Problem: Running “kubectl get nodes” command. Getting “ connect to handshake tls/https” error

When encountering issues with kubectl get nodes and experiencing TLS handshake problems, several potential causes and solutions can be explored:

## **Potential Causes**

1. **Certificate Issues**: Ensure that the certificates used for the Kubernetes API server are valid and not expired. Check the ~/.kube/config file for the certificate-authority and client-certificate attributes[4](https://kubernetes.io/docs/tasks/debug/debug-cluster/troubleshoot-kubectl/).
2. **Network Connectivity**: Verify that there are no network connectivity issues preventing the TLS handshake. Ensure that the necessary ports (e.g., 443 for HTTPS) are open in your security groups or firewall rules[2](https://stackoverflow.com/questions/59958274/unable-to-connect-to-the-server-net-http-tls-handshake-timeout)[5](https://docs.aws.amazon.com/eks/latest/userguide/troubleshooting.html).
3. **Proxy Settings**: If you are using a proxy, ensure that it is properly configured. Sometimes, setting NO\_PROXY for specific IP addresses can resolve the issue[2](https://stackoverflow.com/questions/59958274/unable-to-connect-to-the-server-net-http-tls-handshake-timeout).
4. **System Time Synchronization**: Ensure that the system time on all nodes is synchronized. A mismatch can cause TLS handshake failures[2](https://stackoverflow.com/questions/59958274/unable-to-connect-to-the-server-net-http-tls-handshake-timeout).

## **Solutions**

## **1. Verify Certificate Expiry**

Use openssl to check the certificate expiry dates:

bash

kubectl config view --flatten --output 'jsonpath={.clusters.cluster.certificate-authority-data}' | base64 -d | openssl x509 -noout -dates

## **2. Check Network Connectivity**

Ensure that the security groups allow ingress traffic on the necessary ports (e.g., 443 for HTTPS)[2](https://stackoverflow.com/questions/59958274/unable-to-connect-to-the-server-net-http-tls-handshake-timeout)[5](https://docs.aws.amazon.com/eks/latest/userguide/troubleshooting.html).

## **3. Adjust Proxy Settings**

If using a proxy, unset it or add specific IP addresses to NO\_PROXY:

bash

unset http\_proxy  
unset https\_proxy  
unset all\_proxy  
  
*# Alternatively, add specific IPs to NO\_PROXY*  
export NO\_PROXY=$NO\_PROXY,localhost,127.0.0.1,<IP\_ADDRESS>

## **4. Synchronize System Time**

Ensure all nodes have synchronized system time. On Windows, you can use the following command:

text

w32tm /resync

On Linux:

bash

sudo ntpdate -q <ntp\_server>

## **5. Check kubeconfig File**

Your kubectl command relies on the kubeconfig file to authenticate and connect to the cluster. Ensure that the kubeconfig file points to the correct server, has the proper certificates, and includes the correct authentication details.

To check the current context in the kubeconfig file, run:

bash

kubectl config current-context

You can also check the entire config file with:

bash

kubectl config view

### **Verify the Kubernetes API Server**

Make sure the Kubernetes API server is running correctly and accessible over HTTPS. You can check this by inspecting the logs of the API server or verifying its availability.

* If you have direct access to the cluster, check the status of the API server pod(s).
* Ensure that the API server's endpoint is reachable from the machine you're trying to use kubectl on.

### **Try Debugging with Verbose Output**

You can get more detailed information about what's happening with the TLS handshake by using the -v flag in the kubectl command. This will give you more verbose output that may provide additional details about the TLS handshake issue.:

bash

kubectl get nodes -v=9

These steps should help resolve common TLS handshake issues when running kubectl get nodes.

Problem 2: Getting pull image issue from docker hub

Solution: check toml.conf file and correct the path of docker hub

Problem 3: Master server get disconnected while doing installation.

Solution: use default CPU limits and memory size.

Problem 4: Master server get disconnected while doing installation.

Solution: keepalive range – It uses first IP defined and load balancer also uses same Ip. So, IP clash happened. Due to this system is restarted. Network, subnet and segment should be same for each IP.