



ONTAP Tools 10: Update Secure Cipher Suites for OTV Gateway

https://kb.netapp.com/data-mgmt/OTV/VSC_Kbs/ONTAP_Tools_10%3A_Update_Secure_Cipher_Suit...

Updated: Sun, 05 Apr 2026 20:31:05 GMT

Applies to

- ONTAP Tools for VMware vSphere (OTV) 10.5 only

Description

Note: There is a [script](#) available that will perform the steps outlined in the procedure.

This KB describes how to harden the Gateway TLS configuration by removing legacy Diffie-Hellman (DHE) cipher suites from the Gateway NGINX configuration.

This change removes the following TLS 1.2 cipher suites from the Gateway listener (example: 8443):

- `DHE-RSA-AES256-GCM-SHA384`

- `DHE-RSA-AES128-GCM-SHA256`

Impact / Downtime

- No pod restart required; typically no downtime.

Prerequisites

- Kubernetes access with permissions to:
 - View pods/configmaps
 - Edit ConfigMaps
 - Exec into pods (for reload/validation)
- Identify the following pod names:
 - Gateway pod name (example: <GATEWAY_POD>)
 - Gateway service endpoint for external validation (example: <GATEWAY_IP_OR_DNS>)

Note: Logging into the OTV10 [remote diagnostics shell](#) with the `diag` user will provide you the ability to perform the tasks outlined in this article