How to join an AWS Windows instance to Cornell AD

Prerequisites

Prior to being able to join an AWS Windows instance to Cornell AD you must verify two things:

1. The subnet(s) where you wish to run domain-joined instance must use CIDR blocks officially allocated to you from the Cornell private network.
2. Your VPC is connected to the private Cornell network using Direct Connect. (See Cornell AWS Direct Connect.)

If your AWS account onboarding included Direct Connect, then you should meet both requirements already. The subnet requirement is there to ensure that there are no IP address conflicts and that all hosts are properly registered. The Direct Connect access allows communication to the VPC where IDM has built domain controllers at AWS.

Join At Launch

Unfortunately, you cannot use the AWS-provided "Domain join directory" option at instance creation to join a non-default OU. The default OU used for joining PCs, "Computers", is restricted at Cornell.

Join After Launch

At its most basic, after fulfilling the two prerequisites above, you can use the GUI within the Windows instance to manually join Cornell AD following the normal process you would use on campus. IDM has written instructions available here (https://it.cornell.edu/cornellad/join-windows-computer-cornellad-domain). One thing to keep in mind is that since AWS instances do not conform to Cornell AD's naming convention you will need to rename the instance prior to domain joining. You could also use PowerShell to script the computer object creation, the instance rename, and the domain join.