Troubleshooting Techniques for Private Access Channel (PAC) Configuration in Oracle Analytics Cloud on OCI

18.08.2025, Version 1

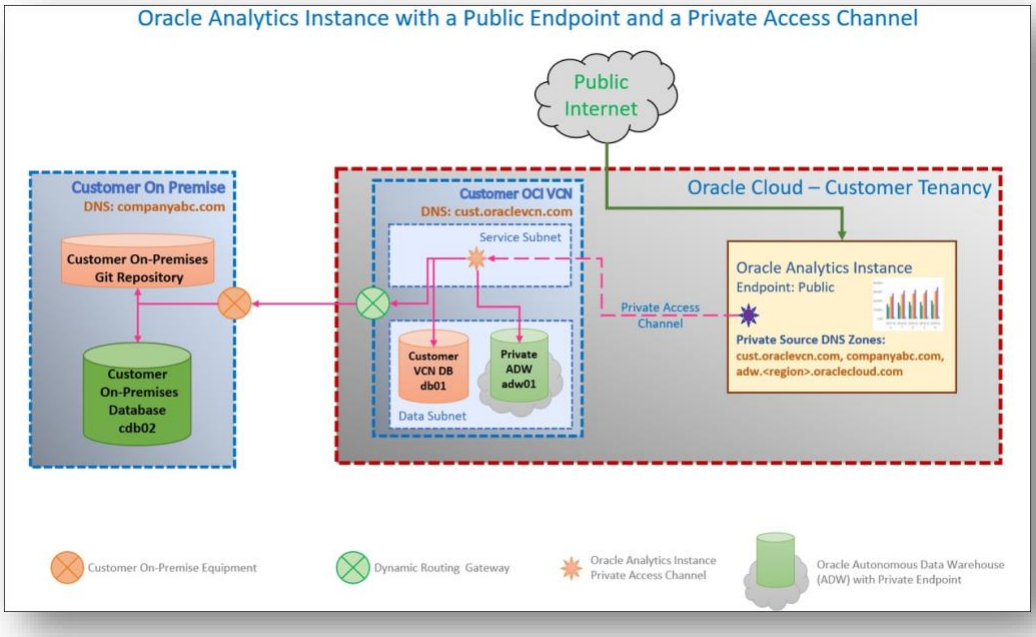
Public

Troubleshooting Techniques for Private Access Channel (PAC) Configuration in Oracle Analytics Cloud on OCI

The Private Access Channel (PAC) is a critical component for securely connecting Oracle Analytics Cloud (OAC) to private data sources within Oracle Cloud Infrastructure (OCI). While it provides a robust and secure link, configuration challenges can occasionally disrupt this connectivity. This document outlines effective troubleshooting techniques, focusing on some common possible scenarios and their diagnostic paths.

Private Access Channel for Oracle Analytics Cloud Instances with Public Endpoint

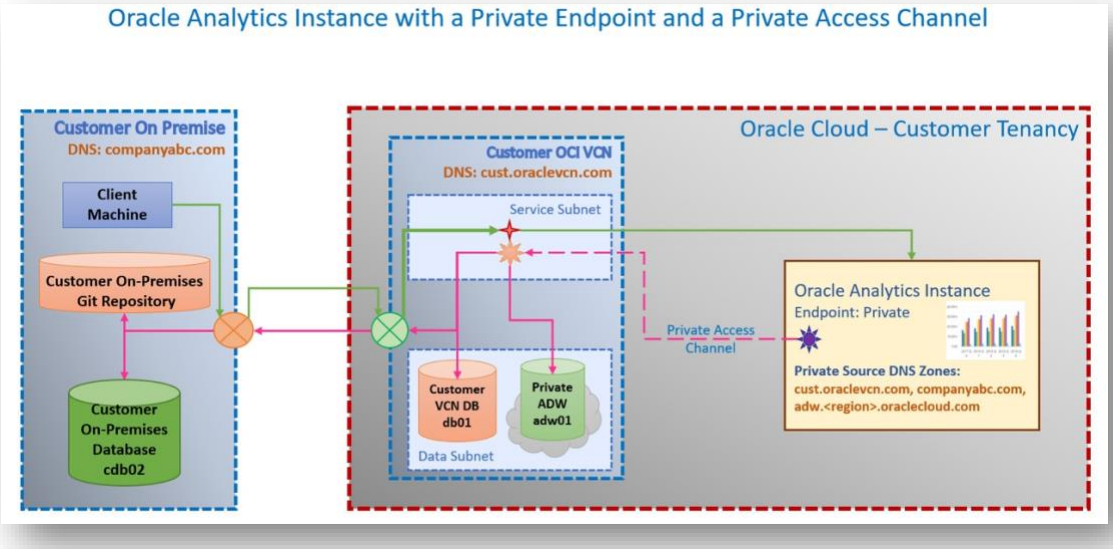
If Oracle Analytics Cloud has a public endpoint, you must specify the VCN and subnet you want the private access channel to use. If you want to restrict outgoing traffic (egress) over the private access channel, you can configure network security groups for your Oracle Analytics Cloud instance that contain one or more egress rules.



Private Access Channel for Oracle Analytics Cloud Instances with Private Endpoint

If Oracle Analytics Cloud has a private endpoint, the private access channel uses the same VCN and subnet as the private endpoint.

If you want to restrict incoming traffic (ingress) or outgoing traffic (egress) over the private access channel, you can configure network security groups for your Oracle Analytics Cloud instance that contain one or more ingress or egress rules.



Scenario 1: Post-Patch Connectivity Failure

A prime example of a PAC configuration issue is the connectivity failure experienced post new patch release. The patch disrupted the previously functional connection between OAC instance and the private Autonomous Data Warehouse (ADW).

- To diagnose this issue, a systematic approach can be initiated. The first test would involve attempting to configure a new connection using an existing OAC instance in a separate Virtual Cloud Network (VCN).
- This effort failed, but for a new reason: a lack of available IP addresses within the subnet, which prevented the PAC from being configured.
- This finding is a crucial initial diagnostic step, as it ruled out an OAC service-wide issue and pointed toward environment-specific problems.
- Following this, a new OAC instance is provisioned with a fresh PAC in an alternative VCN and a new private subnet. This new setup successfully established the required connectivity.
- This successful test confirmed that the problem is not a systemic product defect introduced by the patch. Instead, the root cause is localized to a misconfiguration within the original VCN or a conflict within the post-patch environment.

The successful test provided a clear path forward: to focus on rectifying the configuration of the original environment.

Scenario 2: Incorrect Network Security Rules

Another common cause of PAC connectivity failure is a misconfigured Network Security Group (NSG) or Security List. For the OAC Private Access Channel to function, it must have ingress and egress rules that permit traffic between the OAC instance and the data source, such as an Autonomous Data Warehouse (ADW).

When troubleshooting, it is essential to inspect the security rules associated with both the OAC and the ADW's private endpoints. Specifically, you must ensure that there are:

- An ingress rule in the ADW's NSG/Security List that allows traffic from the OAC's VCN CIDR block.
- An egress rule in the OAC's NSG/Security List that allows traffic to the ADW's VCN CIDR block and the specific port used by the database (typically 1521 for ADW).
- Correct stateful vs. stateless configurations. For stateful rules, the return traffic is automatically handled, but for stateless, a corresponding ingress or egress rule is required for the return path.

Any missing or improperly configured rule will act as a firewall, silently blocking the connection.

Scenario 3: DNS Resolution Issues

For the PAC to connect to a data source using a private endpoint, the OAC instance must be able to resolve the data source's private hostname to its correct IP address. This depends entirely on the VCN’s DNS configuration.

If the OAC instance cannot connect to a data source via its private endpoint, a critical troubleshooting step is to verify DNS resolution. You can check the VCN's DNS settings to ensure that a DNS resolver is in place and that the private zone for the ADW is correctly configured. This can involve using a VCN-specific DNS resolver or a private DNS zone. If the VCN is not configured to resolve the private hostname, the connection attempt will fail.

A good way to test this is to launch a compute instance in the same private subnet as the OAC PAC and attempt to perform a simple DNS lookup or a telnet to the data source’s private endpoint and port. A successful test indicates that the issue is likely elsewhere, while a failure points directly to a DNS problem.

Conclusion

Troubleshooting PAC configuration requires a methodical and structured approach. The initial step is always to isolate the problem by eliminating external factors, such as systemic product defects, through controlled testing. Once the issue is confirmed to be localized to the environment, the focus shifts to a systematic review of the network and security configurations. By checking for common issues like incorrect network security rules or DNS resolution failures, you can effectively diagnose and resolve connectivity issues to restore seamless OAC–ADW connectivity.

Documentation

- https://docs.oracle.com/en/cloud/paas/analytics-cloud/acsds/connect-premises-data-sources-private-access-channel.html
- https://docs.oracle.com/en-us/iaas/analytics-cloud/doc/private-access-channels.html