As an in-memory database, SAP HANA uses multiple network connections to transfer data, for example, from clients to the database during standard operations, between the nodes in a scale-out solution, and between data centers and to persistent storage in a disaster tolerant solution. This paper discusses the SAP HANA network requirements using an SAP BW on SAP HANA system as an example.
Contents

Legal Disclaimer .................................................................................................................. 3
Change history .................................................................................................................... 3

1 Introduction .................................................................................................................... 4

2 SAP HANA network zones ............................................................................................. 5

Client zone ......................................................................................................................... 5

  SQL Client Communication ............................................................................................. 5
  HTTP Client Communication ......................................................................................... 8

Internal zone ..................................................................................................................... 12

  Internode Network ......................................................................................................... 12
  System Replication Network ........................................................................................ 14
  Storage Replication Network ......................................................................................... 15

Storage zone ....................................................................................................................... 16

  Fibre Channel Storage using SAN ................................................................................ 16
  Network attached storage using NFS ............................................................................. 17
  Shared-nothing architecture with Cluster File Systems .................................................. 17
  Backup storage ............................................................................................................... 18

3 Scenario: SAP BW on SAP HANA with system replication ........................................... 19

  SAP BW Scenarios ......................................................................................................... 19
  SAP BW Network Traffic ............................................................................................... 20
  Technical Requirements ............................................................................................... 22

  Recommendations for the Client Zone Network ............................................................. 26

    Client reconnect with the Secure User Store (hdbuserstore) ........................................ 26
    Client reconnect in SAP HANA system replication ....................................................... 27
    IP redirection (or Virtual IP) ........................................................................................ 27
    Connectivity suspend of the application server ............................................................ 29
    Client reconnect for SAP HANA XS applications (http/https) .................................... 29

  Recommendations for the Internal Zone Networks .......................................................... 30

    Internode network ...................................................................................................... 30
    Internal host name resolution ....................................................................................... 31
    System replication network .......................................................................................... 31
    System replication host name resolution ...................................................................... 33

  Recommendations for the Storage Zone Networks ........................................................ 34
Legal Disclaimer

THIS DOCUMENT IS PROVIDED FOR INFORMATION PURPOSES ONLY AND DOES NOT MODIFY THE TERMS OF ANY AGREEMENT. THE CONTENT OF THIS DOCUMENT IS SUBJECT TO CHANGE AND NO THIRD PARTY MAY LAY LEGAL CLAIM TO THE CONTENT OF THIS DOCUMENT. IT IS CLASSIFIED AS "CUSTOMER" AND MAY ONLY BE SHARED WITH A THIRD PARTY IN VIEW OF AN ALREADY EXISTING OR FUTURE BUSINESS CONNECTION WITH SAP. IF THERE IS NO SUCH BUSINESS CONNECTION IN PLACE OR INTENDED AND YOU HAVE RECEIVED THIS DOCUMENT, WE STRONGLY REQUEST THAT YOU KEEP THE CONTENTS CONFIDENTIAL AND DELETE AND DESTROY ANY ELECTRONIC OR PAPER COPIES OF THIS DOCUMENT. THIS DOCUMENT SHALL NOT BE FORWARDED TO ANY OTHER PARTY THAN THE ORIGINAL PROJEC TED ADDRESSEE.

This document outlines our general product direction and should not be relied on in making a purchase decision. This document is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this document. This document and SAP’s strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP assumes no responsibility for errors or omissions in this document and shall have no liability for damages of any kind that may result from the use of these materials, except if such damages were caused by SAP intentionally or grossly negligent.

© Copyright 2018 SAP SE. All rights reserved.

Change history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>October 2014</td>
<td>Initial release</td>
</tr>
<tr>
<td>1.1</td>
<td>October 2014</td>
<td>Minor addition in backup chapter – storage snapshots added</td>
</tr>
<tr>
<td>1.2</td>
<td>December 2014</td>
<td>Bug fix regarding RTT for async replication</td>
</tr>
<tr>
<td>2.0</td>
<td>November 2018</td>
<td>Minor updates regarding new HANA features (XSA, ...)</td>
</tr>
</tbody>
</table>
Introduction

The components of an SAP HANA system communicate via different network channels. It is recommended practice to have a well-defined network topology to control and limit network access to SAP HANA to only those communication channels required for your scenario, and to apply appropriate additional security and performance measures as necessary.

Clients require access to the SAP HANA database, and while SAP HANA is an in-memory database which stores and processes its data in memory, the data is also saved in persistent storage locations to provide protection against data loss. In distributed (scale-out) systems, communication must be possible between hosts; in disaster recovery setups, data is replicated over the network to other data centers.

The components belonging to SAP HANA communicate over several logical network zones:

- **Client zone.** Different clients, such as SQL clients on SAP application servers, browser applications using HTTP/S to the SAP HANA XS server and other data sources (such as BI) need a network communication channel to the SAP HANA database.

- **Internal zone.** The internal zone covers the communication between hosts in a distributed SAP HANA system as well as the communication used by SAP HANA system replication between two SAP HANA sites.

- **Storage zone.** Although SAP HANA holds the bulk of its data in memory, the data is also saved in persistent storage locations – which probably need to be accessed via a network – to provide protection against power failures or other events that cause hosts to become unavailable.

Each communication zone needs special attention about configuration, setup, security and performance requirements. Redundancy is recommended for the internal and the storage networks but is also important for high availability requirements.

The following illustration shows the three logical zones of a distributed SAP HANA system (in this example with 2 hosts plus 1 standby host) on the primary site, which replicates to a secondary site (with 2 hosts) using SAP HANA system replication.

---

1 This is just an example. For SAP BW systems, at least 3 worker nodes are recommended. See the SAP Community Network blog http://scn.sap.com/docs/DOC-39682 as well as SAP Note 1702409 - HANA DB: Optimal number of scale out nodes for BW on HANA.
2  SAP HANA network zones

The logical communication zones of SAP HANA are explained in greater detail in this section².

Client zone

SQL Client Communication

Client applications communicate with an SAP HANA system via a client library (SQLDBC, JDBC, ODBC, DBSL, ODBO ...) for SQL or MDX access from different platforms and types of clients. In distributed systems, the application has a logical connection to the SAP HANA system; the client library may use multiple connections to different hosts or change the underlying connection over time. The following figure provides an overview of some of the clients used on SAP HANA systems and the interfaces provided by the client library.

² For additional information on SAP HANA Networks please refer to SAP Note 2222200 - FAQ: SAP HANA Network.
The SQL client libraries will connect to the first available host specified in the connect string, which can contain a single host or a list of hosts. All hosts that could become the active master because they are one of the three configured master candidates, should be listed in the connect string to allow initial connection to any of the master candidates in the event of a host auto-failover. As a result, the client libraries receive a list of all hosts. During operations, statements may be sent to any of these hosts. The client connection code uses a "round-robin" approach to reconnect and ensures that these clients can reach the SAP HANA database. In the event of failover, a list of hosts is parsed until the first responding host is found.

Please refer to the SAP HANA Master Guide for further details on connect strings with multiple host names.

To ensure transactional consistency in distributed setups, SAP HANA supports distributed transactions, which are transactions that involve data that is stored on different index servers. In this context, the client library supports load balancing by connection selection and minimizes communication overhead using statement routing based on information about the location of the data. Connection selection and/or statement routing are executed based on the setting of the ini parameter client_distribution_mode in the indexserver.ini file (the default setting is statement for statement routing).

- **Statement routing** helps to optimize performance by reducing the amount of data that must be sent over the internal network zone. In principle, clients can send requests to any index server in a distributed system. However, this could lead to a performance decrease if, for example, a query involving data located on server1 is sent to server2. Server2 would have to forward the query to server1 and forward the response from server1 to the client. This overhead can be avoided if the client sends the query to server1 directly. This can be achieved using prepared statements.
A prepared statement is an SQL statement (typically parameterized) that is sent to the server where it is precompiled (1). The prepared statement is returned to the client (2). To execute the statement, the client sends the prepared statement (usually filled with the actual parameters) to the server where (most of) the data is located (3) by opening a new connection. This two-step protocol (prepare and execute) is used for statement routing in a distributed system, where the “prepare” request may return information about the preferred locations for executing the statement. Based on this information, the client library sends requests to execute the prepared statement directly to one of the indicated index servers. If the situation has changed since the “prepare” request was processed, the response for an “execute” request may also contain location information (4). Statement routing is done by the client library and is transparent to the application. With statement routing, different statements of the same transaction may be executed on different servers.

- **Connection selection** is transparent to the client application. Whenever a new connection is created, the client library chooses one of the servers in a round-robin manner. During a long-living connection, the client library may connect to a different server to improve the workload distribution. If a connected server fails, the client library switches to a different server.

- **Command splitting** describes the ability of the client interface to split up the execution of bulk statements that allow, for example, the insertion of a big array of rows with one command. The client library can be configured to split the execution of such a command into batches that are sent using multiple connections. The servers are chosen according to the client-side landscape information.
Command splitting

HTTP Client Communication

In addition, the communication with SAP HANA servers can be initiated by a web browser or a mobile application. These use the HTTP/S protocol to access SAP HANA Extended Application Services (SAP HANA XS) – the so-called SAP HANA XS Classic Model (XSC) and as of HANA 1.0 SPS11 the new SAP HANA XS Advanced Model (XSA). The different approaches of XSC and XSA regarding client communication are roughly documented in the next sections.

SAP HANA XS Classic Model (XSC)

As shown in the following picture, in the Classic Model each SAP HANA instance includes an SAP HANA XS server and an internal SAP web dispatcher – referred to as HDB web dispatcher.
You can have multiple SAP HANA XS servers for purposes of scale-out in a distributed SAP HANA system. In this case, it is recommended that you install an external, itself fault-protected HTTP load balancer (HLB) to support HTTP (web) clients, such as the SAP Web Dispatcher (webdisp) or a similar product from another vendor. In scale-out or system replication landscapes, the HLBS are configured to monitor the web servers on all hosts on both the primary and secondary sites. If an SAP HANA instance fails, the HLB – which serves as a reverse web-proxy – redirects the HTTP clients to an SAP HANA XS instance running on an active host. HTTP clients are configured to use the IP address of the HLB itself, which is obtained via DNS, and remain unaware of any SAP HANA failover activity.

An internal HDB web dispatcher runs between the external HTTP load balancer and the SAP HANA XS server running on each host. This internal web dispatcher provides client access to the SAP HANA XS server via HTTP in a 1:1 mapping.

For more information, please see the SAP HANA Master Guide.

SAP HANA XS Advanced Model (XSA)

Since SPS11 SAP HANA includes this additional, new run-time environment for application development. Applications are either HANA native developments or run in other widely-known application servers and languages making use of APIs to access the SAP HANA database. Essentially, any application that can utilize ODBC, ODBO, or JDBC can integrate with SAP HANA.

SAP HANA extended application services, advanced model (XS Advanced) is a web application server layer on top of the SAP HANA database. It runs in separate processes and communicates with the database via SQL. The so-called “XS Advanced” can be installed on dedicated hosts in the same SAP HANA system or together with other SAP HANA services on the same host.

The XS Advanced platform supports several programming languages and execution environments, such as Java, Node.js, and Python. Other execution environments can be added on demand using a bring-your-own-runtime approach. The XS advanced application runtimes are invoked over HTTP(s) and communicate with the SAP HANA database via SQL.

XS Advanced on-premise (XS Advanced OP) was developed by SAP as an on-premise application platform that is compatible to the SAP CP Cloud Foundry platform. The goal is that you can run the same XS Advanced application on premise and in the cloud, without modification. For further details please see SAP HANA Developer Guide for SAP HANA XS Advanced Model.

In the following picture, illustrating a HANA system with XS Advanced OP, it is shown that the XS controller only exists once in the whole system (like the active master node in a scale-out HANA). This is the entity accepting requests from the browser and dispatching it to the XS execution agents which are located on each host of the distributed XS Advanced system. Example for such requests are pushing, starting and stopping applications, creating service instances, and binding services to applications. To stop and start an XS Advanced instance, you need to stop or start the controller. Administrators and developers can send commands to the controller which has information about all deployed applications and their status (started, stopped) at all time.
The XS controller is the central component of the XS Advanced OP runtime. Requests for managing services and applications are sent to the controller. It stores configuration information in its configuration database, and it has a blob store for application data. XS Advanced OP persists the configuration database and the blob store in SAP HANA.

The controller triggers the XS execution agent to execute applications. The execution agent receives the droplets and starts processes for executing them. For isolation, the applications in different spaces are started with different operating system users that have minimum permissions.

Applications are runnable on certain runtime stacks, such as Java, Node.js or Python.

XS Advanced services are provided in two ways. Some services, such as the User Account and Authentication Service (UAA), are installed as a part of the platform. Others are deployed as XS application and then registered as a service. The job scheduler service is an example of such an application. It is used to schedule events at specified times.

Requests to the XS controller, XS applications, and XS services are made via HTTP(s) and go through a reverse proxy server, which also serves as a load balancer. This is the SAP Web Dispatcher. The dispatcher maps the domain and subdomain names in the HTTP requests to XS applications and forwards the request to the actual hosts and ports where the applications are running. When applications are started with several instances for scale-out, the load balancing is done by the dispatcher. The dispatcher is not only used for requests from external clients, but also for requests between XS applications and between applications and XS services.

XS Advanced OP can be installed on several hosts for scale-out and failover. For scale-out several hosts can be configured as XS worker hosts. Each XS worker host has its own execution agent, which starts and stops the application processes on that host, and its own SAP Web Dispatcher. The XS
controller and the UAA server are central processes, which exist only once in a system. The XS worker hosts can be configured as dedicated XS hosts or as shared workers that also run SAP HANA database processes. For high availability additional XS standby hosts can be defined, which take over, when a worker host fails. See SAP Note 2300936 - Host Auto-Failover & System Replication Setup with SAP HANA extended application services, advanced model for further information on highly available XSA configurations.

In a scale-out landscape with multiple nodes you can have multiple SAP HANA XS execution agents distributed over the participating hosts.
As shown in the above picture, it also is not necessary that the HANA database resides on the same hosts as the XS execution agents; they can run on their own hosts. The XS controller and XS execution agent communicate via https.

A comparison of XS Classic (XSC) and XS Advanced (XSA) can be found in the [SAP HANA XS Advanced Migration Guide](https://help.sap.com/hana).  

**Internal zone**

Once the physical limits of a single host have been reached, it is possible to scale out over multiple hosts to create a distributed SAP HANA system. One technique is to distribute different schemas and tables to different hosts (complete data and user separation), but that is not always possible, for instance, when a single table is larger than the host’s RAM size. SAP HANA supports distribution of its server components across multiple hosts – for example, for scalability.

**Internode Network**

A distributed system can overcome the hardware limitations of a single physical host, and it can distribute the load between multiple hosts. The most important strategy for data scaling is *data partitioning*. Partitioning supports the creation of very large tables (billions of rows) by breaking them into smaller chunks that can be placed on different machines, as illustrated below:

---

3 Master data tables should not be partitioned since they are to be joined to all other tables. Network traffic is reduced, if tables in the same query should have the same partition criteria (first-level) to benefit from query optimizations, e.g. collocated joins of OLAP engine for BW.
In a distributed system, each index server is assigned to one host to attain maximum performance. It is possible to assign different tables to different hosts (by partitioning the database), to split a single table between hosts (by partitioning the table), or to replicate tables to multiple hosts.

In such a system, the name server acts as a central component that “knows” the topology and how the data is distributed. It “knows” which tables, table replicas or partitions of tables are located on which index server. When processing a query, the index servers ask the name server about the locations of the involved data. To prevent a negative impact on performance, the topology and distribution information is replicated and cached on each host. Each SAP HANA system has one master name server that owns the topology and distribution data. This data is replicated to all the other name servers, which are referred to as the slave name servers. The slave name servers write the replicated data to a cache in shared memory from where the index servers of the same instance can read it.

The master name server has its own persistence where it stores name server data (topology, distribution, data). The slave name servers have no persistence as they hold only replicated data in memory.
In a distributed (scale-out) system, all network zones are present with additional traffic going over the internal network due to table distribution and partitioning. For example, index server A processes a query that involves tables located on different servers. When processing the query, the optimizer asks the name server for the location information and chooses the optimal execution plan taking distribution into account. A distributed execution plan is created that also contains the location information. The executor of the distributed plan also needs to be aware of the distribution. It sends parts of the execution plan to remote servers, triggers the execution of the remote operations, and synchronizes distributed execution based on the availability of intermediate results as input for the next steps. Finally, it combines the results provided by the individual servers to generate the result.

SAP HANA supports three ways of distributing data between multiple index servers in a system:

- Different tables can be assigned to different index servers (which normally run on different hosts). Here the entire table is assigned to a specific index server that resides on the master, on the slave, or on all hosts.
- A table can be split so that different rows of the table are stored on different index servers. Splitting tables is currently supported for column store tables only.
- A table can be replicated to multiple index servers, for better query and join performance.

For more information on table placement, please have a look in the SAP HANA Administration Guide at the sections on “Table Partitioning”, “Table Distribution” and “Table Placement”.

**System Replication Network**

In SAP HANA system replication, each SAP HANA instance communicates on the service level with a corresponding peer in the secondary system to persist the same data and logs as on the primary system. The services in the secondary system operate in live replication mode: that is, all secondary system services communicate constantly with their primary counterparts, replicating and persisting data and logs and typically preloading data into memory.

---

*SAP HANA system replication* network connection

---

4 Even if the primary site has a standby host configured, the secondary does not necessary need one (valid since SPS 06).
When the secondary system is first started in live replication mode, each service component establishes a connection with its primary system counterpart and requests a snapshot of the data. From then on, all logged changes in the primary system are replicated over the system replication network. Whenever logs are persisted in the primary system, they are also sent to the secondary system. A transaction in the primary system is not committed until the logs are replicated, as determined by one of the log replication options synchronous, synchronous in-memory and asynchronous. The longer the distance between the primary and the secondary system and the more switches that must be passed, the higher the latency is, which mainly influences synchronous replication.

At regular intervals (the default is every 10 minutes), the data increment (that is, everything that has changed since the last data transportation) is transported from the data area of the primary site to the data area of the secondary site.

When using SAP HANA system replication, you need to prepare the client reconnect for the event of takeover. The redirection of IP addresses or virtual hostnames regarding the change in DNS entries can be done by using either external cluster management software or the SAP HANA takeover hooks. Please check the corresponding section below for further details. More information on system replication and client connection recovery can also be found in the SAP Note 2407186 - How-To Guides & Whitepapers For SAP HANA High Availability and in the SAP HANA Administration Guide.

### Storage Replication Network

The storage replication setup is transparent to SAP HANA: the storage subsystem mirrors (replicates) all data changes to another remote storage device, either synchronously or asynchronously depending on the device type, distance and customer preference.

![SAP HANA storage replication network connection](image)
In synchronous mode, a redo log entry will only be considered complete when it is persisted on both sites: that is, shipped over the storage replication network to the secondary site. This results in a higher latency than without replication. After failover to the secondary site, the storage is remounted, and SAP HANA is restarted. For more details on storage replication, please refer to the SAP HANA High Availability White Paper and the SAP HANA Storage Requirements whitepaper (PDF attachment to SAP Note190082) and contact the hardware vendor for a specific offering.

Storage zone

The SAP HANA database, like other database management systems, uses the host operating system’s “file” abstraction layer for persistent storage. Large files – the data and log volumes in SAP HANA terminology – are located on hard disk drives or solid state drives (SSDs). Persistence is traditionally provided by arrays of hard disk drives, in various direct-attached and network-attached configurations. Direct-attached storage (often in the same enclosure as the server) uses standard protocols like SATA or SAS. Extending the notion of directly attached block storage, some vendors have introduced external storage arrays accessed using the Fibre Channel protocol over storage area networks (SANs).

Fibre Channel Storage using SAN

With the Storage Area Networks the Fibre Channel storage LUNs\(^5\) are mapped to SAP HANA server hosts with a point-to-point connection. In the event of a failover to the standby host, the remapping is managed by the SAP HANA Storage Connector (see SAP Note 190823 - SAP HANA Storage Connector API). SAN LUNs appear to the OS as disks (along with the local disks). For shared SAP HANA binaries NFS/NAS\(^6\) storage is required. Redundant connectivity to the corporate network via LAN (Ethernet) and to storage via Storage Area Network (SAN) must always be configured. In the following picture, the internode network connected via Ethernet (LAN) is attached to an NFS-shared NAS storage holding the SAP HANA binaries, which all SAP HANA servers must be able to access. In addition, each SAP HANA server is connected to its own non-shared storage; the Fibre Channel protocol controls the mapping of each persistence (data and log areas) to LUNs on the SAN. Reconnection of the LUNs residing on the storage in the event of a failover is supported by the SAP HANA Storage Connector API.

---

\(^5\) A logical unit number (LUN) is a unique identifier used to designate individual or collections of hard disk devices for address by a protocol associated with SCSI, iSCSI, Fibre Channel or a similar interface.

\(^6\) Network Attached Storage (NAS) is an alternative storage solution that use network protocols to connect to a remote file server, with access handled on file level.
Non-shared SAN storage attached via Fibre Channel for HANA data and log volumes and shared NFS/NAS storage for HANA binaries.

Network attached storage using NFS

Network Attached Storage (NAS) is an alternative storage solution that uses network protocols to connect to a remote file server. This shared storage infrastructure using NAS provides a shared-everything architecture where data volumes, log volumes and SAP HANA binaries can be accessed via NFS. The NFS file systems are mounted via OS mount: in the event of a node failover, the standby host has immediate access to the shared storage where the data and log volumes are located.

Only one LAN (Ethernet) switch is needed for redundant connectivity to the corporate network and the NAS. The following picture shows a possible internode setup.

Shared-nothing architecture with Cluster File Systems

In a distributed landscape, SAP HANA must be able to read and write all data and log volumes as well as the SAP HANA binaries on all hosts. A cluster file system, such as GPFS\(^7\), spans the local SAP HANA

\(^7\) General Parallel File System from IBM
server node disks, making the data and log volumes as well as the SAP HANA binaries available to the whole scaled-out landscape. In the event of a host auto-failover, the cluster file system provides a standby node with the required data set. To achieve this, all data is transparently persisted twice: one copy on the node writing the data and a second copy on one or more other nodes in the cluster.

For a detailed description of the amount of traffic on the storage network, please read the SAP HANA Storage Requirements whitepaper (PDF attachment to SAP Note190082). Information on SAP HANA certified storage can be found in the SAP HANA Tailored Data Center Integration.

Backup storage

Backups are a low-cost approach to disaster recovery with less extensive requirements than other approaches like storage or system replication. A complete data backup contains the entire payload of all data volumes. Depending on the storage location of the backups\(^{8}\), the network paths to this location can become a bottleneck and lead to performance impacts on production operations, if misconfigured. The amount of traffic on these channels also depends on the total size of the data volumes and on the number of backup generations that are to be created as well as on the frequency with which data is changed in the SAP HANA database resulting in log backup traffic. The communication channels to the backup location with the SAP HANA database should be separate from the communication channels to the data and log volumes of the database to prevent congestions along the way.

Data and logs are usually backed up to the same storage device. Currently, SAP HANA allows configuration of backup storage in three different ways:

- **External backup tools**: Data and log backups are transferred to third-party provider software (using the BACKINT interface), which transports the data and log backups to another location.
- **Shared file system**: An external shared file system is mounted – for example, with NFS – to all hosts in a distributed landscape, thus ensuring that even after host auto-failovers the correct locations can be accessed by the hosts.
- **Storage snapshots**: SAP HANA offers an interface that allows storage vendors to integrate their storage snapshot technology for SAP HANA backup and recovery.

Neither external backup tools using the SAP HANA BACKINT interface nor storage snapshots will be covered in this document. For more details on backup storage, please read the corresponding section in the SAP HANA Storage Requirements whitepaper (PDF attachment to SAP Note190082). Further information on backups and storage snapshots can also be found in the corresponding sections of the SAP HANA Administration Guide.

\(^{8}\) 3rd party backup tools using the SAP HANA BACKINT interface will not be covered in this document.
3 Scenario: SAP BW on SAP HANA with system replication

This section provides a closer look at SAP BW on an SAP HANA landscape setup. It describes typical scenarios that run in an SAP BW system and their dependency on performant and securely working network connections.

SAP BW Scenarios

The scenarios that are influenced by the performance of the relevant network connections are described in the following table.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data load</td>
<td>The SAP application server writes huge bulk inserts (coming from other systems, such as SAP ERP) into the SAP HANA tables – that is, to the delta memory and to the persistence. The insert call arrives on one SAP HANA host, which holds parts of the table. If the insert touches a distributed table, the data located in other parts of the table are synchronously shipped to the corresponding host. In addition, write transactions asynchronously persist the redo log to the log volumes on the storage; in synchronous system replication, they are sent to the secondary site and only persisted when the acknowledgement is received that the data arrived. The delta data shipment done in a system replication setup (per default every 10 minutes) can also cause considerable traffic.</td>
</tr>
<tr>
<td>Reporting</td>
<td>Distributed tables are joined with multiple, possibly very large non-distributed master data tables residing on one host. Depending on the query plan calculated by the optimizer, it is possible that parts of the tables and intermediate results are sent back and forth between the nodes more than once. The worker hosts handle OLAP load exclusively – SAP BW data (master data + cubes/DSOs/PSAs) is distributed evenly across all slaves, and how Cube, DSO and PSA tables are partitioned depends on the table placement rules. In a <em>collocated join</em>, the corresponding records of the files being joined exist on the same host. The values of the partitioning key of the files being joined are partition-compatible. No data needs to be moved to another host to perform the join. This method is only valid for queries in which all of the fields of the partitioning keys are join fields and the join operator is the = (equals) operator.</td>
</tr>
<tr>
<td>Backups to file system</td>
<td>For a data backup, the current payload of the data volumes is read and copied to the backup location. The network traffic required by backups not only depends on the total size of the data volumes, but also on the frequency with which data is changed in the SAP HANA database. For example, if the backup policy requires complete data backups to be performed on a daily basis, the traffic on the networks becomes very relevant.</td>
</tr>
<tr>
<td>Failover (host auto-failover)</td>
<td>The services on the standby host run in idle mode. Upon failover, the data and log volumes of the failed host are automatically assigned to the standby host, which then has read and write access to the files of the failed active host. Row-store as well as column-store tables (on demand) are loaded into memory. The log entries are replayed.</td>
</tr>
<tr>
<td>Takeover (system replication)</td>
<td>The secondary system is already running; that is, the services are active but do not accept SQL and thus are not usable by applications. Just as during a database restart, the row-store tables are loaded into memory from the storage</td>
</tr>
</tbody>
</table>
If table preload is used, then most of the column-store tables are already in memory as they were loaded in the primary site. During takeover, the replicated redo logs that were shipped since the last data transfer from primary to secondary have to be replayed. The client connection is lost, which can be handled by one of the client reconnect options described below.

### SAP BW Network Traffic

The following table lists the network traffic resulting from the SAP BW scenarios mentioned above.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Client Zone</th>
<th>Internal Zone</th>
<th>Storage Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data load</td>
<td><strong>Application server:</strong> The client network connecting the application server requires sufficient bandwidth to handle bulk inserts.</td>
<td><strong>Internode network:</strong> The insert call arrives on one SAP HANA node that holds (parts of) the table. For distributed tables, the data located in other parts of the table are synchronously shipped to the corresponding node – producing high load on the internode communication channel. The channel must provide enough bandwidth to handle this load.</td>
<td><strong>Storage network:</strong> SAP HANA persists a written redo log of up to 1 MB into the log segment files in the log volume. The network path to the storage solution must be sufficient to handle the load on the system. With system replication enabled and using “synchronous” replication, the storage network connection on the secondary site must be equally performant.</td>
</tr>
<tr>
<td>Reporting</td>
<td>The client network must handle bulk result sets of data.</td>
<td><strong>Internode network:</strong> Depending on the optimizer’s query plan, parts of the tables and intermediate results are possibly sent over the internode network more than once.</td>
<td></td>
</tr>
<tr>
<td>Data backups to file system</td>
<td></td>
<td></td>
<td><strong>Storage network:</strong> For a data backup, the current payload of the data volumes is read from the persistent storage of all SAP HANA hosts and transported to the storage where</td>
</tr>
<tr>
<td>Failover (host auto-failover)</td>
<td>The clients must be prepared for failover and thus for client reconnect.</td>
<td>Storage network: Once the data and log volumes can be accessed by the failover host, row-store as well as column-store tables are read from storage and into memory, and the log entries are replayed.</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Takeover (system replication)</td>
<td>The clients must be prepared for takeover when the connection to SAP HANA is lost. This can be achieved with network- or DNS-based IP redirection, and handled either by cluster management software or using SAP HANA takeover hooks.</td>
<td>Storage network: The secondary system is already running. Just as with a database restart, the row-store tables are loaded into memory from the storage subsystem. During takeover, the replicated redo logs that were shipped since the last data transfer from primary to secondary need to be replayed.</td>
<td></td>
</tr>
</tbody>
</table>

The following picture shows a possible network configuration for an SAP BW on SAP HANA system running on four hosts (master, two workers and a standby) that are connected via an internode network (red). Also, there are two types of clients attached: SAP BW application servers (light blue) and other SAP HANA clients (dark blue, for example, the SAP HANA studio). The data is persistently stored on enterprise storage (purple) and backed up to a separate storage location (green). To make this setup highly available, a standby host has been defined; moreover, the data is replicated to another data center using SAP HANA system replication (yellow). In addition, the use of external administration tools is possible thanks to the configuration of a separate, low-bandwidth administrative network (black).
Networks connections for a distributed SAP HANA system, with SAP HANA system replication configured

It is important to configure the networks according to the specific performance and security requirements of the SAP HANA system. Implementing redundancy is highly recommended for the critical networks – such as for the internode communication, the backup network and the storage network – to be prepared for single component failures and to avoid single points of failure. In addition, separate network channels should be available for storage access and for access to the backup location. Otherwise, congestion on the network could lead to a performance drop on the production system because of the concurrent access of transactional load and backup load over the same storage channel.

Technical Requirements

All networks need to be properly segmented and may be connected to the same core/backbone switch. Following the recommendation to configure separate networks for different purposes could result in each SAP HANA server having logical network connections as shown in the following picture.
Logical network connections per SAP HANA server

Besides these logical, in most cases mandatory networks within an SAP HANA system, diverse combinations of network configurations are possible in which one network interface card\(^9\) (NIC) is used to realize multiple logical networks. The following tables show a few – out of many – possible setups based on different performance and security requirements. These setups should be configured redundantly, according to SAP HANA system requirements.

| Client zone: | If there are no security and performance concerns, all clients coming from outside of the SAP HANA database (such as the SAP application servers, SQL clients and external administration clients) can run over one NIC. |
| Internal zone: | The internode network must have its own NIC for performance and security reasons, which could also apply to the system replication network according to the business’s requirements. |
| Storage zone: | If non-shared FC SAN storage is used for the data and log volumes, a separate Ethernet NIC must be available for backup storage needing a shared storage. But even if NFS shared storage is used for the data and log volumes as well as for backups, it is highly recommended to separate these connections to prevent data traffic congestion. |

| Client zone & internal zone: | If there are no security and performance concerns, SAP HANA system replication can use the same public NIC that is used by all SAP HANA clients (like SAP application servers, SQL clients); the networks should be configured as separate VLANs. For security reasons, the administration network might require its own NIC. |
| Internal zone: | The internode network must have its own NIC for performance and security reasons. |
| Storage zone: | If non-shared FC SAN storage is used for the data and log volumes, a separate Ethernet NIC must be available for backup storage needing a shared storage. But even if NFS shared storage is used for the data and log volumes as well as for backups, it is recommended to separate the connections to prevent data traffic congestion. |

\(^9\) NICs are also referred to as network interface controllers, network adapters, LAN adapters, and so on.
is used by all clients (like SAP application servers, SQL clients and the administration client); the networks could be configured as VLANs that separate clients and system replication.

**Internal zone:**
The internode network must have its own NIC for performance and security reasons.

**Storage zone:**
If non-shared FC SAN storage is used for the data and log volumes, a separate Ethernet NIC must be available for backup storage needing a shared storage. But even if NFS shared storage is used for the data and log volumes as well as for backups, it is recommended to separate the connections to prevent data traffic congestion.

The different networks that are required to run SAP BW on SAP HANA, with SAP HANA system replication as the disaster recovery solution, can be configured as VLANs (virtual local area network) and VSANs (virtual storage area network – in the case of Fibre Channel attached storage). Areas which can communicate with each other, and others which are not allowed to, can be configured in a network switch.

Modern Ethernet switches support segregation of ports into multiple different network segments. These segments are known as VLANs. Network packets are only switched between servers with ports in the same VLAN. Hence, VLANs can be considered as (virtual) isolated Layer-2 network segments. Data traffic between the segments in this constellation is prohibited. In the following picture, three different IP ranges for the client network, the system replication network and the internode network are configured as VLANs within one Ethernet switch, showing on a basic level one possible way to structure the different networks.
In a redundant setup, two ports can be bundled on one or more network cards to make the NICs (network interface cards) highly available and increase throughput. Also known as bonding, the process of bundling two network ports into one virtual unit results in the ports being considered by the system as one device. This means that both ports have the same IP address. On the switch, the ports can be assigned to different VLANs; load balancing is active on the bundled ports to select a physical connection using different algorithms such as round-robin, hashing over the IP address and/or TCP port number, or other methods depending on the switch vendor.

For reasons of availability, redundant switches are recommended. This means that the bonding of two physical NIC ports on the SAP HANA hosts must be configured in such a manner that each port in the trunk connects to a separate Ethernet switch. This is roughly described in the following picture, using the Fibre Channel SAN storage network as an example. A setup like this is recommended for all VLANs (for Ethernet switches) and VSANs (Virtual SANs for Fibre Channel switches) used in SAP HANA.
Recommendations for the Client Zone Network

In the example used in this document (see above), three separate client networks have been configured (for administration, SAP application servers, and other SAP HANA clients). All clients must be able to access all hosts in a distributed system. The application server network and the network for other SAP HANA clients such as the SAP HANA studio, BI clients, and so on could be either separated – if there are special security requirements, for example – or used together. They should provide a transfer rate of 10Gbit/s on their connections (10GbE\textsuperscript{10}) which should also be configured for high availability; that is, redundant network cards should be available in each server to be prepared for the loss of a physical connection.

The other administrative network mentioned is reserved for external administration tools, where a simple 1GbE connection would be sufficient. This network is an operating system management network, which is non-redundant and for management use only. It is not vital to the SAP HANA services.

Client reconnect with the Secure User Store (hdbuserstore)

For the clients in a host auto-failover landscape, the use of virtual IP addresses is recommended. In the secure user store of the SAP HANA client (hdbuserstore), user logon information can be securely stored, including passwords, using the SAP NetWeaver secure store in the file system (SSFS) functionality. This allows client programs to connect to the database without having to enter a password explicitly.

The hdbuserstore can also be used to configure failover support for application servers (for example, for SAP BW) by storing a list of all (virtual) host names to which the application server can connect. All nodes that are master candidates should be added to the hdbuserstore. Please refer to SAP Note

\textsuperscript{10} In computer networking 10 gigabit Ethernet (10GE or 10GbE or 10 GigE) refers to various technologies for transmitting Ethernet frames at a rate of 10 gigabits per second.
Client reconnect in SAP HANA system replication

Even after a takeover was executed, the client or application server needs to be able to continuously reach the SAP HANA system, no matter which site is currently the primary site.

There are several ways to prepare for the client reconnect:

- **IP redirection**: A virtual IP address is assigned to the virtual host name. In the event of a takeover, the virtual IP unbinds from the network adapter of the primary system and binds to the adapter on the secondary system.

- **DNS redirection**: In this scenario, the IP address for the host name in the DNS is changed from the address of the primary system to the address of the secondary system.

And there are several methods to automatically perform the client reconnect, all of which have their advantages. Which one you use will be determined by corporate IT policies as well as the existing configuration and infrastructure.

- **Cluster Management Software**: External cluster management software can be used to perform the client reconnect after takeover. Some of SAP’s hardware partners are currently working on or already offer an integration of SAP HANA high availability in their cluster management solutions.

- **Takeover Hooks**: They are provided by SAP HANA in the form of a Python script template. Pre- and post-takeover actions are implemented in this script, which are then executed by the name server before or after the takeover. One of the actions could be rebinding the IP addresses. A description of the takeover hooks can be found in the [SAP HANA Administration Guide](https://help.sap.com). If there are no existing constraints, IP redirection has the benefit of being faster to process in a script rather than synchronizing changes of DNS entries over a global network. One way to do this is described in the next section. See also the [SAP HANA High Availability White Paper](https://help.sap.com) and the [SAP HANA Administration Guide](https://help.sap.com) for client reconnect information.

**IP redirection (or Virtual IP)**

Connections from database clients that were configured to reach the primary system need to be "diverted" to the secondary system after a takeover. As shown in the following pictures, an additional "logical" (virtual) hostname with its own separate logical IP address must be defined, and then initially mapped to the L2 MAC address of the original host in the primary system.

---

11 As mentioned above, these hooks are extended so that they also can be used in host auto-failover landscapes. They will be called „HA/DR Providers“ and also offer a Python script template which can be filled with pre- and post-takeover actions.

12 Special care must be taken if the secondary is activated with a takeover but the original primary should continue working as the productive system (for example, if system replication is used to create a system copy). Only cluster management software can decide if the new primary should indeed run as the new primary.
Virtual host names for SQL client access

As part of the takeover procedure, a script is executed which re-maps the unchanged virtual IP address to its corresponding takeover host in the secondary system. This has the advantages that recovery times are shorter and that no special client-side configuration is necessary.

Takeover and SQL client reconnect

A script performing the IP address redirection could look like this:

1. `ip addr del 10.0.1.1 eth0`
   `ip addr del 10.0.1.2 eth0`
   `ip addr del 10.0.1.3 eth0`
2. `drop arp cache`
3. `hdbnsutil -sr_takeover (wait for system to be ready)`
4. `ip addr add 10.0.1.1 eth0`
   `ip addr add 10.0.1.2 eth0`
   `ip addr add 10.0.1.3 eth0`

Alternatively, a script could use this command: `ifconfig eth0:1 10.0.1.1`
The SAP Host Agent could also be used to rebind a virtual IP address. As root user, you will have to execute the following:

```
/usr/sap/hostctrl/exe/saphostctrl -function ACOSPrepare -op ifup -iface eth0 -vhost hanahaerp -nmask 255.255.252.0
```

**Connectivity suspend of the application server**

For short maintenance tasks, a takeover to the secondary site can be performed without interrupting the SAP NetWeaver application server. This is possible with the “Connectivity Suspend” feature that provides real zero downtime maintenance. Long-running transactions continue to run after the takeover without the switch of sites being noticeable. For more information on “Connectivity Suspend”, please refer to SAP Note 1913302 - Suspend DB connections for short maintenance tasks. For near zero downtime maintenance of a system running SAP HANA system replication, please refer to the SAP HANA Administration Guide.

**Client reconnect for SAP HANA XS applications (http/https)**

As mentioned above in the section about HTTP client communication, SAP HANA requires an external load balancer. The load balancer can be either the SAP Web Dispatcher or a third-party tool. It must be able to retrieve the topology information from a list of possible hosts. This list of host names needs to be configured at the load balancer, which only reports an error if all the hosts in the list are unavailable and as long as one load balancer host can still be accessed.

The following picture shows a way to make the SAP Web Dispatcher – used as the external load balancer in this example – takeover-safe, in the sense that new hosts are found after a takeover to the secondary site. It is very similar to the option described above for SQL clients, where IP redirection is used.

\[13\] Help regarding the usage of the saphostctrl web method ACOSPrepare is provided with this command: `/usr/sap/hostctrl/exe/saphostctrl -help ACOSPrepare`
Virtual host names for HTTP client access

Similar to the client libraries, the SAP Web Dispatcher has a configuration parameter (\texttt{wdisp/system = XSSRV=...}) that contains the connect strings to available SAP HANA XS servers for the initial connection. This configuration parameter provides the SAP Web Dispatcher with a list of all available SAP HANA XS servers. The SAP HANA XS server returns a list of internal host names because the local web dispatcher is part of the internal host network (and not of the public network used by the clients).

**Recommendations for the Internal Zone Networks**

10 Gbit/s non-blocking switches are required for the SAP BW internode, storage, and system replication networks as they have an available data rate which is higher than the maximum possible data traffic; each port can handle the full data transfer rate assigned to it at any time. It must be ensured that no links in the SAP HANA system are over-subscribed and that no bottlenecks arise.

**Internode network**

For the SAP HANA internode network, one fully redundant 10GbE network is required for the node-to-node communication of the SAP HANA processes. The internal network requires separate network interface cards that are exclusively configured as part of a private network, using separate IP addresses and ports. The customer’s high-availability requirements determine if and how to apply redundancy to the different SAP HANA network segments, but a configuration using separate VLAN with fully redundant switches – as described above – is strongly recommended.

The \textit{HW Configuration Check Tool} (documentation attached to \texttt{SAP Note 1943937 - Hardware Configuration Check Tool – Central Note}) provides tests and reports for new single-host and distributed systems to determine if the hardware you intend to use meets the minimum performance criteria required to run SAP HANA in production. Two tests are part of the network test package – one measuring the throughput in one direction and the other measuring the throughput in both directions. The following internode network KPIs were measured with this tool indicating the minimum bandwidth:

- 9.5Gbit/s for single-stream test (throughput in one direction)
- 9.0Gbit/s for duplex-stream test (throughput in both directions, 2 x 9Gbit/s)
Internal host name resolution

If nothing else is configured during the installation of SAP HANA, the operating system host names (hostname -f will show the FQDN\(^{14}\)) are used – called internal host names. For all communication between SAP HANA services (index server, name server, and so on), internal host names are used.

You can also configure alternative host names – called virtual host names. These must be resolvable during the installation and later during SAP HANA operations. This is achieved by adding a hostname-to-address mapping for the TCP/IP subsystem for all hosts and on all hosts of a scale-out SAP HANA database to the operating system file /etc/hosts or to the Domain Name System (DNS). How to use virtual hostnames during installation is described in the SAP HANA Server Installation Guide. This way, the virtual host names will be used as the internal host names of the SAP HANA database.\(^{15}\)

The SAP HANA database must also be configured to use a separate internal network definition in a distributed landscape for inter-service communication. Internal host name resolution can be configured with a dedicated internal network during installation, using the following option with the hdblcm tool:

```
hdblcm ... --internal_network=192.168.1.0/20
```

In addition, you will need to set the ini file parameter internal_hostname_resolution manually at a later point in time. Once this definition has been made, the SAP HANA services will only listen on this interface if the listeninterface is specified as “internal” in the global.ini file of the system:

```
[communication]
listeninterface=internal
[
[internal_hostname_resolution]
192.168.1.1-host1
192.168.1.2-host2
192.168.1.3-host3
```

Please see the SAP HANA Master Guide where these network-specific SAP HANA settings are described in greater detail.

System replication network

Basically, the same principles apply to the internode network as to the network used by SAP HANA system replication to replicate data to the second data center. A 10GbE bandwidth connection which is configured as a separate VLAN with redundant switches should connect all relevant nodes with each other.

Since SAP HANA system replication is a solution that involves the transfer of large amounts of information across significant geographic distances, the limitations in Wide Area Networks (WAN)

---

\(^{14}\) Fully Qualified Domain Name

\(^{15}\) The internal hostnames of an SAP HANA database can be identified e. g. by checking this path on operating system level: /usr/sap/<SID>/HDB<n>/hostname/sapprofile.ini. Also all SAP HANA system views containing a HOST column show these internal host names, e. g. check M_DATABASE with SQL.
technology will influence the decision on whether you choose synchronous or asynchronous replication.

The following factors of the WAN between two data centers must be considered when deciding on the SAP HANA system replication method to use.

**Bandwidth**

Bandwidth in computer networking refers to the data rate supported by a network connection, which is commonly expressed as bits per second (bps). It influences the data replication speed and thus – at least in synchronous replication – the performance of writing transactions on the primary site.

**Latency**

Network latency is defined as the time delay observed as data transmits from one point to another. Latency can easily be determined by the round-trip time and can be measured with the help of the SAP Niping tool (described in SAP Note 1100926 - FAQ Network Performance). Latency depends on the speed of the transmission medium (for example, copper wire, optical fiber or radio waves) and the delays in the processing from devices along the way (for example, routers and modems). A low latency indicates high network efficiency. The latency between the data centers limits the possible protection level (for example, encryption) for business data, and thus influences the decision regarding data center locations.

**Packet Loss and Delivery Errors**

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination, which also influences the required technical setup in the data center(s) for disaster recovery and the data replication architecture. One important remark: The MTU size configuration must correspond to the available network capacity for the SAP HANA system replication network connection all the way from the primary to the secondary data center! Otherwise, problems could occur during configuration of SAP HANA system replication (such as hanging services after initial registration of the secondary site).

There is no straightforward recommendation regarding the bandwidth and the latency a system replication network must provide. A rough estimation of the required performance is given in the How-to Guide Network Required for SAP HANA System Replication, which is referred to from the SAP Note 2407186 - How-To Guides & Whitepapers For SAP HANA High Availability. It describes that the

---

16 Maximum Transmission Unit (MTU) describes the maximal packet size (in bytes) of one protocol of the network layer (layer 3) of the OSI model. The setting can be checked on OS level with "ifconfig".
network used for SAP HANA system replication must meet the following two minimal requirements regarding throughput and latency:

- **Throughput**: It must be possible to transport the size of the persistently stored data within one day from the primary to the secondary data center.
- **Latency**: The redo log shipping time for 4 KB log buffers must be less than a millisecond or in a low single-digit millisecond range – depending on the application requirements (relevant for synchronous replication only).

A network connection of 10Gbit/s between data centers is recommended by SAP.

**System replication host name resolution**

A separate network for system replication can be defined in the SAP HANA ini parameters. This is recommended to prevent the use of a public network for replication and to meet security and performance requirements. The following picture shows an example of a scaled-out SAP HANA database using a separate internode network (described above) and a separate network for the SAP HANA system replication traffic.

![Diagram of SAP HANA system replication network](image.png)

*Multihost SAP HANA system replication over a separate network with a separate internal network on each site*
The changes regarding the network used by SAP HANA system replication to the `global.ini` must be done prior to registering the secondary site, because `-sr_register` uses this mapping.

On both sites, virtual host names are used without the need to adapt `/etc/hosts` entries accordingly; this is since the host names used must be unique across data center boundaries; that is, no internal host name on the primary site is allowed as a host name on the secondary site. The `global.ini` file must be changed as follows:

```ini
[system_replication_hostname_resolution]
/IP-address_host1_other_site=<internal_host1_other_site>
/IP-address_host2_other_site=<internal_host2_other_site>
...
```

The section `[system_replication_hostname_resolution]` only contains hosts from other sites. For multitier system replication configurations, only direct neighbors need to be added.

Further details on SAP HANA network setups are given in the SAP HANA Master Guide. For security topics like SSH encryptions of the network connections, please refer to the SAP HANA Security Guide.

**Recommendations for the Storage Zone Networks**

The required bandwidth for the storage network is ≥ 10 GbE for Ethernet for NAS and ≥ 8 GbE for FibreChannel in SANs. SAP recommends configuring the network with full redundancy. It is also important that the storage network used to access the data and log volumes of the SAP HANA databases are separated from the backup storage network where data backups and log backups are stored. Otherwise, creating a data backup could impact the performance of write transactions on the SAP HANA database.

In addition, the SAP HANA NFS network for the shared directory `/hana/shared` should be in a fully redundant 10GbE network. Every node in the cluster must be able to access this shared resource for the SAP HANA binaries. However, public access should be prohibited.

If GPFS is used, the recommendations for the internode network apply because the disks holding the clustered file systems are locally attached to the SAP HANA nodes.

For more information about SAP HANA storage requirements, please see the SAP HANA Storage Requirements whitepaper (PDF attachment to SAP Note190082).

**4 Summary**

SAP HANA supports a wide range of possibilities for network configuration. Various setups can be employed depending on the system landscape at the customer site. Single-host systems, distributed landscapes and high availability/data recovery (HA/DR) setups pose different questions and require different decisions with regards to the client zone, the internal zone, and the storage zone.

The sizing of the network depends largely on the load on the system and the system landscape. If a disaster recovery solution (system or storage replication) is added to the overall system, the network requirements need to be considered very carefully because the performance of the primary system
as well as business continuity could be impacted. The performance requirements that have to be fulfilled by the network depend mainly on the workload that is running on the SAP HANA database.

Network security and segmentation are functions provided by the network switch vendor and need to be configured accordingly.

5 References

SAP HANA official documentation

SAP HANA Administration Guide
SAP HANA High Availability White Paper
SAP HANA Tailored Data Center Integration
SAP HANA Security Guide
SAP HANA Server Installation Guide

SAP Notes

SAP Note 190823 - SAP HANA Storage Connector API
SAP Note 1930853 - HDBUserStore contains too many SAP HANA nodes
SAP Note 1913302 - Suspend DB connections for short maintenance tasks
SAP Note 1943937 - Hardware Configuration Check Tool – Central Note
SAP Note 1100926 - FAQ Network Performance
SAP Note 1999880 - FAQ: SAP HANA system replication
SAP Note 2407186 - How-To Guides & Whitepapers For SAP HANA High Availability