The Ansible playbook, question2\_remediation.yml, was developed to remediate the target compliance issues. Code was extracted from the [ansible-lockdown](https://github.com/ansible-lockdown/Windows-2019-CIS) repository on GitHub and simplified to meet the requirements listed in the scenario. Ansible-lockdown, when deployed in full, provides a more robust mechanism for remediating servers for CIS compliance. The remediation presented here targets just the specified issues to provide a quick, effective solution without implementing the more complex solution in its entirety.

It is recommended that these remediation steps be implemented into the baseline Ansible playbooks/roles used to deploy new Windows 2019 servers going forward.

A note of caution: CIS Benchmark item 2.2.21 prevents local accounts from connecting remotely to the server. This may impact services if the accounts used to run services are local and not domain joined.

**Remediation:**

ansible-playbook question2\_remediation.yml -e host\_name=TARGET [--tags rule\_18.9.45.4.1.2 | rule\_2.2.21 ]

TARGET: The Windows 2019 host needing remediation. This should be an existing host or host group in Ansible inventory.