SAP on Google Cloud: High availability

Overview

Contents

About this document

This document is part of a series about working with SAP on Google Cloud. The series includes the following documents:

- High availability (this document)
- Migration strategies
- Backup strategies and solutions
- Disaster-recovery strategies

Introduction

The term *high availability (HA)* is used to describe an architecture that improves a system's availability. The availability of a system refers to a user's ability to connect to the system and conduct the required operations. If a user can't connect, the system is perceived as unavailable, regardless of the underlying issue. For example, a networking issue can prevent users from accessing the service, even though the system is running.

A high-availability setup interacts with multiple components of the architecture to minimize the points of failure, typically by using redundancy.

To measure a service's performance throughout the year, the metric of *percentage of uptime* is used to calculate the ratio of uptime to the aggregate of uptime and downtime. A system that is available for ~8750 hours during the 8760 hours of a year has an uptime of 99.89% (8750/8760) and a downtime of 10 hours.

Though HA setups aim to minimize the downtime for failures within a data center (such as server hardware or software failures), they do not protect against disasters that affect the entire region. To protect against regional failures, you should develop a disaster-recovery (DR) strategy.

Levels of high availability

The following sections cover various levels of a high-availability architecture for SAP landscapes and how you can set them up using Google Cloud services. The levels are as follows:

- Infrastructure
- Database setup
- Application servers

Level 1: Infrastructure

This section describes some of the mechanisms that Google Cloud offers for services relevant to SAP deployments. Though these mechanisms help to improve uptime of the infrastructure and access to the application, they may not protect against data loss during failures. These mechanisms might expose users to significant downtime periods until the virtual machine (VM) instances are back online again.

Zones and regions

Google Cloud is highly available by design, with a redundant infrastructure of data centers around the world that contain *zones* designed to be independent from each other. Zones usually have their own independent software infrastructure, power, cooling, network, and security infrastructure that are isolated from other zones. To deploy fault-tolerant applications that have high availability, we recommend deploying applications across multiple zones and multiple regions to help protect against unexpected failures of components, including a single zone or region. Depending on your business requirements, you might meet availability targets without implementing conventional on-premises safeguards against hardware, storage, and networking failures, such as redundant power supplies or disk arrays. Google Cloud takes care of the infrastructure stack and relieves you of this responsibility, which can save you both time and money.

Deploy nodes of an HA cluster across two or more Compute Engine zones within the same region. This deployment ensures that they are on different physical machines and protects against zonal failure.

Keep the zones within the same region to ensure that the nodes are close enough geographically to meet SAP latency requirements for high-availability systems.

For more information about zones and regions, see Choosing a region and zone.

Before you design and implement any high-availability strategy on Google Cloud, review the Google Cloud Service Level Agreements. For general information about the reliability, privacy, and security of Google Cloud, see Trusted Infrastructure.

Live migration

If there is planned Google infrastructure maintenance on the host system where a VM instance is running, Google Live Migration moves the VM instance from one host to another without disrupting the application. This built-in feature comes at no additional cost and functions regardless of the size or complexity of your workload. Live Migration does not trigger a restart of the application, so you don't need to provide any startup scripts to use it.

Compute Engine monitors the state of the underlying infrastructure and automatically migrates the instance away from an infrastructure maintenance event. No user intervention is required. The target instance is identical to the source instance, including the instance ID, private IP address, and all instance metadata and storage. The database and application servers running on an instance during Live Migration continue to run without requiring any manual activities. By default, standard instances are set to use Live Migration. We recommend keeping this setting.

For more information, see the Live Migration on Compute Engine documentation.

Host auto restart

Compute Engine provides a setting for VM instances to automatically restart if there are unplanned shutdowns. Rather than triggering an alert that requires a manual reaction of an administrator, Compute Engine automatically starts the instance on a different host so the application can return to an operational state as fast as possible. Because this restart only affects the infrastructure layer, the application running on top of it might not start automatically. To solve this issue, you can reference startup scripts that are executed after the instance has been restarted, for example, to trigger SAP NetWeaver to start in the background. By default, instances are set to automatically restart. We recommend keeping this setting.

For more information on how to configure availability settings, see Setting instance availability settings. You can also reference the SAP documentation to develop a suitable startup script.

Level 2: Database setup

When you architect a high-availability setup for your database system, you can protect it against data loss if there is a failure. Given the distributed nature of SAP systems, all of your business-critical data is stored in a central database system. You protect this component first to minimize the impact of a failure event on the database instances. While a high-availability solution for a database can yield high uptime values, these architectures typically cost more than other levels of high availability. You might have to make a tradeoff between your goals for zero data loss and always keeping the system running and the total running costs of the environment.

SAP systems are designed to work with multiple database systems. Which mechanism you use to achieve a high-availability setup depends on the database you are running.

SAP HANA databases

This section covers HA architectures for a selection of common databases. For detailed information and setup instructions, see the database documentation for each database.

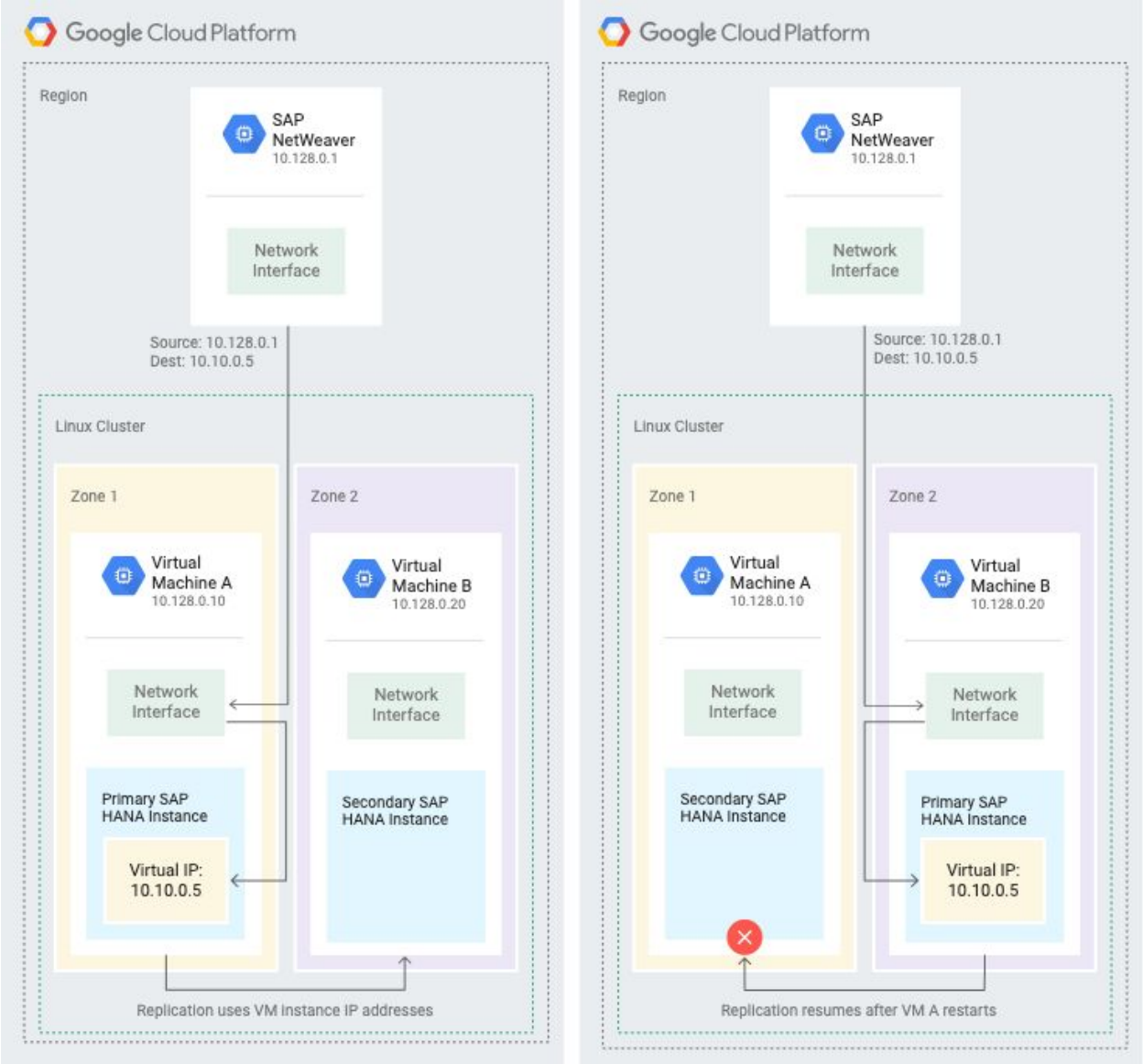
SAP HANA is an in-memory, column-oriented, relational database management system.

Synchronous SAP HANA System Replication

Synchronous SAP *HANA System Replication* (HSR) is an application-native mechanism for ensuring the high availability of any SAP HANA system. Data is continuously replicated from a primary system to a secondary system and can be preloaded into memory to allow for a rapid failover if there is a disaster. This setup can help you to resume productive operations with minimal downtime and zero data loss.

The mechanism to ensure no loss of data works as follows: Each SQL transaction on the primary database instance is not committed until it is committed on the standby instance. This mechanism keeps the standby instance 100% synchronized and satisfies a zero recovery point objective. On Google Cloud infrastructure, you can use synchronous replication for instances that reside in any zone within the same region. To protect the system against a failure of an entire zone, choose different zones for the primary and standby instance; that is, don't place them both in the same zone.

Google Cloud offers a Deployment Manager template for automated provisioning of an SLES Linux cluster with two SAP HANA systems. As shown in the following diagram, the template provisions a primary single-host SAP HANA system on one VM instance and a standby SAP HANA system on another VM instance. Both instances are in the same Compute Engine region.



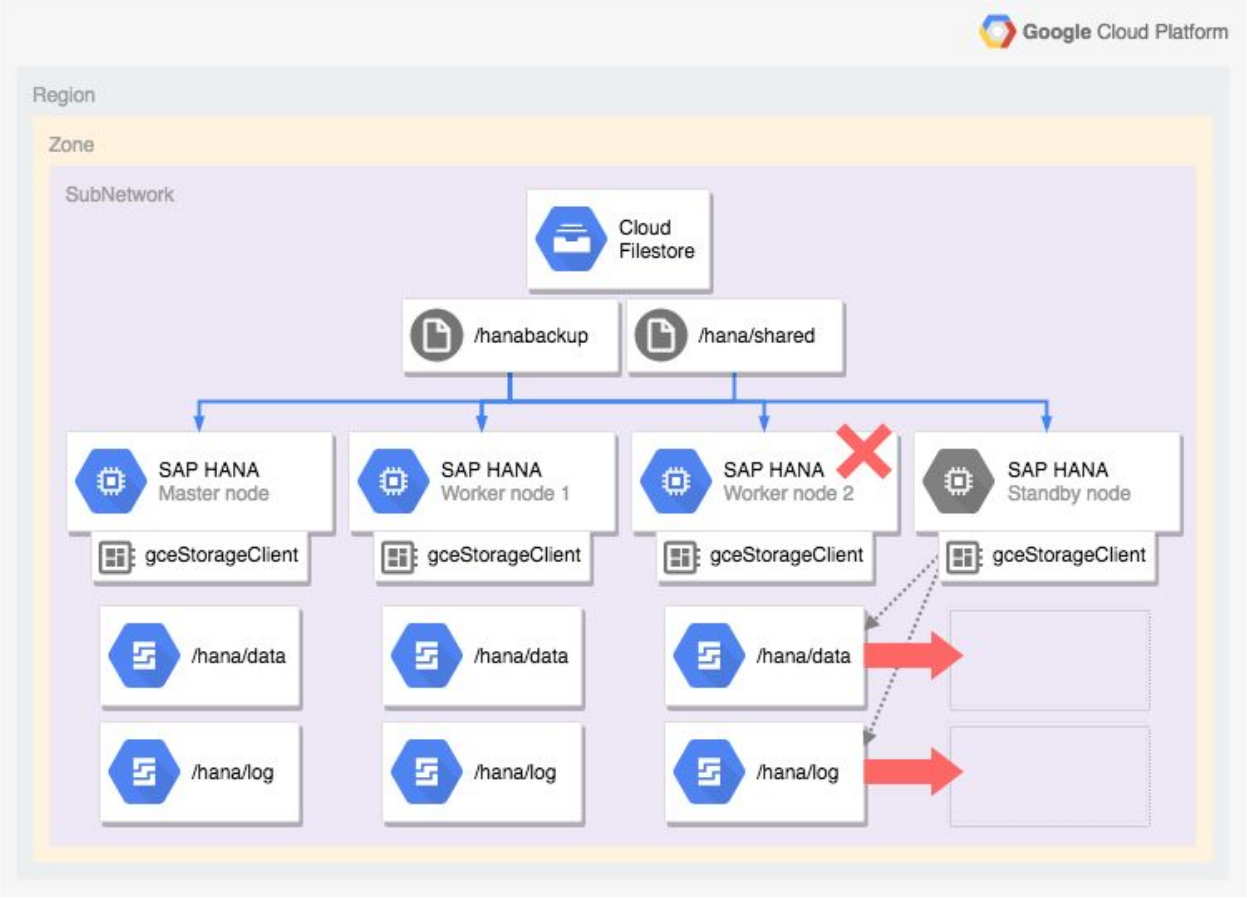
For more information about automated deployment and installation, see the SAP HANA deployment guide.

SAP HANA host auto-failover on Google Cloud

Google Cloud supports SAP HANA host auto-failover, the local fault-recovery solution provided by SAP HANA in a scale-out deployment. The host auto-failover solution uses one or more standby hosts that are kept in reserve to take over work from the master or a worker host if there is a host failure. The standby hosts do not contain any data or process any work. After a failover completes, the failed host is restarted as a standby host.

SAP supports up to three standby hosts in scale-out systems on Google Cloud. The standby hosts do not count against the maximum of 16 active hosts that SAP supports in scale-out systems on Google Cloud.

The following diagram shows a multi-host architecture on Google Cloud that includes support for SAP HANA host auto-failover. In the diagram, worker host 2 fails and the standby host takes over.



For more information, see [HA/DR planning for SAP HANA.]

SAP ASE databases

SAP ASE databases have a built-in Always On feature for high availability and disaster recovery. Two SAP ASE servers are set up in parallel: one is the primary instance and the other one is a warm standby companion instance. Set up both servers with their own set of resources; that is, each Compute Engine VM must have its own set of disks attached to it. (This setup is also known as a *shared nothing* configuration).

During regular operations, the primary instance ensures that data is copied to the companion instance through a replication management agent. Depending on the setup, the HA architecture can run in a synchronous replication mode, ensuring that no data is lost if there is a failure on the primary instance. For synchronous replication, you set up both instances with a small network latency (SAP recommends less than 5 ms) to avoid decreasing the performance of the database system for write-intensive operations. For an ASE HA setup in Google Cloud, place primary and companion instances in different zones in the same region to ensure good network connectivity between the instances. This configuration helps to protect against the loss of an entire zone.

For more information on deploying ASE in Google Cloud, see the SAP ASE Planning Guide.

MaxDB databases

For MaxDB, SAP uses a standby database to ensure faster return to operation if there is a failure on the primary database instance. The standby database is a copy of the original database at a given point in time. After the original database is copied to initialize the standby database, a regular process of log shipping occurs. All transaction logs that have been committed to the original database are imported, which brings the standby database to the latest state of data. If there is a failure, the standby database can take over quickly because all data has been loaded and processed up to the point in time of the last log shipping. Within Google Cloud, set up the two instances in different zones, each running in a separate VM with its own disks attached to it.

For more information about using a standby database, see the SAP Standby Database documentation.

Though this configuration lets you quickly return to operation after a failure, a small risk of loss of data remains between the point of failure and the time when the last log shipping to the standby instance occurred. Any transactions committed during this time period are lost, because the standby database did not receive all logs. There is, however, another option of a hot standby system with a shared log area, where the master database shares the same log area with one or many standby databases. This solution allows a setup with zero data loss, but

requires a network storage system instead of individual disks attached to the VM instances. For a high-availability shared storage solution, you can use third-party file-sharing solutions such as Elastifile or NetApp Cloud Volumes. In a failure event, a standby instance can take over from the master instance. During this takeover, the instance can access the latest logs that were committed, replay these logs, and continue operations as if it had always been the master database.

For more information on hot standby databases, see Hot Standby Database with Shared Log Area in the SAP documentation.

IBM Db2 databases

Db2 databases offer a highly available and disaster-tolerant IBM Db2 (HADR) cluster on Google Cloud that is supported by SAP. The cluster is configured and managed by IBM Tivoli System Automation for Multiplatforms (TSAMP) and uses the IBM Db2 HADR function for replication purposes. Applications connect to the primary IBM Db2 server through a floating IP address, which, if there is a failover, TSAMP reassigns to the standby server. The IBM Db2 HADR function supports up to three standby servers. Deploy the instances of the cluster in multiple zones of the same region.

With HADR, one or multiple standby database servers are available to take over from the primary server if there is a failure. Any data that is committed on the primary server is replicated immediately to standby servers running in synchronous replication mode, so that no data is lost if an infrastructure failure occurs on the primary server.

To deploy an IBM Db2 HA cluster for SAP, consult both the SAP and Google Cloud documentation. The SAP-provided IBM Db2 High Availability Solution: IBM Tivoli System Automation for Multiplatforms covers the general cluster requirements and the installation and configuration of the IBM Db2 instances, TSAMP, and the HA cluster. The Google Cloud-provided IBM Db2 high-availability cluster for SAP deployment guide covers how to set up the Google Cloud resources and certain cluster configuration tasks that are specific to Google Cloud.

Microsoft SQL Server databases

With Microsoft SQL Server, you have several options to ensure business continuity if there is a failure on the database server. You can use a standby database to prevent data loss by regularly shipping logs from the primary database to the standby database. You can customize the time between two log-shipping events depending on the acceptable amount of data loss and the amount of load the system can take. The maximum data loss increases as the time between

two log shippings increases, but more frequent log shipping leads to higher load on the database.

For even better data protection during a failure event, you can use the option for AlwaysOn Availability Groups. This option allows for synchronous and/or asynchronous replication of all transactions to one or multiple standby databases, allowing for zero data loss in a synchronous replication setup. For synchronous replication, deploy both instances to the same Google Cloud region to allow low latency between the instances, but spread the instances among multiple zones to protect against the failure of an entire zone.

For more information, see Configuring SQL Server AlwaysOn Availability Groups and refer to the supported configurations list (SAP Note 2456432).

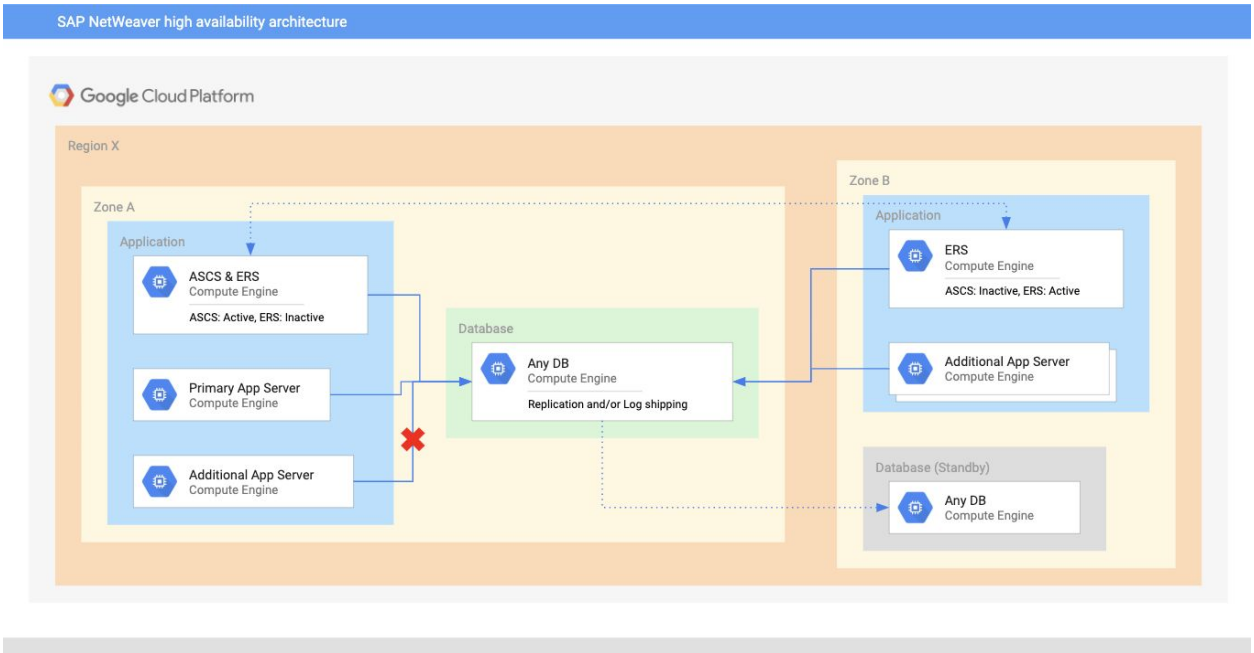
Level 3: Application servers

SAP applications usually run on the SAP NetWeaver platform, which provides the option of horizontal scaling to ensure support for high-availability setups on the application layer. Horizontal scaling allows for setups with multiple application servers sharing the load equally. If there is a failure on one of the instances, not all users are affected, and those who are affected can log in to one of the other servers without having to wait for the failed instance to restart. This approach can improve the end users' experienced uptime.

To coordinate the multiple application servers, the ABAP SAP Central Services (ASCS) provide two processes, the message service and the enqueue service. While the message service ensures a proper distribution of load between the application servers, the enqueue service takes care of transactional consistency by keeping an inventory of all existing database object locks. If users on different app servers try to edit the same object, the enqueue service blocks the second request until the first one is completed. In an HA setup, you must protect the enqueue service against failure, because a loss of the lock information can lead to database inconsistencies and prevent users from committing any transactions in the application. You can run a secondary instance with the Enqueue Replication Service (ERS) on independent resources from the ASCS. ERS continuously replicates the current state of the database lock table and if the ASCS instance fails, the ERS instance can take over with the latest lock information available.

To support this setup in Google Cloud, distribute the instances across multiple zones within the same region.

The following architecture diagram illustrates a sample setup with multiple application servers in two different zones and a failure on one of the application servers. Because other servers are already running and connected to the same database, the users can immediately log on to the application again. The ASCS and ERS instances are also distributed between multiple zones to protect against zonal failure.



For more information, see Building High Availability for SAP NetWeaver and SAP HANA on Linux and the SAP NetWeaver documentation.

The SAP NetWeaver global file system is a single point of failure that needs to be available to all SAP NetWeaver instances in a HA system. To ensure the availability of the global file system on Google Cloud, either highly available shared storage or replicated zonal persistent disks can be used.

For a high-availability shared storage solution, you can use file-sharing solutions such as Elastifile or NetApp Cloud Volumes. Google Cloud provides an NFS file server solution, Cloud Filestore, but Cloud Filestore does not currently provide a file server that is highly available across zones.

For replication of zonal persistent disks for Linux systems, you can use a Distributed Replicated Block Device to replicate the persistent disks that contain the SAP global file system between the nodes in a HA cluster.

For more information about storage options on Google Cloud, see File Servers on Compute Engine and Compute Engine storage options.

Summary

To architect a high-availability setup for SAP landscapes in Google Cloud, many options are available. There is not one general recommendation to fit every use case, but rather several choices to pick from, depending on the business requirements of uptime for each layer. Moving an SAP system from on-premises hardware to Google Cloud infrastructure can improve the availability through built-in features of the VM layer like Live Migration and Host Auto Restart, and thus improve the uptime without any additional configuration. Downtime caused by hardware failures can be reduced or even eliminated without requiring any customer activity.

For the database layer, various strategies exist depending on the database system. Typically, these strategies are either based on a regular copy of database logs to a standby system or a set of database instances running in a synchronous replication mode, where every transaction is replicated to a secondary system before the commit is sent back to the application layer. For such a setup, the two database instances must be placed inside the same Google Cloud region for low-latency requirements.

On the application layer, the SAP NetWeaver architecture can provide users with multiple application servers to ensure that the failure of one instance does not block all users from accessing the system. Any users who lose connection can log in with a different server immediately. With the flexible infrastructure in Google Cloud and automated deployment scripts, you can add an application server on-demand and place multiple application servers in a log-in group to improve the uptime of the application layer.

Further reading

Documentation for general concepts in Google Cloud:

- Live Migration | Compute Engine documentation
- Setting instance availability policies | Compute Engine documentation
- Designing for high availability

Google Cloud documentation for SAP deployments and operations:

- High availability for SAP HANA
- SAP ASE planning guide
- SAP MaxDB planning guide
- IBM Db2 for SAP planning guide
- SAP NetWeaver operations guide

SAP Help pages on business continuity of SAP NetWeaver and databases:

- Certified and supported SAP HANA IaaS platforms
- SAP HANA High Availability Support
- Overview of the HADR System for SAP ASE
- Business Continuity for the SAP MaxDB Database
- Replication and High Availability for MaxDB
- High Availability with the Standalone Enqueue Server
- High Availability of the SAP Web Dispatcher
- SAP Solutions on Google Cloud: Supported Products and Google virtual machine types (Note: 2456432)
- SAP on Google Cloud: Support prerequisites (Note: 2456406)