VERITAS

Veritas Alta Application Resiliency for SAP NetWeaver /S/4HANA in Microsoft Azure

High Availability and Disaster Recovery Reference Architecture

SAP® Certified
Integration with SAP NetWeaver®

SAP® Certified
Integration with SAP S/4HANA®

VERITAS ALTA™

White Paper | February 2023

Contents

Abstract

An ever-increasing number of organizations are transitioning their mission-critical applications and services to run not just on-premises but in the public cloud as well. Nowhere is this more evident than with solutions such as SAP NetWeaver / S/4HANA and SAP HANA, which when combined represent nearly 25% of the global ERP market share.

As organizations seek to expand their SAP NetWeaver /S/4HANA footprint in the public cloud, the need to address and ultimately improve its availability becomes of paramount importance. While seemingly adequate for most outage scenarios, when a failure event does in fact occur, the recovery process requires multiple manual steps to failover, reverse the replication as well as perform a failback. In addition there is no virtual IP or integrated HA failover orchestration with SAP Central services or components. This process is timely and prone to human error both of which involves server downtime and inevitably leads to loss of revenue opportunities and a potential impact to your business reputation.

The purpose of this document is to provide the necessary guidance for implementing a highly available SAP NetWeaver / S/4HANA environment in the Azure cloud using Veritas Alta™ Application Resiliency.

It is intended for the following audiences:

- Organizations who deploy SAP systems on Microsoft Azure for development, testing, training, sandboxing, demonstration, or production purposes and want to monitor and manage SAP NetWeaver / S/4HANA solutions for high availability and disaster recovery
- SAP basis and SAP implementation consultants who are familiar with Microsoft Azure and want to manage the availability of the SAP Landscape in Microsoft Azure using Veritas Alta Application Resiliency
- This document does not replace any standard SAP documentation or Microsoft Azure documentation. For information on basic SAP high availability configurations in Azure, refer to the Microsoft Azure documentation at: https://learn.microsoft.com/en-us/azure/sap/large-instances/hana-overview-high-availability-disaster-recovery
- https://docs.microsoft.com/en-us/azure/virtual-machines/workloads/sap/sap-hana-high-availability

When installing SAP solutions on Azure, always refer to the standard SAP documentation and notes for the respective SAP solution.

For more information about SAP on Azure, refer to the Microsoft Azure documentation at:

https://docs.microsoft.com/en-us/azure/virtual-machines/workloads/sap/sap-hana-availability-overview

Introduction to Veritas Alta Application Resiliency

Veritas Alta Application Resiliency is a new cloud-focused offering that is based on InfoScale which is a leading solution for application high availability and storage management with over 30 years of innovation and market leadership in both Software-Defined Storage, application aware resiliency and disaster recovery. Combining intelligent volume management, an advanced high-performance shared file system and application aware system clustering, Veritas Alta Application Resiliency is responsible for protecting the world's most mission-critical applications and databases across multiple industry verticals. Used extensively in the financial sector, healthcare and the public sector, it enables customers to rapidly deploy highly available, performant, multi-tier IT business services on nearly any type of infrastructure, operating system, platform, or underlying storage and compute infrastructure. Moreover, it provides extensive integration with SAP NetWeaver /S/4HANA and SAP HANA database environments, with an emphasis on minimizing downtime, ensuring data integrity, achieving linear scale and simplifying with automation.

When considering whether or not to deploy Veritas Alta Application Resiliency within the Azure public cloud, you'll want to recognize that we provide not only an intuitive configuration model, with inclusion in the Azure Marketplace, but a more granular, application-centric view of your critical services. As part of Azure's Shared Responsibility model, Azure addresses the potential for infrastructure outages only, if applications are installed across multiple Availability Zones (AZ's) with 99.99% uptime. The customers part of Azure's shared responsibility model is to ensure application availability which necessitates a dependency upon 3rd party clustering solutions. With Veritas Alta Application Resiliency, you gain out-of-the-box availability support for all SAP HANA and S/4HANA components while simultaneously benefiting from the resilience of the Azure infrastructure.

Veritas Alta Application Resiliency protects the following critical SAP components, ensuring overall application availability in a distributed SAP environment

- Databases
    - o SAP HANA DB
    - o Oracle RDBMS
    - o SAP MAxDB
    - o SAP Sybase ASE
    - o IBM DB2
    - o Microsoft SQL server
- Central Services instance (ENQUEUE)
- Enqueue replication server (ERS)
- Primary application server (PAS)
- Additional application servers (AAS)

As an example, by itself SAP Central services are installed on one instance at a time and are therefore considered single points of failure (SPOF). Since multiple SAP application server (dialog) instances can be configured to run in parallel, they do not form a SPOF. However, when an application deployed in the same AZ or across AZs fails, Microsoft Azure restarts only the application VM instances or redeploys the instance where the application has failed. This impacts the overall Recovery Time Objective (RTO). In order to achieve the demanding Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for mission critical environments, Veritas Alta Application Resiliency ensures the proper failover of all SAP components to a designated or alternate Azure instance on which the application can reside for an RTO of under one-minute and an RPO of zero.

In order to monitor critical applications organizations often resort to OS-specific or customized scripts. To make this easier Veritas Alta Application Resiliency comes with the largest catalog of pre-built enterprise agents that simplify such deployments, thereby eliminating the need for custom tools. With intelligent failover capabilities, organizations can reduce the cost of redeploying instances by reducing the number of standby or passive servers within Azure by using cost effective N + 1 and N-to-N failover configurations.

By providing a packaged solution Veritas Alta Application Resiliency makes it simple and fast to configure high-availability (HA) and disaster recovery (DR) for critical SAP workloads. Moreover, the need for non-disruptive recovery validation across Azure regions can be met with Veritas Alta Application Resiliency's FireDrill DR testing capability.

In addition, Veritas Alta Application Resiliency provides agents for each of the following application and infrastructure components:

- SAP NetWeaver /S/4HANA (SAPNW)
- SAP HANA (SAPHDB)
- SAP Components (SAP Components)
- Microsoft Azure IP (Azure IP)
- Microsoft Azure Route (AzureDNSZone)

Types of Veritas Alta Application Resiliency configurations

The following graphic depicts various availability and recovery configurations created using Veritas Alta Application Resiliency:

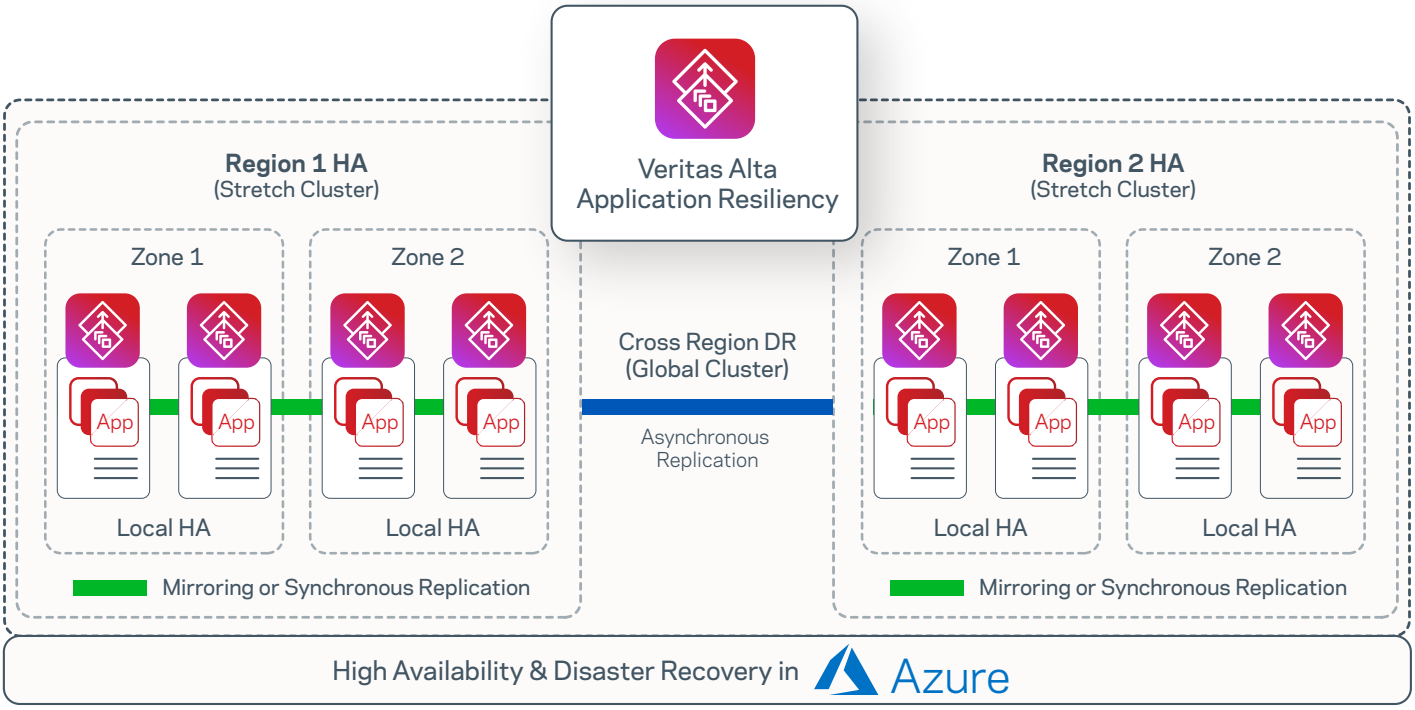


Figure 1. Veritas Alta Application Resiliency HA and DR Configurations

Veritas Alta Application Resiliency Capabilities for SAP Ecosystems

The following HA and DR capabilities of Veritas Alta Application Resiliency makes it ideal for managing an SAP ecosystem in Azure:

- Business continuity with minimal application downtime during failures through complete automation for the SAP landscape
- Optimal server utilization due to cost-effective failover configurations for development, testing, or production environments
- Support for cost optimization, Recovery Point Objective (RPO), and Recovery Time Objective (RTO) requirements for SAP workloads in Microsoft Azure
- Failover between on-premises data centers and Microsoft Azure
- Failover between Microsoft Azure availability zones (AZ)
- Failover between Microsoft Azure regions
- Failover between Azure and other cloud service providers

- SAP agents that provide:
  - A similar customer experience both on-premises and in Microsoft Azure
  - Flexible Storage Sharing (FSS) for data sharing in Microsoft Azure across instances
  - Replication across Microsoft Azure AZs and regions using Veritas Volume Replicator

About Veritas Virtual Business Services (VBS)

IT services are no longer standalone applications running on single servers. Business services or multi-tier applications like SAP Business Suite applications make up most of an IT organization's critical workloads, with different components of the application running on different tiers of infrastructure, each with their own unique availability requirements. A failure in any tier can bring down the entire business service and managing the recovery is time consuming and complex. Virtual Business Services are aware of the complete business service and takes the appropriate action in the event of a failure to restore the entire service. When an individual component fails, Virtual Business Service provides automated orchestration of the connections to other computing resources, within an availability zone, across availability zones or even across regions. This means faster recovery and minimal downtime–with no manual intervention.

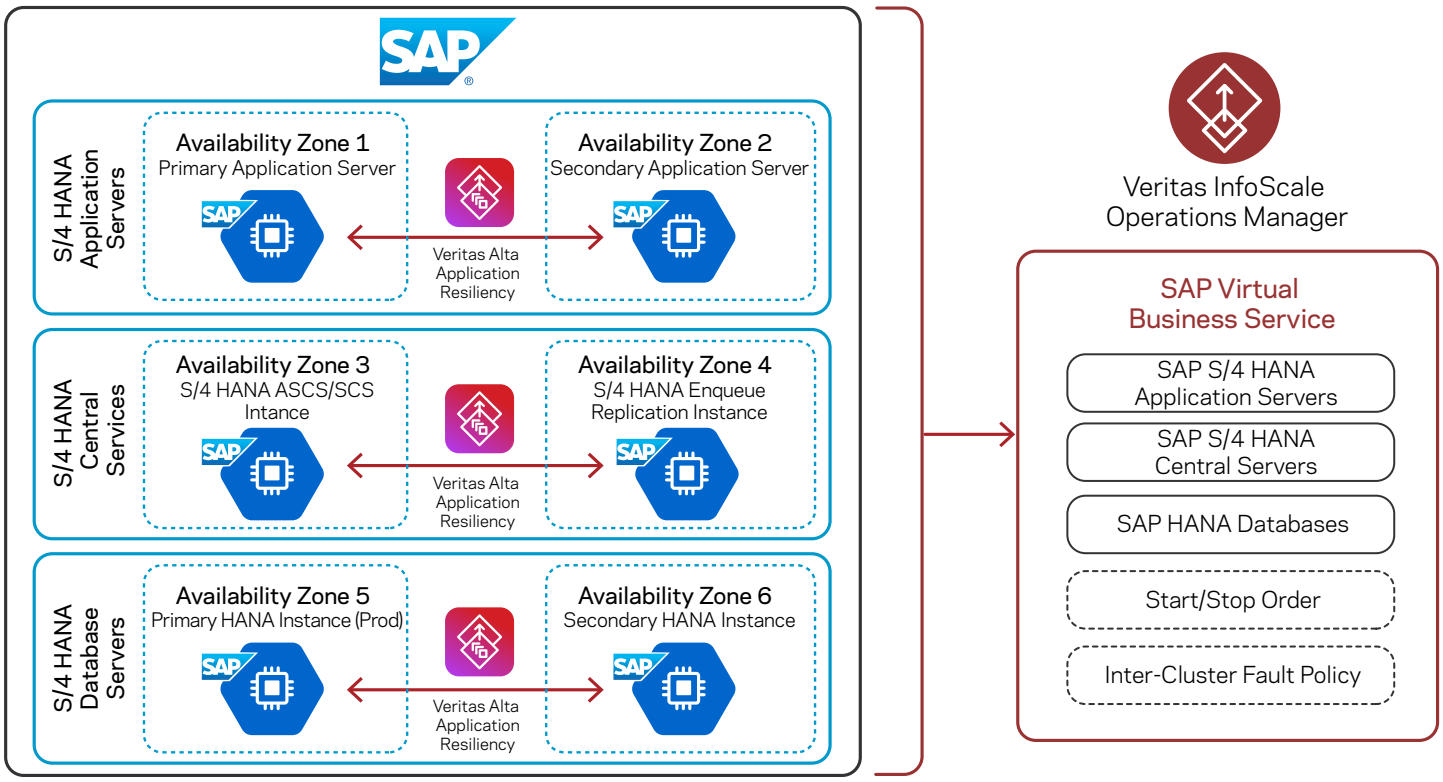


Figure 2. Sample VBS Architecture

Flexible Storage Sharing Feature of Veritas Alta Application Resiliency

Veritas Alta Application Resiliency's FSS feature combines a distributed, high-performance, and highly available file system with the latest cloud storage and networking technologies. FSS lets you unlock the potential of Direct Attached Azure managed disks, without sacrificing performance or availability. With FSS, you can use Microsoft Azure block storage services to create a highly available shared storage cluster in the cloud that provides high performance and resiliency for your critical applications.

Note: FSS supports all Azure storage volumes and can be used for SAP NetWeaver / S/4HANA Application server instance mounts like sapmnt, trans, SAP Central Service instance (ENQUEUE) and Enqueue Replication instance (ERS) mounts for fast failover over and high availability. FSS is not yet certified by SAP for the SAP HANA DB.

For details, see the Veritas FSS datasheet at: https://www.veritas.com/content/dam/www/en_us/documents/data-sheet/DS_alta_shared_storage_V1801.pdf

Replication in Veritas Alta Application Resiliency

Veritas Alta Application Resiliency includes Veritas Volume Replicator (VVR) which is a software-based data replication solution designed to contribute to an effective disaster recovery plan. VVR enables you to maintain a consistent copy of application data at one or more availability zones or regions.

VVR benefits from the robustness, ease of use, and high performance of Veritas Volume Manager (VxVM), and at the same time, adds replication capability to VxVM. It can replicate existing VxVM configurations, and can be transparently configured while the application is active.

VVR replicates the application writes on the volumes at the source AZ to one or more alternate AZ or region. It provides a consistent copy of application data at the remote locations. If a disaster occurs at the source location, you can use that copy to simply restart the application at the alternate AZ or region.

The system on which the application is running at the source location is called the Primary system, and the system at the target location is called the Secondary system.

The volumes on the Primary system must be initially synchronized with the volumes on the Secondary system. VVR lets you initialize the application data between the primary location and the secondary location using your IP network.

Considerations for Using FSS or VVR across Availability Zones

It's important to take the following considerations into account when using FSS or VVR across AZs:

- FSS can be used in active-active applications where the application can access the data on both AZs simultaneously. VVR cannot be used for active-active applications
- When either FSS or VVR synchronous replication is used, the application throughput depends on the network characteristics, because the data needs to be mirrored or synchronized to the other AZ.
- For applications that can sustain some increase in RPO but need high throughput, Veritas recommends using VVR asynchronous replication.
- FSS can be used in Azure to provide a shared storage environment to the applications running on multiple nodes in a cluster.
- VVR can be used for replication across regions in Azure.

High Availability SAP Agents

Veritas Alta Application Resiliency provides a number of SAP specific high availability agents which can be found here: https://sort.veritas.com/agents.

Veritas Cluster Server Agent for SAP NetWeaver / S/4HANA

The Veritas SAPNW agent is a certified Cluster Server agent from the SAP ICC program. The Cluster Server agent for SAP NetWeaver / S/4HANA (SAPNW) provides high availability for SAP NetWeaver / S/4HANA instances. The agent can monitor and manage the status (online/offline) of an NetWeaver / S/4HANA instance. It also monitors the system processes and the server state and shuts down the instance in case of a failover.

The SAPNW agent supports the following NetWeaver / S/4HANA features:

- Fast Failover of faulted Instances within an AZ
- Applications instance failover in case of an AZ failover
- Auto-restart of an SAP NetWeaver / S/4HANA instance before takeover
- In-depth monitoring and Intelligent Monitoring Framework (IMF) support
- Support for in-depth TRACE and Debug Log levels for troubleshooting

Veritas Alta Application Resiliency integration with SAP library and the Veritas connector script

The SAP NetWeaver agent enables the integration of Veritas Alta Application Resiliency with SAP NetWeaver (7.x or later) and SAP Kernel (7.20 x or later) DCK. For this purpose, it uses an SAP-provided library (saphascriptco.so) and a Veritas provided cluster connector script (sap_symc_cluster_connector). This integration enables the SAP sapstartsrv component to communicate SAP instance status changes that are made by SAP clients to Veritas Alta Application Resiliency.

In a typical Veritas Alta Application Resiliency cluster, when an SAP administrator changes the status of an SAP instance using an SAP client, such as sapcontrol or startsap, the following events occur:

- When the administrator stops the SAP instance, Veritas Alta Application Resiliency detects a fault and performs the clean operation
- When the administrator starts the SAP instance, Veritas Alta Application Resiliency detects that the instance is brought online outside of its control

You must enable communication between sapstartsrv and Veritas Alta Application Resiliency. Doing so ensures that sapstartsrv can inform when an SAP client is used to start or stop an assigned SAP instance. Veritas Alta Application Resiliency can then detect the correct status of the SAP instance.

ENSA2 Support:

Under high availability it is mandatory that the old mechanism of Standalone Enqueue Server (ENSA1) has to fail over to the cluster node where the active ERS is running to acquire the replicated enqueue table which resides in the shared memory of the active ERS node.

The new Standalone Enqueue Server 2 and Enqueue Replicator 2 provides an improved high availability architecture with robust, fast replication and failover.

In ENSA2, if the ASCS fails it can start on a separate node in the cluster and copy the lock entries from the enqueue replicator 2. It is not mandatory that it fails over to the active ERS2 node.

The Veritas SAPNW agent supports both of the Enqueue replication methods and is certified by SAP.

SystemD Support:

SystemD is a system and service manager for the latest Enterprise Linux operating systems. It manages the application operations in system space. By default, SAP Application servers run in user space (init). As such, the SAP application servers do not stop gracefully during system reboots and this can cause application crashes in high availability systems.

The Veritas SAPNW/SAPHDB agents provide graceful shutdowns of the SAP applications during system reboots.

Veritas agent for SAP HANA

The Cluster Server agents monitors specific resources within an enterprise application. They determine the status of resources and start or stop them based on external events that may affect application availability.

The Cluster Server agent for SAP HANA (SAPHDB) provides high availability for HANA instances where the data is replicated with HANA System Replication. The agent brings a HANA instance online, monitors the instance, and takes the instance offline. It also monitors the system processes and the server state and shuts down the server in case of a failover.

Veritas agent for Microsoft Azure IP

Veritas provides the AZUREIP agent, which lets you monitor and manage the following networking resources in Azure:

- Private IP: A private IP is a private numerical address that networked devices use to communicate with one another
- Azure IP: An Azure IP address is a static IPv4 address designed for dynamic cloud computing, and is associated with your Microsoft Azure account
- Overlay IP: Microsoft Azure allows you to redirect IP address traffic to an Azure instance in a Virtual Private Network (VPC) regardless of the subnet or AZ to which it belongs. An overlay IP lets you fail over IP addresses between cluster nodes when they are spread across multiple subnets or AZs

Veritas also supports the Azure load balancer which enables the movement of virtual IPs between the clustered hosts as an alternative.

Veritas agent for Microsoft AzureDNSZone

Azure DNSZone is a highly available and scalable cloud Domain Name System (DNS) web service. Veritas provides the AzureDNSZone agent to update and monitor the mapping between host names and IP addresses. The agent manages the mapping for the Azure route domain when failing over nodes across subnets. When you create a hosted zone, AzureDNSZone automatically creates a name server (NS) record and a start of authority (SOA) record for the zone.

If the resource records need to be dynamically added and deleted from the Azure route domain during failover, you must use the AzureDNSZone agent. The agent updates the NS with the new resource record mappings during failover and allows the clients to connect to the failed over instance of the application.

Note: If you do not want to use the AzureDNSZone agent, you can continue to use the Veritas DNS agent for managing DNS records.

Typical NetWeaver /S/4HANA Deployment Architecture Configuration Across Availability Zones in Azure

The following two graphics describe the overall deployment of an SAP NetWeaver / S/4HANA application server with an SAP supported database and with SAP HANA in Azure across Availability Zones.

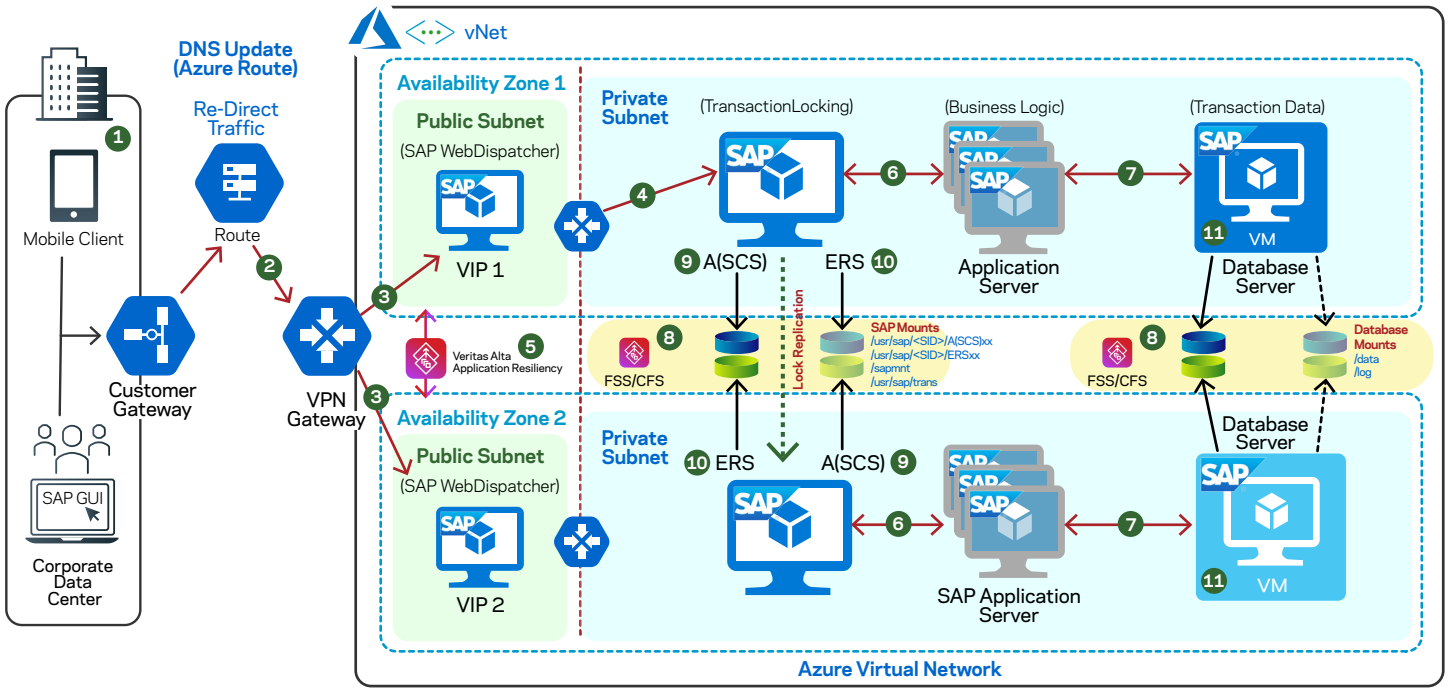


Figure 3. SAP NetWeaver with Non-HANA Databases

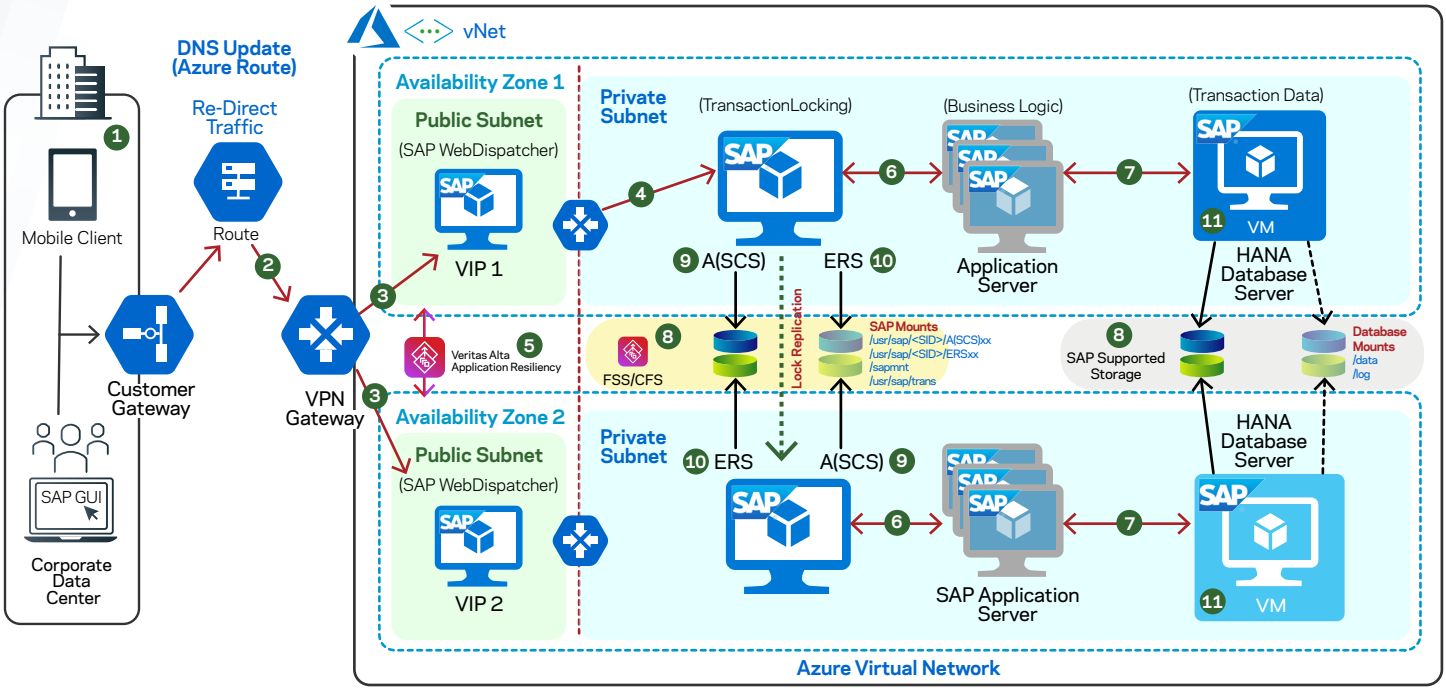


Figure 4. SAP S/4HANA with HANA Database

Note: FSS supports all Azure storage services. VxVM, VxFS, and FSS can be used with S/4HANA / SAP NetWeaver application servers as well as most database management systems, however these features are not currently supported for use with SAP HANA databases.

Both solution architectures illustrate the recommended approach to achieving high availability for SAP NetWeaver / S/4HANA with SAP recommended databases in Azure using Veritas Alta Application Resiliency. High availability for your front-end and middle tier can be obtained by using Azure Load Balancers or Application Gateways. This ensures the uptime SLA of 99.99% for your application and database tiers and shows overall how it's implemented using a combination of Azure Availability Zones and Veritas Alta Application Resiliency.

Data Flow Sequence

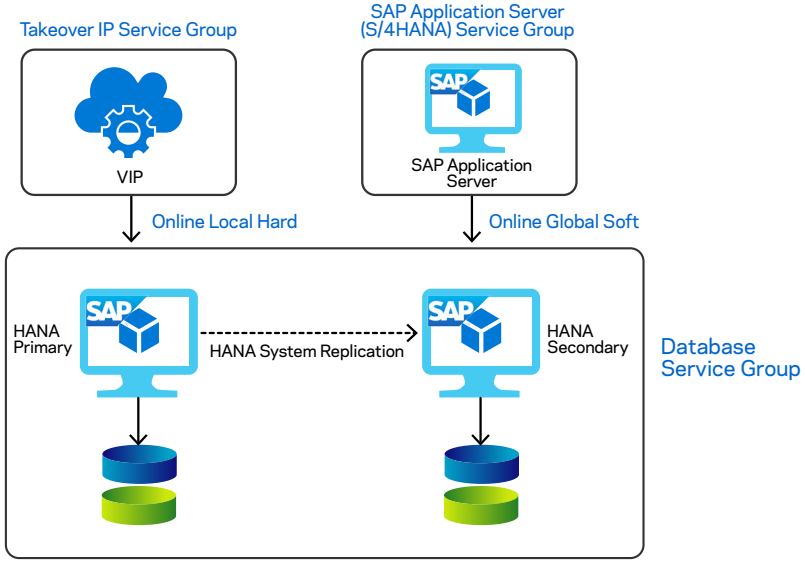
1. In this example, the SAP user executes a request via SAP's NetWeaver / S/4HANA Fiori interface, custom application interface, SAP GUI or others.
2. Azure high-speed express route gateway is used to connect securely from an on-premises network to Azure Virtual Machines and other Azure resources.
3. Web front end (SAP Web Dispatcher) is configured in a load balancer and it connects to the appropriate application server to handle the dialog work.
4. Request flows into the highly available SAP Central Services ASCS(ENQUEUE) and then through SAP application servers running on Azure Virtual Machines in an Azure VM. Availability zones offer a 99.95 percent uptime SLA.
5. Veritas Alta Application Resiliency is configured across VMs under Availability Zones.
6. SAP Central Service Instance ASCS and Replication server are single points of failure that are monitored and controlled by Veritas Alta Application Resiliency to achieve 99.99% SLA.
7. The user request flows into the highly available SAP ABAP SAP Central Services (ASCS), and then through SAP application servers running on Azure Virtual Machines. The request moves from the SAP app server to the database running on an AZ1 high-performance Azure VM.
8. Veritas Alta Application Resiliency manages Azure storage for SAP Central Services,SAP Kernel and database using the Flexible Storage Sharing feature.
9. The Veritas SAPNW agent monitors ASCS instance across AZ1 as active and ERS instance as standby.
10. The Veritas SAPNW agent monitors ERS instances across AZ2 as active and ASCS instance as standby.

11. The primary database is active on Availability Zone1 (AZ1) and secondary/standby on Availability Zone2(AZ2) servers running on SAP certified virtual machines are clustered at the OS level for 99.99% availability using Veritas Alta Application Resiliency. Database replication is handled by Flexible Storage sharing from primary to standby, achieving a zero Recovery Point Objective (RPO).

Note: In addition to configuring the database for HA, DR, or both, you need to ensure that the client applications (ex: the S/4HANA / NetWeaver application server, JDBC, ODBC connection, and so on) can re-establish their connection with the database system after the failover. To do so, you can configure either network-based IP redirection or network-based DNS redirection of your database system. Veritas agents for SAP support end-to-end HA and DR for SAP NetWeaver and SAP S/4HANA.

Common Dependency Between SAP S/4HANA and SAP HANA Databases

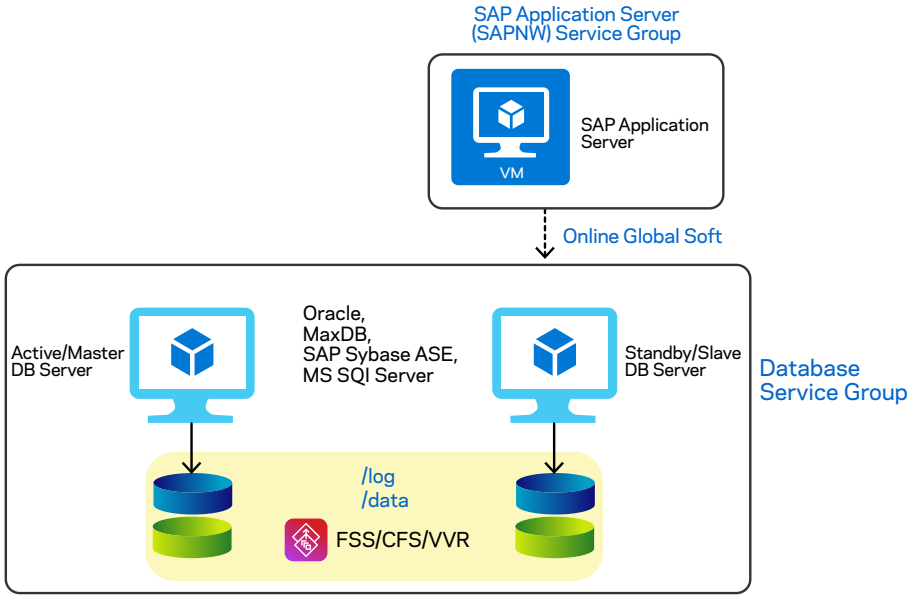
The following graphic depicts the typical dependency between an SAP application and an SAP HANA database:



Note: FSS supports all Azure storage services. VxVM, VxFS, and FSS can be used with S/4HANA / SAP NetWeaver application servers as well as most database management systems, however these features are not currently supported for use with SAP HANA databases.

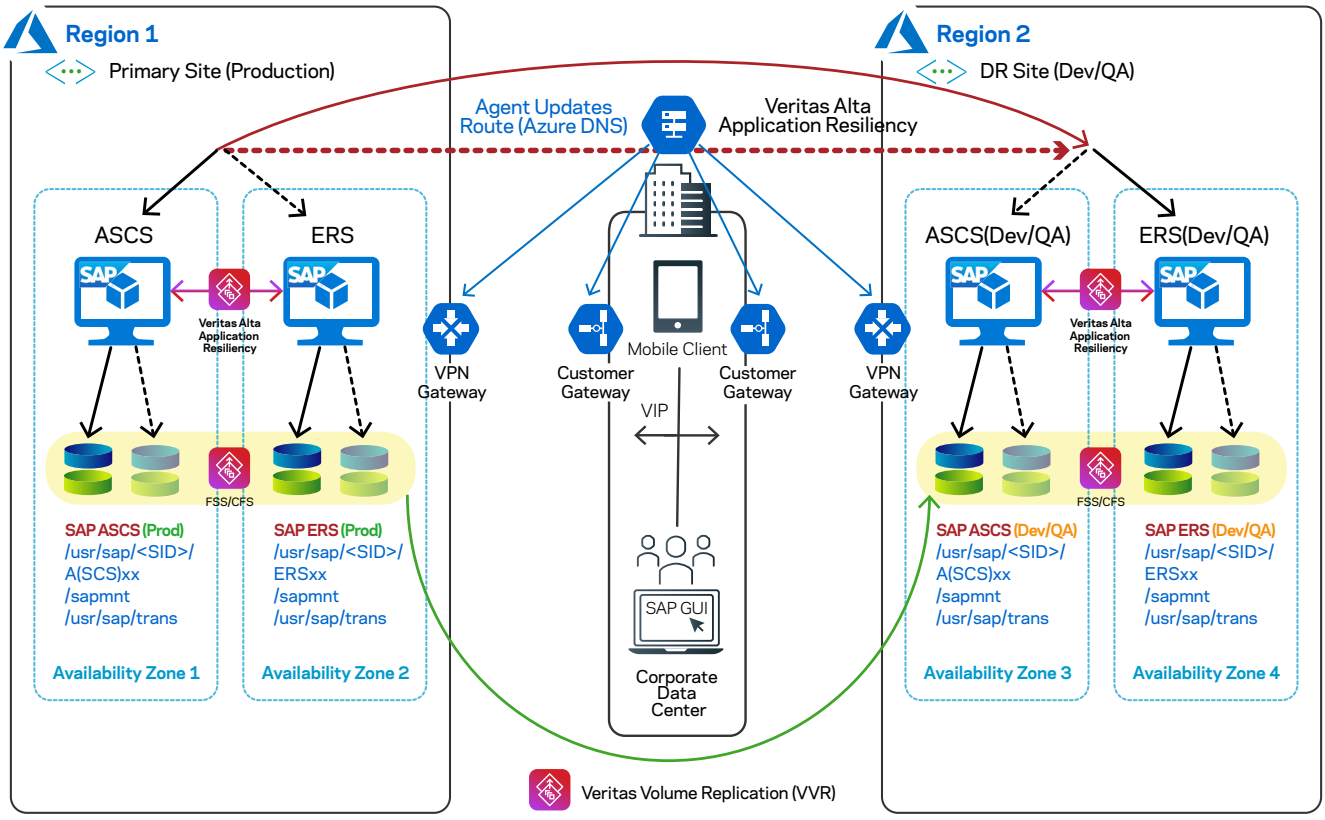
Common Dependency Between SAP NetWeaver and Other Databases

The following graphic depicts the typical dependency between an SAP application and an SAP suported database:



Cost Optimization OF SAP Instances in Azure for SAP NetWeaver / S/4HANA

Microsoft Azure lets you create and optimize SAP instances for development, testing, or production environments. If an SAP production application instance outage occurs, Veritas Alta Application Resiliency fails over the instances between the designated SAP systems without disrupting the client connections. Thus, it reduces the overall Total Cost of Ownership (TCO) in case of a disruption or outage of SAP instances on Azure.



Supported use Cases for SAP NetWeaver / S/4HANA in Azure

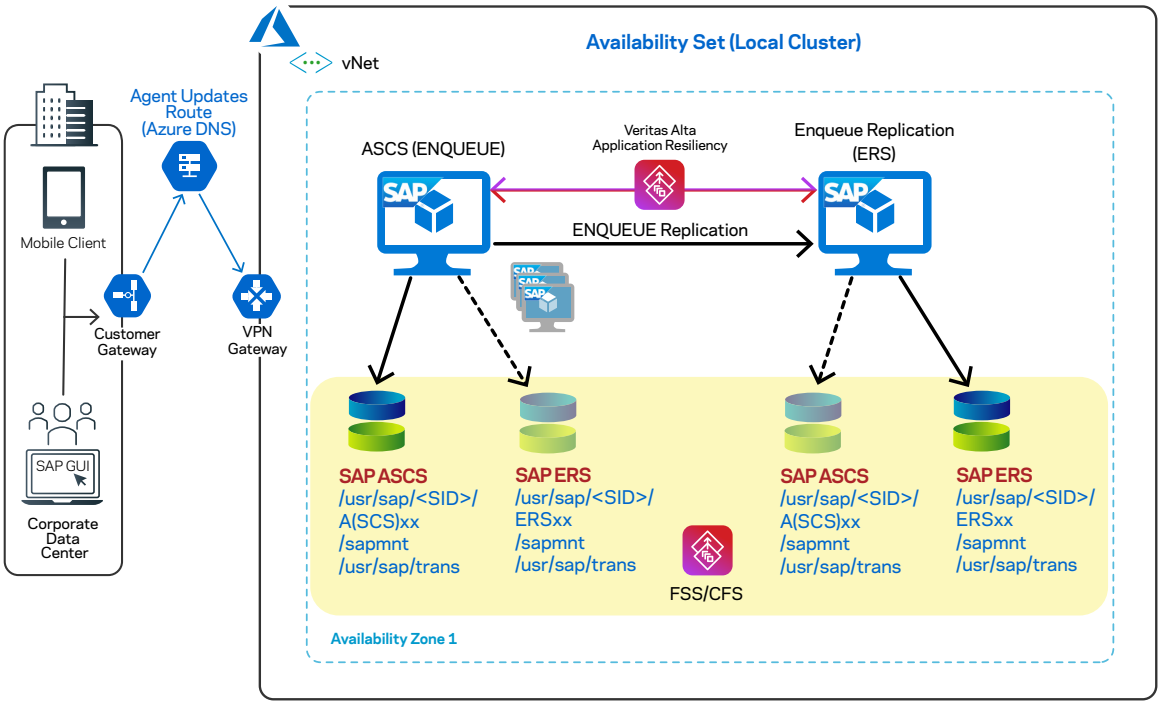
Veritas Alta Application Resiliency can monitor and control SAP NetWeaver / S/4HANA-based application instances in the following scenarios:

- SAP Application instances configured in Azure Availability set(local cluster)
- SAP Application Instances running across AZs (within the same Microsoft Azure region)
- Disaster Recovery between AZs across regions
- On-premises to Azure failover(DR)

SAP NetWeaver / S/4HANA instances on Availability Set

Install and configure an SAP Central Service instance with a virtual host name and ensure that the virtual host name is resolvable from all of the other SAP instance hosts.In this use case enqueue server and enqueue replication server instances exist in the same AZ with availability set.

After you set the enqueuer or the replication parameter to TRUE (enque/server/replication = true), all the enqueue locks are replicated to the enqueue server and are available on the replication server. If the enqueue server instance fails or becomes unavailable, the SAPNW agent detects the fault and automatically triggers the failover of the enqueue server to the enqueue replication server node. Thus, the enqueue replication server is converted to the enqueue server. In this use case, two instances are configured with the SAP standalone enqueue server(ENQUEUE) and the SAP enqueue replication server(ERS).



Note: SAP Application data and sapmnt are mounted and manged with Veritas FSS/CFS,VxVM and VxFS tools.

Note: The failover scenario works as per SAP high availability certification guidelines.

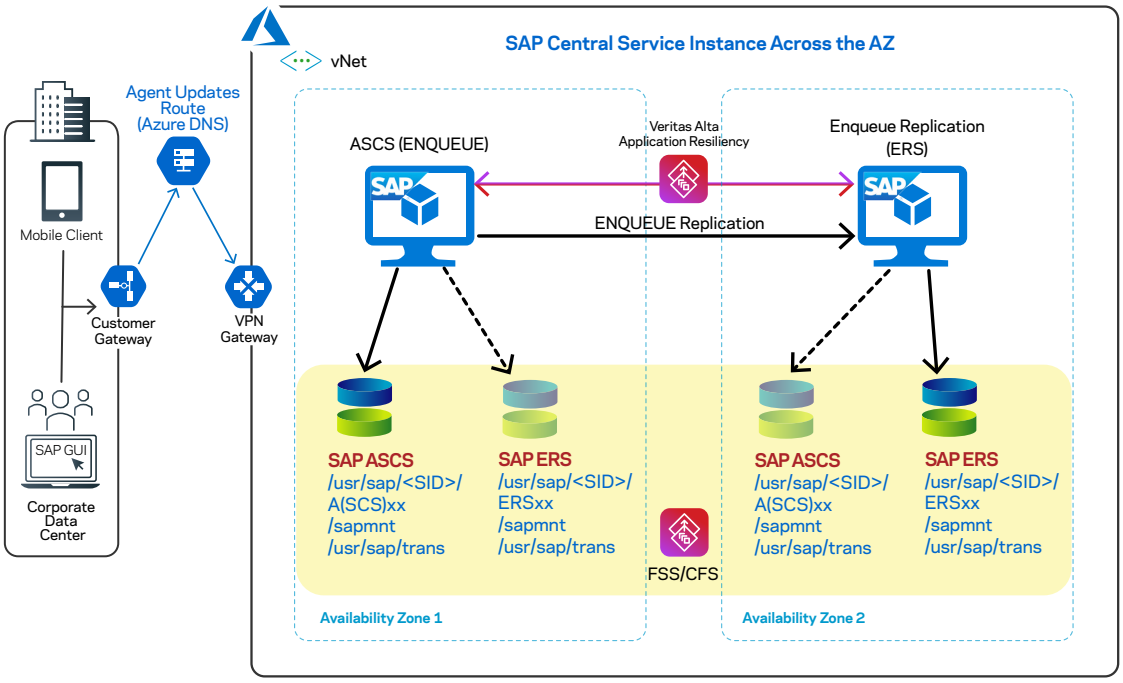
After the fault is cleared and the node is recovered, the enqueue replication server starts replicating back the enqueue locks from the enqueue server.

You can refer to the following link to learn more about availability set:
https://docs.microsoft.com/en-us/azure/virtual-machines/linux/tutorial-availability-sets

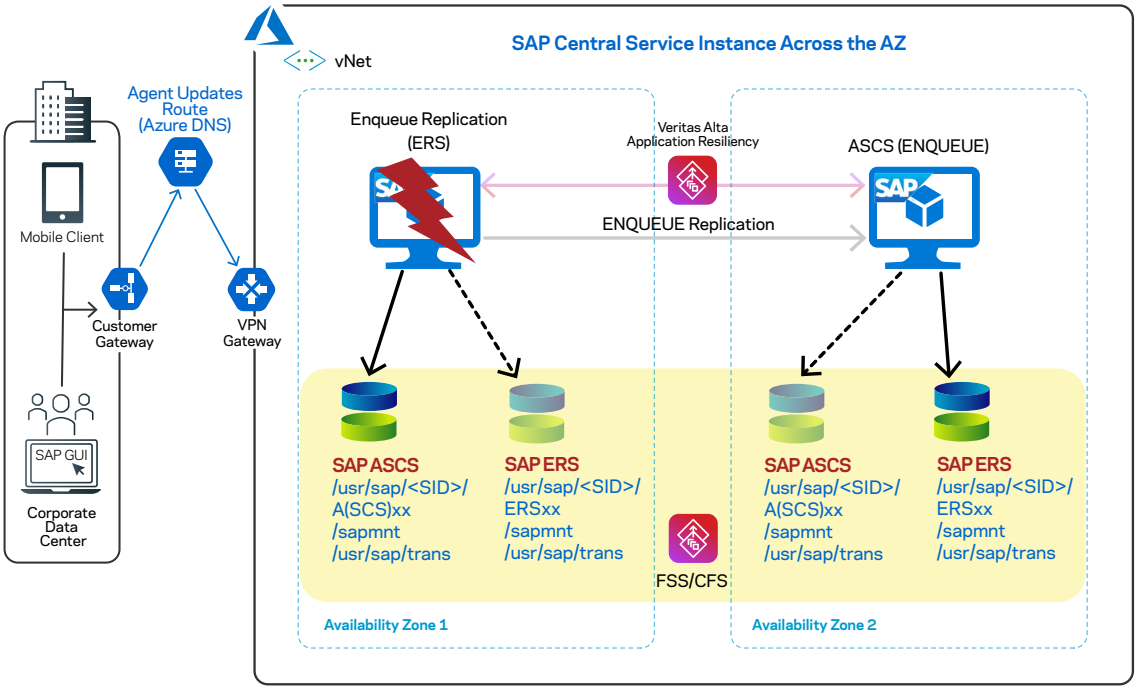
SAP Application server instances across AZs in the same Microsoft Azure region

In this configuration, the ASCS and the ERS instances are configured on different AZs in the same region. When ENQUEUE Replication is enabled between the two instances, all the enqueue locks are replicated to the ERS instance.

In this example, the ASCS and the ERS instances are configured in different AZs with local clustering.

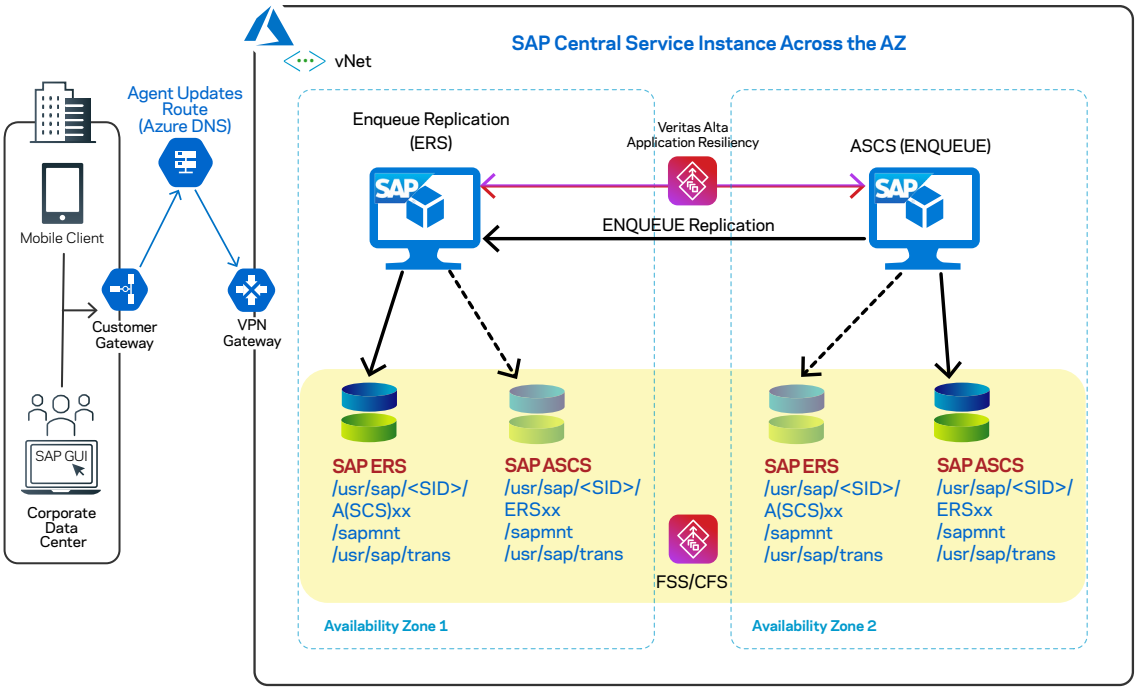


If the ASCS(ENQUEUE) instance fails or becomes unavailable, the SAPNW agent identifies the fault and automatically triggers the failover operation on the ERS instance residing on Availability Zone 2. The following graphic depicts this action:



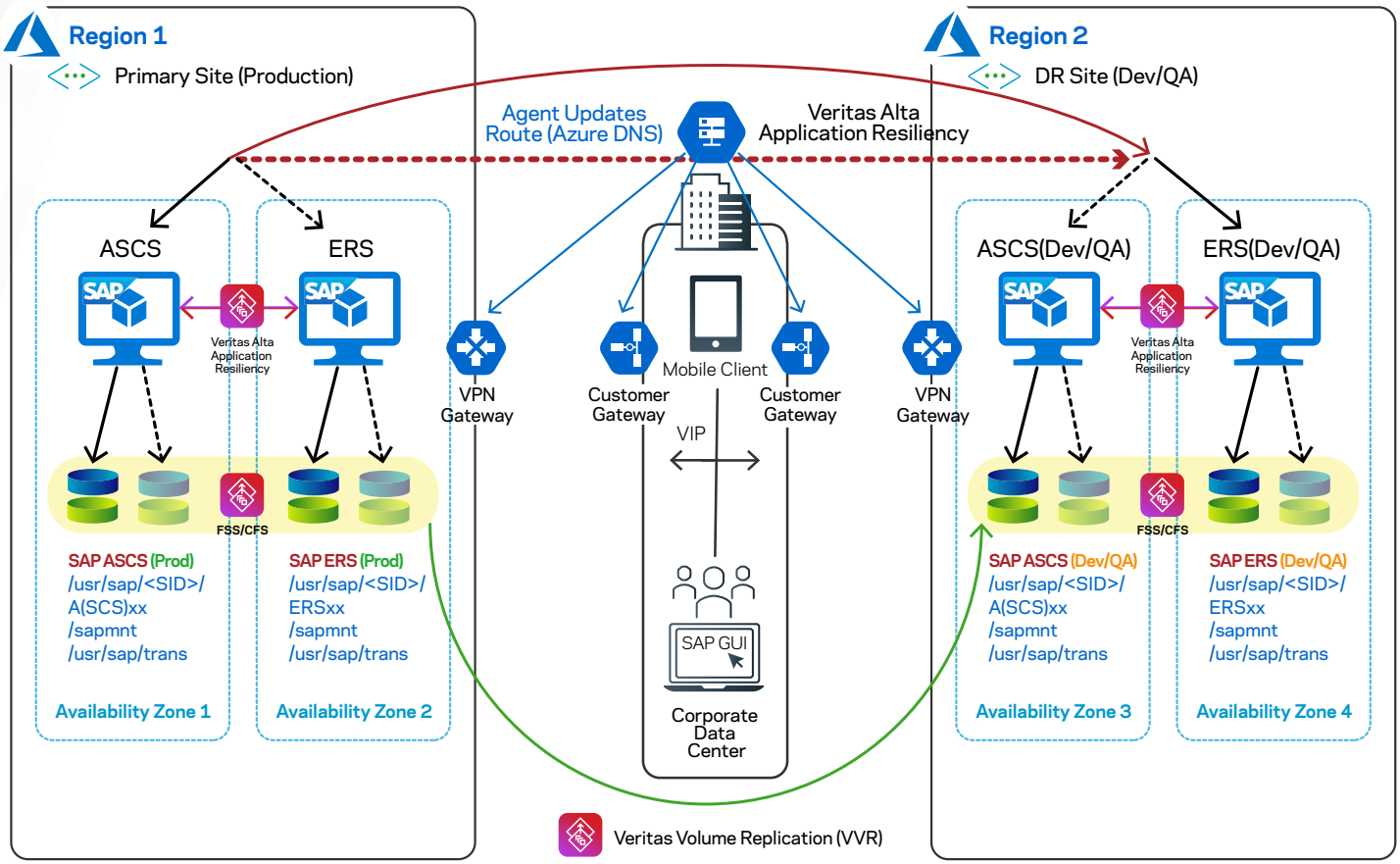
You may choose to clear the fault and perform any other necessary maintenance activities on the old ASCS instance. Thereafter, the SAPNW agent can automatically switch over the ERS instance to Availability Zone 1. ENQUEUE Replication can then continue in the reverse direction.

The following graphic illustrates this action:

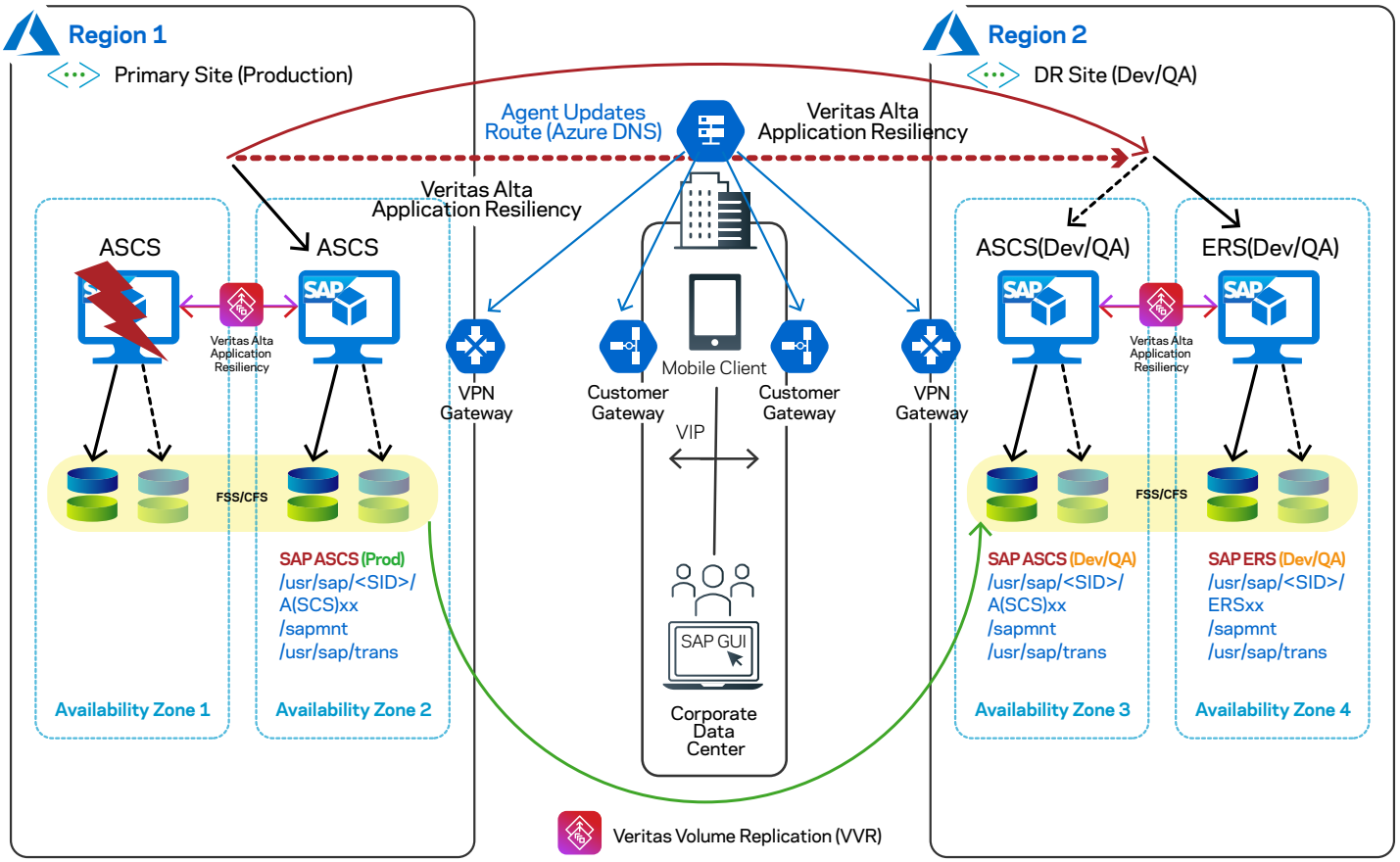


SAP Application instances across Microsoft Azure regions

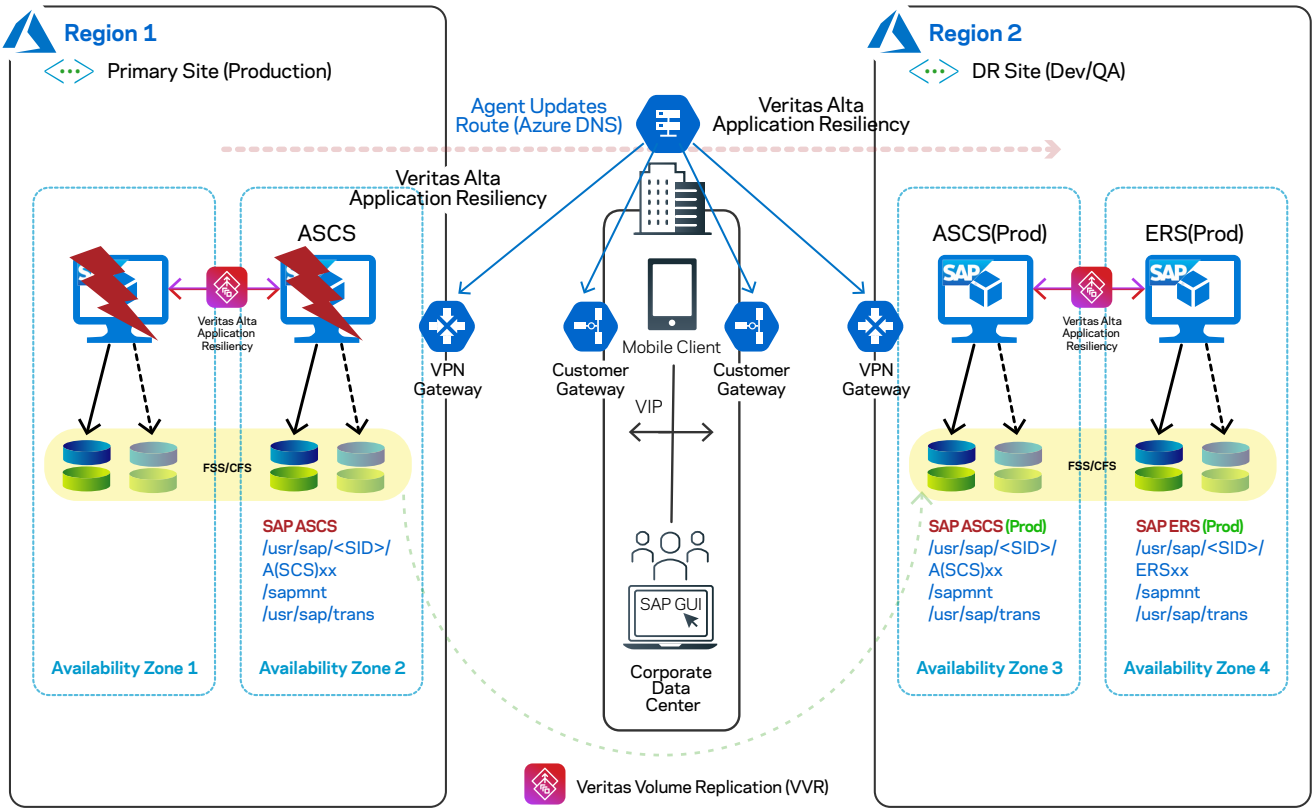
In this scenario, the SAP application production instances running in the primary site are configured in Availability Zone 1 and Availability Zone 2 respectively, in Region 1. The second set of Dev/QA SAP application instances runs on the DR site in Region 2. The SAP application data replication is manged by Veritas Volume Replicator (VVR) technolgy between Regions 1 and 2. The following graphic depicts this configuration:



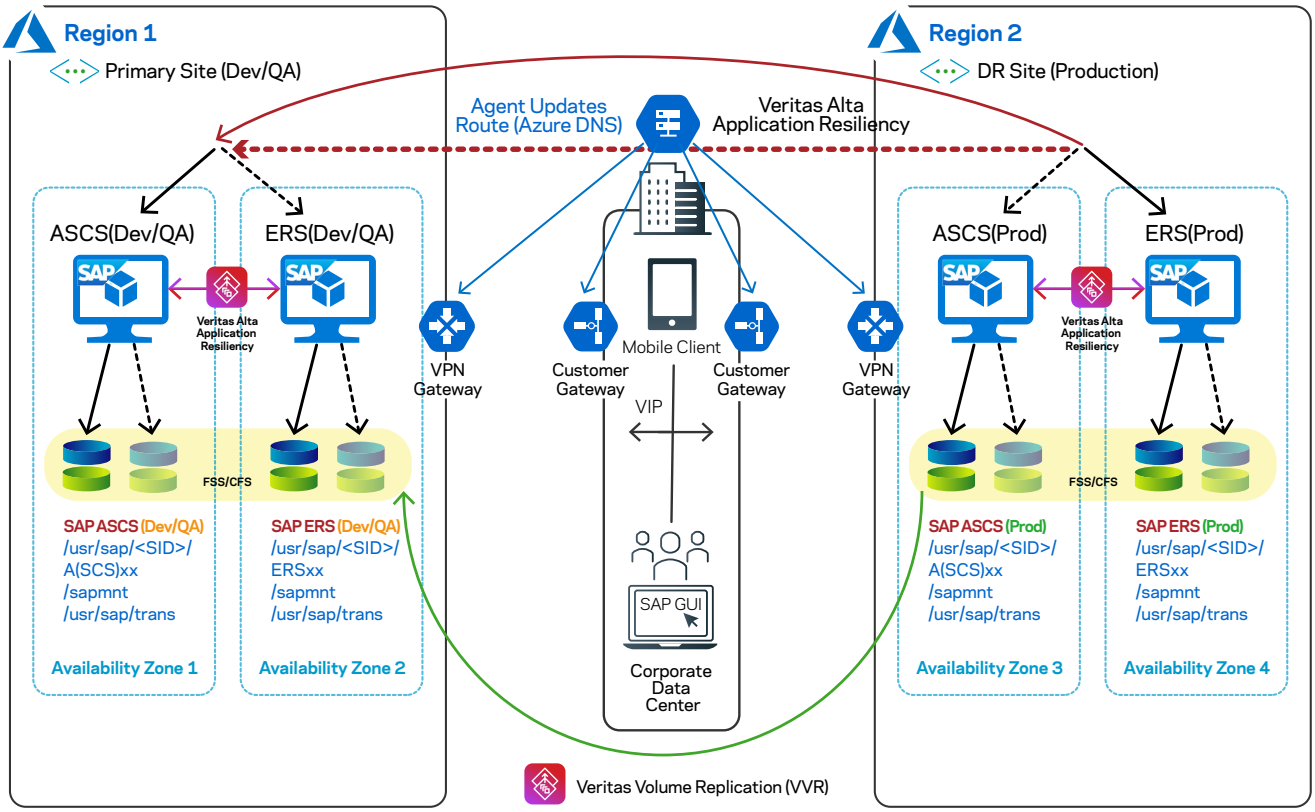
If one of the primary instance fails, the SAPNW agent automatically triggers failover of the ASCS (ENQUEUE) resource from the AZ1 to the AZ2 ERS instance in the same region. The following graphic represents the use case:



If all the instances across an AZ or Region fail, the SAPNW agent automatically triggers the switchover action by failing over the ASCS resource from the primary site to the DR site instances in the remote region. The following graphic depicts how the DR site in the remote region becomes active using the Veritas Global Cluster Option (GCO) configuration:



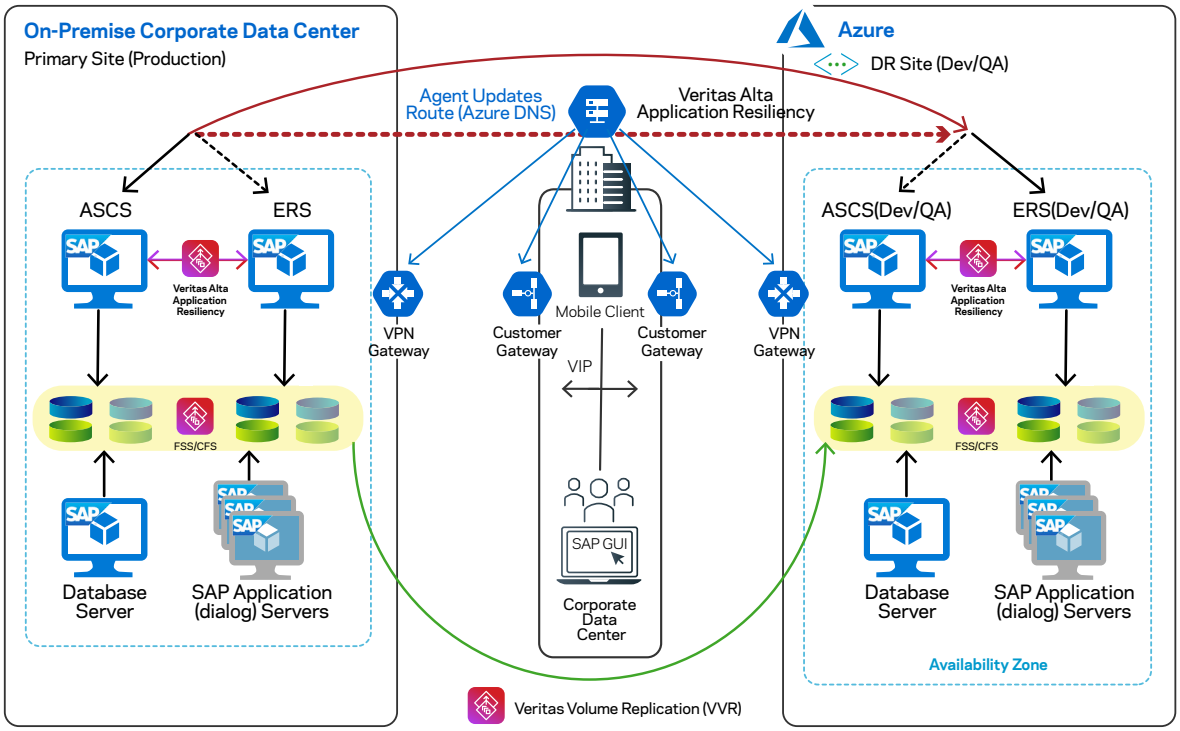
Thereafter, you'll need to clear the faults on the instances in Region 1 and then they can be used as the new Dev/QA systems. The following graphic shows the direction of the replication being reversed:



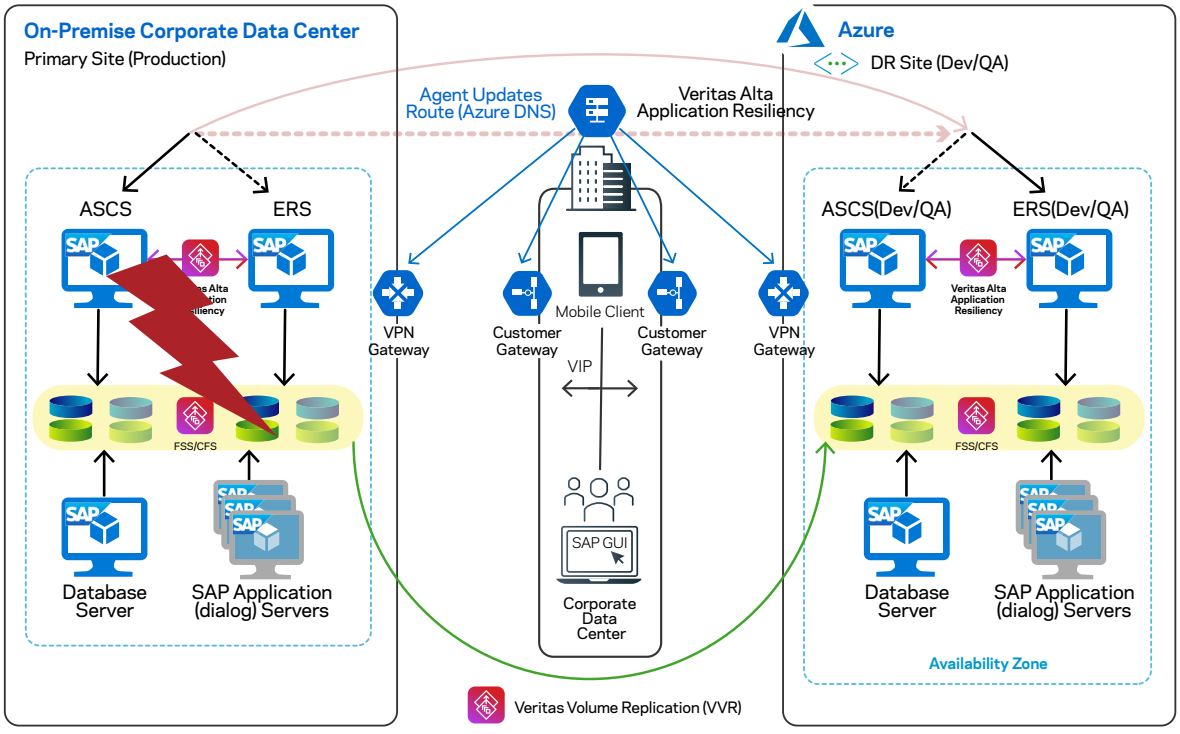
For details, refer to the Veritas agent installation and configuration documentation at: https://sort.veritas.com/agents/getting_started

On-Premises to Azure Failover (DR)

In this use case, all the SAP application instances are on-premises (primary site). Shared components like the sapmnt, trans, database data volumes and log volumes are configured with Veritas' Clustered File System (CFS). VVR manages the replication of data across sites. On Azure (secondary site), the storage volumes are allocated from Azure storage and shared components are configured with FSS.



When a disaster occurs at the primary site, all the SAP application and database instances are migrated to Azure. This can be triggered automatically or done manually by bringing the SAP applications online in Azure, which then becomes the primary site. The AzureIP and AzureDNSzone agents manage the virtual IPs and virtual hostnames in the Azure environement.



Configuration Procedure

1. Configure a VPN to connect to the Microsoft Azure cloud. Follow the procedure as per the Azure documentation.

2. Create Azure instances based on the planning document and the sizing of instances recommended by Azure for SAP systems.

3. Install and configure Veritas InfoScale Enterprise on all of the servers in cluster. For details, refer to the Installation Guide.

4. Allocate SAP-recommended storage.

5. Prepare the cloud environment as follows:

   a) Create the Azure instances

   b) Allocate SAP-recommended storage

   c) Install and configure Veritas Alta Application Resiliency solutions with valid licenses

   d) Configure Veritas Flexible Storage Sharing(FSS) and mount the following SAP mount points:

   - /sapmnt/
   - /usr/sap/<SID>/ASCSxx (xx implies the Instance Number 00-99) /
   - usr/sap/<SID>/ERSxx /
   - usr/sap/trans

Note: FSS supports all Azure storage services. VxVM, VxFS, and FSS can be used with S/4HANA / SAP NetWeaver application servers as well as most database management systems, however these utilities are not currently supported for use with SAP HANA databases.

For details, refer to the following InfoScale documentation:

- Storage Foundation and High Availability Configuration and Upgrade Guide
- Storage Foundation Cluster File System High Availability Administrator's Guide
- Storage Foundation Cluster File System High Availability Configuration and Upgrade Guide
- Veritas InfoScale Disaster Recovery Implementation Guide

For specific instructions, see the Storage Foundation Cluster File System High Availability Administrator's Guide.

Install and configure SAP NetWeaver / S/4HANA on the Microsoft Azure instances on primary and disaster recovery sites as per your disaster recovery plan.

7. Configure Veritas Volume Replication between the sites in Azure and ensure that all of the required ports in Azure are enabled for replication.

8. Configure InfoScale cluster service groups and resources for the SAP NetWeaver / S/4HANA instances. For details, refer to the following InfoScale documentation:

- Storage Foundation and High Availability Configuration and Upgrade Guide
- VCS saphdb install guide: https://sort.veritas.com/agents/download_docs/19437/vcs_sapnw_install

Summary

With SAP NetWeaver / S/4HANA representing a significant portion of the overall global ERP market share, application availability and performance is critical. Veritas Alta Application Resiliency is a certified solution to ensure HA as well as simplified DR automation and testing for SAP application servers running in Azure. It has direct integration with SAP NetWeaver / S/4HANA and Azure native tools, giving it visibility into all of the components and processes that need to be managed as part of an HA configuration for maximum application uptime. Some key benefits of using Veritas Alta Application Resiliency to manage HA and DR for SAP NetWeaver / S/4HANA in Azure are:

- Near-instant fault detection that provides minimal RTO and RPO for SAP applications and databases
- Automation of the entire failover process and non-disruptive DR testing across Azure regions
- Flexible configuration options that support multiple usage scenarios within Azure zones and regions
- Support for the broader SAP ecosystem that may include HANA and non-HANA SAP deployments

With the ability to provide best-in-class architectural flexibility, availability and resiliency for SAP NetWeaver / S/4HANA, Veritas Alta Application Resiliency enables businesses to improve upon SAP application SLA's while reducing infrastructure footprints by integrating Azure into their IT strategy. Whether running on-premises, in a hybrid cloud configuration or entirely within a cloud environment, Veritas Alta Application Resiliency is an enterprise software-defined availability and resiliency solution for SAP NetWeaver / S/4HANA in Azure that provides the tools needed to run SAP applications with maximum uptime and fulfill an organizations portion of Microsoft Azure's shared responsibility model.

References

SAP notes for SAP in Azure:

- 1588667: Overview of related SAP Notes and Web-Links
- 1656099: Supported SAP, DB/OS and Microsoft Azure products
- 1656250: Support prerequisites
- 171356: SAP Software on Linux: Essential information

Azure documentation:

- SAP on Azure
- SAP on Azure Implementation Guide

Veritas documentation:

- Veritas InfoScale
- Veritas InfoScale Trial License
- Veritas InfoScale Windows Documentation
- Veritas Cluster Server Agent Pack Getting Started Guide
- Reference Architecture for SAP HANA and S/4HANA in Microsoft Azure

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1025 02/23