



ClusterLion

for SAP HANA



Connection and Authorization Overview

ClusterLion Architecture



Table of contents

- Table of contents..... 1
- 1 Introduction 2
 - 1.1 ClusterLion Agent..... 2
 - 1.2 Configuration Portal 2
 - 1.3 Quorum Service..... 2
- 2 User Accounts 2
 - 2.1 Linux User on SAP HANA Machines..... 2
 - 2.2 Integration User (vCenter, HMC) 3
 - 2.3 SAP HANA user 3
- 3 Network Communication..... 3
 - 3.1 ClusterLion Agent ↔ SAP HANA Machine..... 4
 - 3.2 ClusterLion Agent ↔ Integration application (vCenter, HMC)..... 5
 - 3.3 ClusterLion Agent ↔ ClusterLion Configuration Portal..... 5
 - 3.4 ClusterLion Agent ↔ ClusterLion Quorum Service..... 5
 - 3.5 ClusterLion Configuration Portal ↔ ClusterLion Quorum Service 5

1 Introduction

The ClusterLion for SAP HANA solution in a virtualized environment (VMware, PowerVM) incorporates a handful of components talking to each other. This document provides an overview of the general ClusterLion architecture and detailed information about the network communication and needed user accounts of its components.

1.1 ClusterLion Agent

The ClusterLion Agents are standalone applications deployed as virtual machines which constantly monitor SAP HANA installations, whereby a single agent can handle multiple HANA instances in parallel. To gain the complete picture of the state of the database, the agents use multiple different connections to fetch all relevant metrics.

1.2 Configuration Portal

This frontend application is deployed as a virtual machine in one of the datacentres and is used to setup and configure the ClusterLion installation. The administration users can define the ClusterLion mode of operation for each SAP HANA instance separately over the web application or a REST API¹.

1.3 Quorum Service

There are various disaster scenarios a HA solution for application clusters must be able to handle. All implementations need an independent third location at which the monitoring data is analysed and a switchover decision is made in case of a detected failure. The network connection to this additional location must be trusted to be available all time. If this connection is lost, the quorum will not be able to receive any data and, in the worst case, a failure of a monitored HANA database stays undetected and no switchover will be performed.

2 User Accounts

To allow the integration into the customer environment, following user accounts must be created for the ClusterLion.

2.1 Linux User on SAP HANA Machines

The ClusterLion needs to fetch status information from the HANA database and the Linux OS on the SAP HANA machines. Therefore a dedicated Linux user with *sudo* privileges must be provided, which is used by the ClusterLion-Agents to login to these machines via SSH.

¹ [ClusterLion for SAP HANA – Integration API](#)

The Linux user needs *sudo* privileges in order to be allowed to add and remove IP addresses (Failover IP) and run CLI commands as SID admin.

2.2 Integration User (vCenter, HMC)

It is critical for the ClusterLion to know the power state of all monitored virtual instances at any time. So, the ClusterLion Agents log into the respective vCenter or HMC application with a dedicated user with minimal rights.

He must only be allowed to fetch the power status information of the to be monitored SAP HANA machines and in case of an identified disaster case he must be allowed to shutdown the primary machines of the according database instance.

2.3 SAP HANA user

To ensure working database queries, the ClusterLion Agents have a built-in HANA client. This client uses a dedicated HANA database user "clusterlion" to fetch additional health metrics from a system table.

If the SAP HANA instance is configured in a cost optimized setup (Q/DEV instances on the secondary machine), this user will also require the rights to alter the DB resources via SQL commands.

3 Network Communication

Figure 3-1 provides a detailed connection overview of how the individual ClusterLion components are interconnected. To keep the drawing more readable, the ssh and http connection between Agent 1 and the secondary HANA machine as well as the connection between Agent 2 and the primary HANA machine has been left out.

In case of a PowerVM environment, the vCenter server is replaced by one (or multiple) HMC instances.

The datacentre's internal communication uses standard protocols (e.g. ssh, http) and configurable standard ports.

The connection to the quorum service uses the MQTTS protocol which runs over TCP/IP. It is specifically designed for connections where the network bandwidth is limited and only a small amount of data must be transmitted.

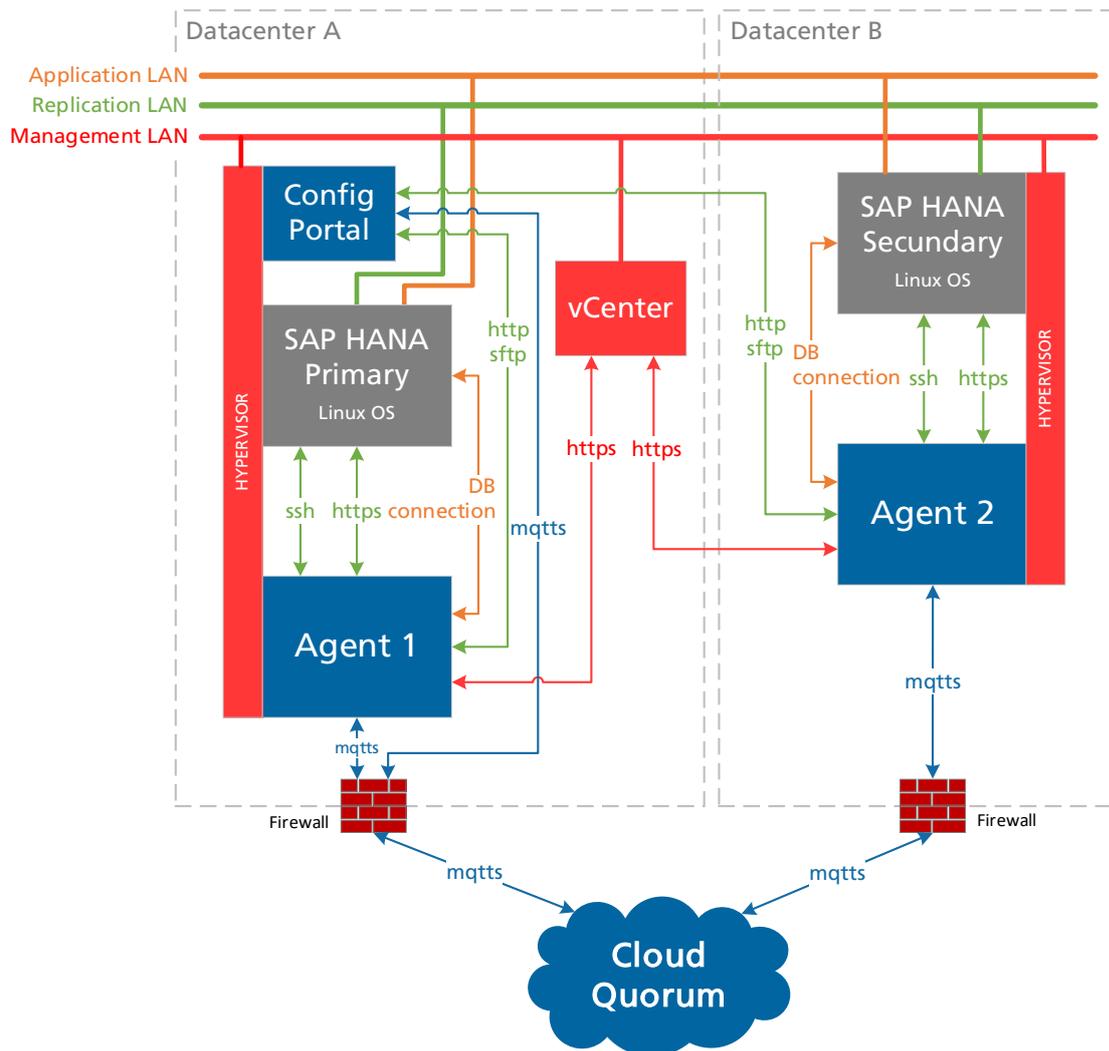


Figure 3-1: Basic ClusterLion connection schema (VMware)

3.1 ClusterLion Agent ↔ SAP HANA Machine

Most of the status information of the SAP HANA system health is queried from the SAP HANA machines by the agents via ssh connections. For this connection the replication network between the two HANA sites is used. Following metrics are fetched:

- Status of the SAP HANA System Replication
- SAP HANA Operation Mode and Replication Mode
- Status of the configured failover IP address

Additionally, the https endpoints provided by the *sapcontrol* tool are used to fetch the current status of the SAP HANA processes.

To ensure a working database connection the agents use a built-in HANA client to query monitoring information from the HANA instance. The client uses the application network as other clients would do.

3.2 ClusterLion Agent ⇔ Integration application (vCenter, HMC)

The agents retrieve the power status of the virtual machines from the integration application via its API. In case of an observed disaster case, the agent will also trigger the shutdown of the primary HANA machines of the according HANA instance over this connection.

3.3 ClusterLion Agent ⇔ ClusterLion Configuration Portal

The configuration portal application sends configuration data over encrypted (AES 256) messages to the agents and in case of software updates the software bundle file containing the new release data will be transmitted to all agents via a sftp connection.

3.4 ClusterLion Agent ⇔ ClusterLion Quorum Service

All collected information, which represents the complete health status of the SAP HANA system, is sent to the ClusterLion Quorum Service. The data to be sent is completely anonymized, encrypted (AES 256) and transmitted over an SSL secured channel by using the MQTT protocol.

The returning action triggers (payload: **0** or **1**) are received and further interpreted by the agents. An internal, hard-coded lock mechanism provides additional safety by not allowing a failover if the database is still responding to queries.

3.5 ClusterLion Configuration Portal ⇔ ClusterLion Quorum Service

The Configuration Portal uses the same communication channel as the agents to receive some basic information from the quorum service:

- Disaster rule execution status
- ClusterLion mode of operation (Operation/Maintenance/Disabled)

Since the operation modes can only be changed in the Configuration Portal by an internal user, this connection is also used to send messages containing the new operation mode information to the quorum service.

ProLion GmbH
Maierhöfen 8/3
2813 Lichtenegg
Austria
office@prolion.com

prolion.com