Oracle Utilities Live Energy Connect

Security Guide

F74937-06

Last Updated March 13, 2024

ORACLE

Oracle Utilities Live Energy Connect Security Guide

F74937-06

Contents

Getting Started

This security guide provides an overview of the Oracle Utilities Live Energy Connect (LEC) v8.0 security process and covers the following:

- Establishing machine-level roles and security policies limiting access to the system on which LEC is deployed
- Setting appropriate firewall rules to limit security vulnerabilities
- Specific protocol security measures

Audience

This guide is intended for system, network, and security administrators tasked with installing, configuring, and maintaining Oracle Utilities Live Energy Connect v8.0.

It covers the following topics:

- Installing system prerequisites and the Oracle Utilities Live Energy Connect v8.0 software
- Setting appropriate firewall rules to limit security vulnerabilities
- Specific protocol security measures

Prerequisites

Oracle Linux 8 (OL8) must be installed on the target host prior to installing Oracle Utilities Live Energy Connect v8.0. An additional dependency, the Oracle Cloud Native Environment (OCNE) framework, will be downloaded and installed to the host system when Oracle Utilities Live Energy Connect v8.0 self-extracting archive runs.

It is strongly recommended that the OL8 operating system be installed with a security profile such as NIST 800-171 and that OpenSCAP be used periodically to confirm security compliance for the host system. See details on using OpenSCAP with OL8.

Oracle Utilities Live Energy Connect v8.0 will typically be deployed to on-premise systems that are air-gapped, with no direct public network access. Procedures should be in place to push critical updates and patches of OL8 and OCNE to production systems in a timely fashion. For an example, see Using a Private Registry .

Protocol-Specific Considerations

The following sections are the protocol-specific considerations for Oracle Utilities Live Energy Connect (LEC) v8.0.

ICCP

The ICCP protocol (IEC 60870-6/TASE.2) is based on MMS (ISO 9506) and allows for client and server roles. ICCP and MMS allow for TCP/IP connections to be inbound, outbound, or both, irrespective of the client/server role. The default MMS IP port is 102.

By default, the LEC Server listens on localhost:102. To override this when it is required to allow an inbound connection, the following command line modification must be added (through the Extra params field in the LCM Server tab): **/listen=<interface>**. For example, **/listen=192.168.1.1**. You can specify 0.0.0.0 to listen on all local interfaces. See the Oracle Utilities Live Energy Connect Configuration Manager User Guide for more information.

MMS TCP/IP port 102 connections and traffic must be allowed between the LEC system and any configured ICCP peers, based on the connection inbound/outbound configurations.

DNP3

DNP3 (IEEE 1815) is a protocol that uses TCP/IP or UDP/IP as a transport layer. LEC Server can be configured to accept inbound connections, make outbound connections, listen for inbound UDP messages, and send outbound UDP messages.

DNP3 is an unsecured protocol that offers no encryption nor authentication, and therefore must only be enabled for use on a secure operating network. DNP3 also uses configurable IP ports. TCP/IP connections and traffic must be allowed between the Server machine and any configured DNP3 master/outstation (client/server) peers based on connection inbound/outbound configurations.

2030.5

2030.5 is a REST-based networking protocol for transmitting control messages to and status messages from aggregators and other systems important to renewable power generation. The Oracle Utilities Live Energy Connect v8.0 cluster supports a containerized implementation of a 2030.5 server. For secure operation, a NGINX web server is installed on the Oracle Utilities Live Energy Connect v8.0 host machine and configured as a HTTPS reverse proxy to the 2030.5 server running inside the Oracle Utilities Live Energy Connect v8.0 cluster. Current standards for HTTPS security, certificate key length, and other relevant standards should be followed.

General Operational Considerations

Oracle Utilities Live Energy Connect v8.0 is a microservices-based server application that is deployed in a Kubernetes cluster to host systems running Oracle Linux 8 (OL8) and Oracle Cloud Native Environment (OCNE). Upon initial installation, the Oracle Utilities Live Energy Connect v8.0 cluster runs in a default mode, with a single configuration pod and no networking pods

installed. As pods supporting network protocol interfaces are installed in the cluster, various protocol-specific IP ports will need to be opened to support interfaces to remote devices and systems.

Customer network and security policies vary, but in general it is recommended that inbound and outbound network access to and from the Oracle Utilities Live Energy Connect v8.0 cluster be limited to the specific ports required for enabled protocol functionality and be limited to specific peer IP addresses. Enforcement at the network level and the local machine firewall level is recommended.

Installing Oracle Utilities Live Energy Connect v8.0

Oracle Utilities Live Energy Connect v8.0 is distributed as a TAR archive file that must be extracted on the host prior to installation. The Oracle Utilities Live Energy Connect v8.0 distribution includes a bash script that manages the configuration of the software on the host system. The bash installation script must be run as the root user. The script will apply appropriate access controls to installed and configured components using the least privilege principle. See the Oracle Utilities Live Energy Connect v8.0 Installation Guide for more information.