### ENT#4027 웹 서버 TLS 취약점 제거

* TLS 1, TLS 1.1의 기본 상태가 비활성화로 변경되었습니다. TLS 1, TLS 1.2를 사용하려면 부팅 옵션에 -Daraqne.rpc.weak\_tls=enabled를 추가하십시오.
* TLS 1.2에서 CBC 암호화, DH 슈트가 포함된 TLS 암호화 슈트의 기본 상태가 비활성화로 변경되었습니다. CBC 암호화, DH 슈트가 포함된 TLS 암호화 슈트를 사용하려면 부팅 옵션에 -Daraqne.rpc.weak\_cipher=enabled를 추가하십시오.
* TLS 접속 시 2048 비트 이상의 DH 그룹으로 강제하여 LOGJAM([CVE-2015-4000](https://github.com/advisories/GHSA-v98w-p8f7-9qqf)) 취약점을 해결했습니다.
* TLS 접속 시 CBC 암호화를 금지하여 LUCKY13([CVE-2013-0169](https://github.com/advisories/GHSA-pg96-42c4-p633)) 취약점을 해결했습니다.