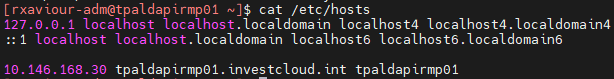
InvestCloud Apigee OPDK Installation – Issues & Resolutions

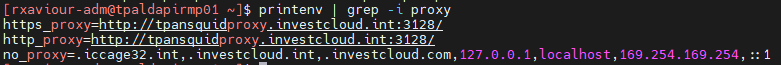
# Loopback address was being returned for hostname -i

Issue: Loopback address (127.0.0.1) was being returned for the command hostname -i. For Apigee OPDK Installation, it is a mandatory pre-requisite to have hostname -i command returning the private IP address of the node. If, the command is returning incorrect address such as loopback address, the components installed on that node might get registered with the wrong IP address. When components running on other servers attempt to connect to this component, they’ll use wrong IP address and will lead to communication failure.

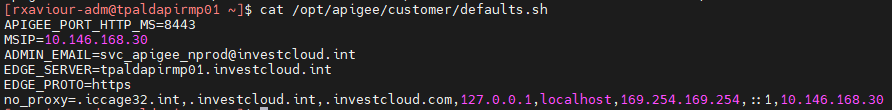
Solution: Edit */etc/hosts* file and add an entry with the private IP address of the node and hostname of the node against it. E.g.:  




# Forward proxy SHELL variables causing apigee-adminapi.sh calls to fail

Issue: It is a common practice across many organizations to set forward proxy configuration on Linux servers as shell variables. These variables are: *http\_proxy* – forward proxy to be used when invoking endpoints using HTTP protocol, *https\_proxy* – forward proxy to be used when invoking endpoints using HTTPS protocol and *no\_proxy* – list of endpoints, IP addresses when invoked, proxy configuration must be skipped. Clients such as curl, wget etc. will evaluate these configurations to decide whether to use the forward proxy to invoke the URL it is given. apigee-adminapi.sh is making use of curl internally and when management APIs are invoked, the API calls were forwarded via forward proxy. Forward proxy was not configured to route internal traffic. This was causing certain install steps to fail.  


Solution: To make sure apigee-adminapi.sh is not using forward proxy, add *no\_proxy* configuration in /opt/apigee/customer/defaults.sh and add the IP address of management server also against *no\_proxy* configuration.



# Component installation failing due to misconfigured ol8\_appstream repository

Issue: The SSL certificate required for mutual authentication with InvestCloud’s software repository was corrupted/removed as part of a server maintenance operation. Apigee component installation will work only if all configured yum repositories are accessible and packaged can be read. As the ol8\_appstream repository was not accessible, component installation was failing.

Workaround: Move the repository configuration file away from /etc/yum.repos.d or rename file with different extension to disable the repository temporarily. Fixed by renaming /etc/yum.repos.d/old8-internal.repo to /etc/yum.repos.d/old8-internal.repo.bkp.

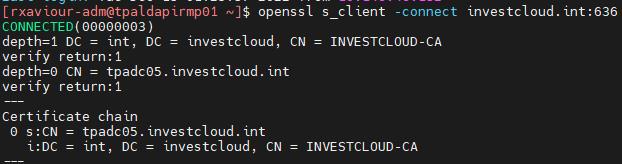
Solution: Customer system administrator fixed the issue by adding the correct set of certificate-key pair required for mutual authentication with local software repository.

# Connections to single entrance LDAP endpoint failing when using ldaps protocol

Issue: Regarding the LDAP integration, we are able to integrate using ldap protocol on port 389. But when try configuring using ldaps protocl (port 636), not working as intended. We've havde identified the cause of the issue as: Apigee is configured to use endpoint investcloud.int, and the certificate presented by the ldap server does not have CN or SAN matching the endpoint. Apigee management server built on Java is attempting to verify the certificate presented by LDAP and failing due to above mentioned mismatch.

Error on Apigee:

Caused by No subject alternative DNS name matching investcloud.int found.  
        sun.security.util.HostnameChecker.matchDNS(HostnameChecker.java:230)  
        sun.security.util.HostnameChecker.match(HostnameChecker.java:106)  
        sun.security.ssl.X509TrustManagerImpl.checkIdentity(X509TrustManagerImpl.java:461)  
        sun.security.ssl.X509TrustManagerImpl.checkIdentity(X509TrustManagerImpl.java:431)



Solution: Instead of connecting to ldaps://investcloud.int endpoint:636, configured apigee to connect to ldaps://tpadc05.investcloud.int:636. We could have connected to ldap://investcloud.int:389 for HA. But as security has precedence over availability, we’ve decided to connect to ldaps://tpadc05.investcloud.int:636 where HA is not available but the credential exchanges between Apigee and LDAP will be always secured by TLS.

# With external role mapping enabled, default organization is needed for assigning roles while a user is logging in

Issue: With external role mapping enabled, after a user is successfully authenticated, the authorization part, i.e., the role mapping is done as follows: The LDAP will be queried to find out LDAP groups the authenticated user belongs to. For each valid group, the user will be assigned with a corresponding role in Apigee. In Apigee sysadmin is the only role that is not scoped to an entire organization. All other roles are scoped to an organization. When a user with and organization scoped role is logging into the UI, the management server does not know, which organization are they logging into as there could be multiple organizations. So, this requires the ExternalRoleMapperServiceV2 to use a default valid organization when it is not sure which organization is the user is logging into. In case of non-prod environment, the default value was set to icfsm-nonprod. When the same code was re-used in production, the default value was no longer valid.

Solution: Rebuilt ExternalRoleMapperServiceV2 with icfsm-prod as the default value of organization when it is not sure yet. Now customer will have to maintain two branches of ExternalRoleMapperServiceV2 implementation: one for non-prod and another one for prod.

