirm:$false
```

Automatic

Frame provides a feature for automatically deleting the Active Directory (AD) computer object associated with a **terminated** Frame instance. When the feature is enabled, AD computer objects will be marked for deletion when an instance is terminated because of:

1. A Publish,
2. the reduction of the Max Default Capacity of an instance pool, or
3. the termination of a domain-joined persistent desktop or non-persistent VM under Status or via Frame Admin API.

Every 30 minutes, Frame Platform will determine the list of terminated Frame instances whose AD computer objects have not yet been deleted. Frame will then transmit the AD computer object list to one or more powered-on, domain-joined instances are in **Running** status (not in use by a user). The available instances will then contact the Windows domain controller to delete the AD computer objects. If domain-joined instances are not available to handle these requests, then Frame Platform will wait 30 minutes to try again.

Since customer administrators must manually configure Sandbox and Utility Servers to be joined to a Windows domain (if desired), customer administrators are responsible for removing these AD computer objects themselves.

Prerequisites

- This automatic AD object cleanup feature applies only to non-persistent, domain-joined Frame accounts.
- The workload VMs must be running **Frame Server 8.7 or greater** for this AD computer object deletion feature.
- The service account specified within Account Dashboard > Settings > Domain Settings must have permissions to delete computer objects within the specified domain as mentioned in **step 10** of the Domain Controller Prep document.

Known Limitation

This feature requires **at least one AD domain-joined instance** to be powered on and not in a Frame session within the Account in order to execute the computer object deletion. As a result, this feature is not triggered during the Account Termination process, in scenarios where the Max Instances setting is set to 0 across all available Instance Pools, or when all domain-joined instances are being used by users.

Enable/Disable Automatic Removal of AD Computer Objects

This feature is automatically enabled for all new domain-joined accounts created after May 4, 2023.

If you wish to enable this feature on an older account or disable it, simply navigate to the **Account Dashboard** where the domain is configured. From there, navigate to **Settings > Domain Settings** and enable/disable the toggle, as shown below:

image.png

Revision #5
Created 1 October 2025 04:51:40
Updated 14 January 2026 05:30:15 by Nikola Savic