Oracle® SD-WAN Private Registration Server

Installation and Upgrade Guide

Original Publication Date: Nov 1, 2019

Table of Contents

About This Document 3
Audience 4
References 4
Overview 4
Prerequisites 5
Network Deployment Options 5
Option 1: Deploy to Private LAN 5
Option 2: Deploy to Public Internet 5
Private Registration Server Packet Flow 5
Private Registration Server Deployment 7
Option 1: Deploy to Private LAN 7
Option 2: Deploy to Public Internet 9
SSL Certificates 11
Talari Configuration 12
Troubleshooting 12
Private Registration Server Command Line Tools 13
Appendix A: Easy 1st Install 13
Easy 1st Install Site Deployment Criteria 13
Use NCN to Upload Client Package to Registration Server 14
Deploy the Talari Appliance 14

About This Document

This document discusses the deployment and configuration a private Talari registration server for the Easy 1st Install process.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
    - For technical issues such as creating a new Service Request (SR), select 1.
    - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations

- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click Industries.
3. Click the Oracle Communications link.

   Under the SD-WAN header, select a product.
4. Select the Release Number.

   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.

References

The following documents are available:

APN 7.3 GA New Features Guide

Overview

The Talari Private Registration Server offers customers the ability to host an independent registration server for use in the Easy 1st Install process. The private registration server may be deployed for access via a company intranet or for access via the public internet, and using either a static IP host or a DNS-resolvable Fully Qualified Domain Name (FQDN).

- Only one private registration server with one ethernet interface is supported per APN.

- All configuration packages expire seven days after being uploaded to the registration server. The Talari Private Registration server is supported with APN 7.3 P3 or above.

Prerequisites

- Talari Private Registration Server installation package
- Ubuntu 16.04 server with the following specifications:
  - 4 CPUs ○ 4 GB RAM ○ 100 GB storage ○ 1 Ethernet interface
  - ○ *OPTIONAL:* Certificate signed by trusted Certificate Authority (see SSL Certificates section)

Note: It is recommended that the Ubuntu server is dedicated solely to serving the Talari Private Registration server.

Network Deployment Options

Option 1: Deploy to Private LAN

Description: Deploy the private registration server for access via incumbent private intranet, using either an IP host or a Fully Qualified Domain Name.

Option 2: Deploy to Public Internet

Description: Deploy the private registration server for access via the public Internet, using either an IP host or a Fully-Qualified Domain Name.

All deployment options require minor configuration changes to the Talari appliances for the feature to function as intended. Please see the **Talari Configuration** section of this document for information on the required configuration steps.

Private Registration Server Packet Flow

Once the Private Registration Server (PRS) is installed and operational, the high-level data flow for the Easy 1st Install process to complete properly is as follows:

- User provides the serial number for the site being deployed to the NCN
- The NCN uploads package to the PRS ○ Connectivity must exist to the PRS from the NCN management port IP ○ The NCN pushes the client package to the PRS via HTTPS

- Once the client appliance is powered on and has an IP address/gateway/DNS for the management port, the following occurs:
  - The client will attempt to establish an HTTPS session via its management port to the PRS and provide its serial number
    - Once the serial number is validated via the HTTPS session, the PRS will provide a URL for the client to download the appliance package
  - The client appliance will establish a second HTTPS session to retrieve the appliance package based on the validated serial number

For more detailed information on the Easy 1st Install process, please see Appendix A.

Private Registration Server Deployment

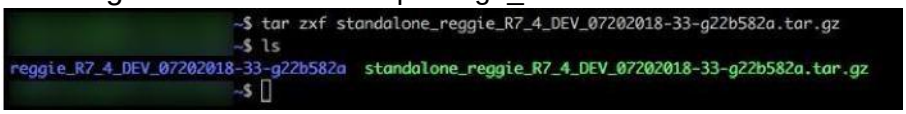
Option 1: Deploy to Private LAN

Deploy the Private Registration Server:

Step 1. Download the Private Registration Server installation package\\

Step 2. Copy the installation package to the Ubuntu 16.04 server.

Step 3. Unpack the Private Registration Server installation package using the following command: tar zxf <package_name>



Step 4. Run the install script located in the /<package_name>/install directory. Please note that the installation script must be installed using sudo or run as the root user: sudo ./install.sh

The installation script will automatically download any necessary dependencies and configure all required components.

Step 5. Deployment of the Private Registration Server is complete.

Installation may be verified by running the reggie.pl script located in the /<package_name>/tools directory with the -h option. If the installation has completed successfully, the script will run and display a list of options for the script. For more details about these options, please see the Troublshooting section.

Option 2: Deploy to Public Internet

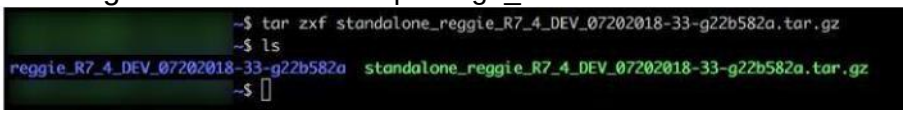
When deploying the private registration server for access via the public Internet, port forwarding must be configured on the site firewall to permit incoming traffic to the registration server from client appliances.

Deploy the Private Registration Server:

Step 1. Download the Private Registration Server installation package

Step 2. Copy the installation package to the Ubuntu 16.04 server.

Step 3. Unpack the Private Registration Server installation package using the following command: tar zxf <package_name>



Step 4. Run the install script located in the /<package_name>/install directory. Please note that the installation script must be installed using sudo or run as the root user: sudo ./install.sh

The installation script will automatically download any necessary dependencies and configure all required components.

Step 5. Once installation is complete, edit /var/www/reggie/config/reggie_config.json and replace the default IP address in the basePackageUrl parameter with the public IP for the registration server.

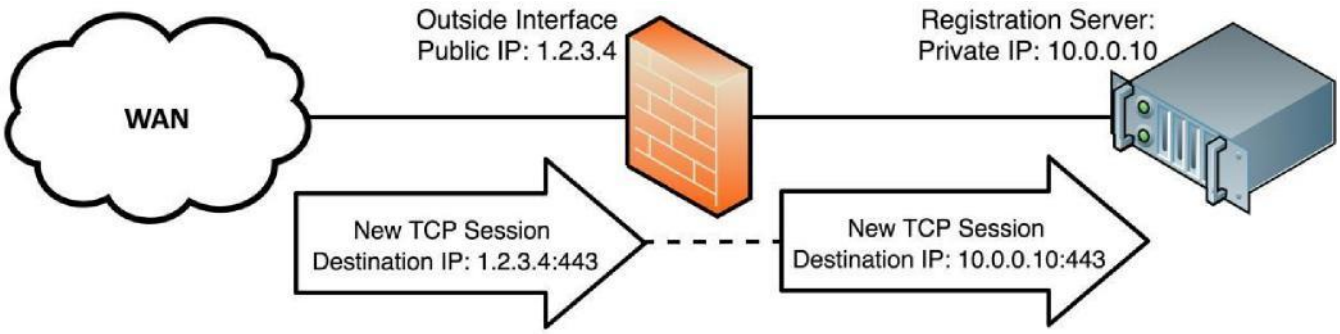
Note: If this parameter is not updated, the URL sent to Talari clients during the Easy 1st Install process will not be valid and the process will fail.

Step 6. Deployment of the Private Registration Server is complete. Installation may be verified by running the reggie.pl script located in the /<package_name>/tools directory with the -h option. If the installation has completed successfully, the script will run and display a list of options for the script. For more details about these options, please see the Troubleshooting section.

Configure the Firewall:

In order for the registration server to be accessible to APN sites via the public Internet, a port-forwarding rule must be configured to pass new traffic from Talari appliances to the server. The port-forwarding rule should pass new TCP 443 traffic to the outside interface of the firewall to port 443 on the registration server.

For example, if the outside interface of the firewall has the IP 1.2.3.4 and the IP address of the registration server is 10.0.0.10, new TCP traffic arriving on the firewall destined for 1.2.3.4:443 should be forwarded to 10.0.0.10:443.



SSL Certificates

The Talari appliances and registration server do not support SSL verification using selfsigned certificates. The deployment scenarios outlined above assume that a certificate signed by a trusted Certificate Authority is not installed on the Ubuntu server, and instruct the user to disable SSL verification accordingly. Additionally, SSL verification is only supported in conjunction with deployment using an Internet FQDN.

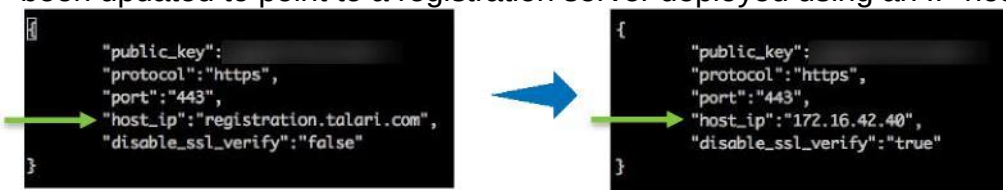
If a certificate signed by a trusted Certificate Authority is installed on the Ubuntu server and the server is being deployed using an Internet FQDN, the “disable_ssl_verify” parameter may be set as “false” to enable SSL verification.

Talari Configuration

The NCN and all appliances ship with a pre-configured file which points to the public Talari registration server. This file must be edited so that all appliances will use the private registration server.

Step 1. SSH or console into an appliance and edit /home/talariuser/reggie.cfg.

Replace the default host_ip value of "registration.talari.com" with the IP or Fully Qualified Domain Name of the private registration server and set disable_ssl_verify to "true". In the example below, the host_ip value has been updated to point to a registration server deployed using an IP host on



an incumbent private LAN:

If deploying the Private Registration Server for access via the public Internet using a host IP, the host_ip value should be replaced with the public IP address for the server.

Note: For more information about using SSL certificates with the private registration server, please see the SSL Certificates section.

Step 2. Save the changes to reggie.cfg.

Step 3. Reboot the appliance for the configuration changes to take effect. Once the reggie.cfg file has been updated and the appliance has been rebooted, the Easy 1st Install process may proceed as usual.

Note: See Appendix A for a full outline of the Easy 1st Install process.

Troubleshooting

In certain scenarios, the Easy 1st Install process may fail:

- Configuration packages expire from the registration server seven days after upload. If a site is brought up more than seven days after the configuration package is uploaded by the NCN, no configuration package will be available for download from the registration server.
  - Resolution: Upload the configuration from the NCN again.
- If the NCN and clients are not rebooted after editing the reggie.cfg file, they will continue to utilize the public Talari registration server. This issue can be confirmed by taking packet captures from the Talari appliances to determine whether they are sending traffic to the correct registration server.

- Resolution: If the appliances are sending traffic to registration.talari.com rather than the intended private registration server, confirm that the reggie.cfg file is configured as desired and reboot the appliance.

Private Registration Server Command Line Tools

The reggie.pl script included in the /<package_name>/tools directory provides tools for managing and troubleshooting the private registration server. Invoke the script with the h option to view a list of all available options.

Option	Usage
-c	Clears appliance packages from the registration server. Clears all appliance packages by default. Can be used with -s.
-s	Used in conjunction with -c to specify packages for a specific site.
-e	Purges packages more than seven days old.
-l	Lists all appliance packages held on the server.
-d	Delete an appliance package, as identified by ID (left-most column displayed by -l).
-p	Checks for duplicate serial numbers.
--diagnostics	Generates a diagnostic package to be uploaded for review by Support
-v	Displays the version of the registration server software.
-h	Displays all options for the reggie.pl script.

Appendix A: Easy 1st Install

Easy 1st Install Site Deployment Criteria

NCN:

- Easy 1st Install can be used once the Network Control Node (NCN) has been set up for your network.
- Active Appliance Package: The NCN must be running an active configuration which includes the appliance for the site being installed.

Client Site Connectivity:

- DHCP, and DNS connectivity to the management interface are required to use Easy 1st Install, and the registration server must be reachable via the management interface over either a private intranet or the public Internet. If communication with the registration server is blocked, Easy 1st Install will fail.
- Cable the LAN and WAN ports in accordance with the Talari configuration for the site.

Use NCN to Upload Client Package to Registration Server

1. Log in to the Web Console of the NCN.
2. Navigate to **Configuration > Easy Install.**
3. Locate the Site name of the appliance being deployed.
4. Click the Edit pencil to open the Set Serial Number window.
5. Enter the serial number of the appliance being deployed and click the Set Serial Number button.
6. Observe the **Upload/Activate** column. Click the **Upload/Activate** text when it appears.
7. Continue to observe the **Upload/Activate** column. Once the text reads **Upload Complete**, proceed to the next section.

Deploy the Talari Appliance

8. Cable the appliance with the provided cables.
9. Ensure that the appliance management interface is cabled for connectivity to the registration server.
10. Connect the power cord to the appliance. Connect the other end to an appropriately grounded power source. The appliance will power on automatically.
11. The appliance will begin the Easy 1st Install process. Please allow up to ten minutes for the process to complete. (From the NCN Web Console, observe the **Configuration > Easy Install** page for status updates during installation.)
12. Once the Easy 1st Install process has completed, the Talari service will automatically be enabled.