Move to Fully Remote

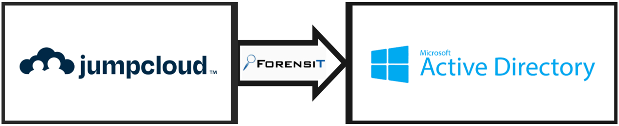
Phase 1: Jump Cloud to Active Directory

PROBLEM: Logins to remote sessions do not have password policy.

SOLUTION: Leverage existing JumpCloud that controls computer accounts to sync passwords to existing Active Directory that controls remote login to create single password solution.

PROBLEM: End users might have data outside of remote sessions on local PCs.

SOLUTION: Use ForensiT tool to migrate JumpCloud profiles to the AD Domain profile. This will ensure any important data stored locally on PC will be accessible.



EXECUTION:

- WEEK 1: Test JumpCloud sync and ForensiT profile migration DONE
- WEEK 2: Test with 5 End Users and evaluate End User experience, successes, and pain points
- WEEK 3: Communicate with End Users with information and instructions; Ashish finalize script
- WEEK 4: Cutover - Sync remaining user accounts and use automation to migrate profile

RESULT: Unified login for computer and remote sessions and the ability to enforce policies on the local machines and server

Phase 2: Data Migration

PROBLEM: Migrate any local data to the server storage with minimal End User impact

SOLUTION: Once computer logins are converted to AD domain logins, we will use automations in Ninja to migrate data in the userprofile behind the scenes. \\share.ritemgmt.co\Files\U

EXECUTION:

- WEEK 1: Create the Ninja automation and test data migration with a test user account
- WEEK 2: Test with a group of 5 end users to evaluate end user experience
- WEEK 3: Communicate with End Users with information and instructions
- WEEK 4: Enable policy to allow data transfers to commence when logging in

RESULT: Unified remote and computer login with important data transferred to remote server. Entire workload shifted to remote session only.

NOTE We will be maintaining JumpCloud temporarily for laptops that rarely see the office. Our next plan is to find a solution for those laptops.