Application Architecture SAP Analytics Cloud

Status	Approved
Owner	SHEPHERD-ext, Robert
Stakeholders	WANAMAKER, Craig RUFFINONI, Francois DAHN-ext, Werner Owen Pettiford, Guillaume Muller
LeanIX Link	SAP Analytics Cloud - SyWay

Introduction

SAP Analytics Cloud (SAC) is a public Software-as-a-Service (SaaS) product that provides analytics capabilities (Business Intelligence, Planning, Predictive Analytics) in one product. It is a component of BTP. In the SyWay design, and in alignment with the SyWay Analytics Approach, SAC is used as the visualisation, analytics, and planning tool for data obtained from SAP data sources (i.e. Datasphere, S/4HANA, selected SAP SaaS products).

As of December 2025, it is recognised that Datasphere (DSP) will be a component of SAP's enterprise data solution, Business Data Cloud (BDC). However, BDC is currently out of scope for SyWay. BDC will be reviewed in 2026 and, if adopted, some elements of this document may change.

Purpose

The purpose of this document is as source of information about SAC which will facilitate the support of SyWay implementation. It provides additional information to supplement the over-arching application architecture document for SAP BTP.

Scope & Objectives

This document applies to SAP Analytics Cloud only. The architecture of SAP Datasphere is covered in a separate Application Architecture Design document.

Linked Documents

Information from other documents is referenced throughout this document. This is to avoid duplication and prevent contradictions. The key documents referenced are:

Application Architecture SAP BTP

SAP Analytics Approach

SAP Analytics and Reporting Standards

Security Approach

Security Approach for Analytics

Application Architecture SAP Datasphere

Network and Infrastructure Architecture DD-TEC-070

DD-TEC-170 Transport Management for Release 4

CD-SOL-020 Reporting Approach

Application Architecture

Key Decisions and Requirements

The table below provides details of SAC specific architectural decisions. (Decisions made e.g. for the BTP platform are not restated.)

Decision	Rationale
The project will utilise seamless planning whereby SAC planning stores its data in DSP	This is SAP's strategic direction. Seamless planning offers far better functionality when integrating planning data for reporting and reference data for planning
DSP and SAC will be deployed in the same data centre	SAP do not support seamless planning across different data centres
SAC will only connect to a single DSP tenant	SAP limitation

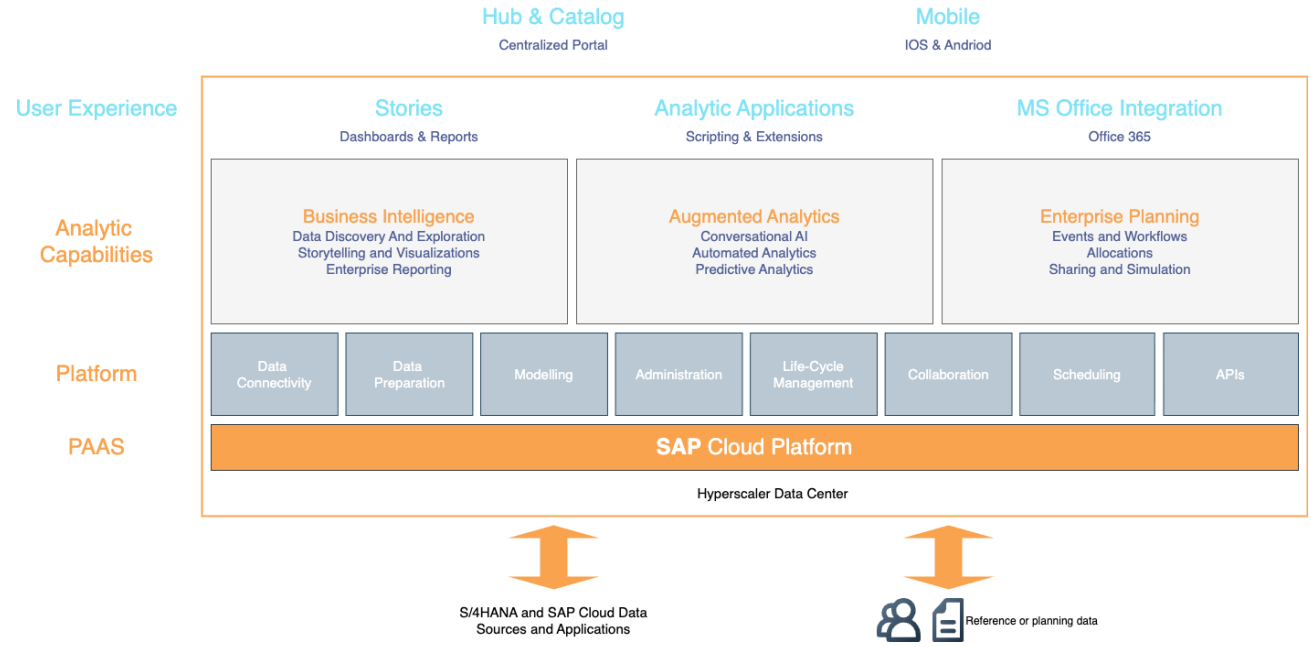
SAC will only connect to SAP sources	Primary data sources for SAC are Datasphere, S/4HANA, and selected SAP SaaS applications (not all SaaS applications support SAC client connections). SAC will not be used to directly connect to, and visualise data from, non-SAP applications, e.g. via SQL connectivity to other databases.
SAP Business content (delivered models) will be used as a reference for model design	This will lead to faster implementation
SAC will access data via live connections, not acquired connections, wherever possible	Datasphere is the SyWay data warehouse and all data should come through this system This makes data available for cross-system reporting and ensures a consistent approach to authorisations
Use SAP Horizon Light Theme with minor changes to colour palettes to create a SyWay theme	This will align with Fiori tiles for overall look and feel, but remove more gaudy colours in line with Syensqo Design

Application Architecture Design

Customer Number	3008440
Cloud Provider	MS Azure
Cloud Region	Netherlands (SAP's EU20 data center)
Service model	Software as a Service
Licence	Subscription
Deployment model	Public cloud. Deployment on a dedicated tenant is available at an extra cost, but not seen to be warranted given most processing occurs in Datasphere.
Database	HANA Cloud

Application Architecture Components

The diagram below is a representation of the offical SAP SAC application architecture edited to reflect SyWay usage. The original diagram can be found in the document: SAC Technical and Administration Overview.



Application Security

Authentication

As an application on BTP, SAC inherits the authentication mechanisms described in Application Architecture SAP BTP.

Authorisation

This is described in the Application Architecture SAP BTP document. Additional information can be found in the Security Approach and Security Approach For Analytics documents, with additional information describing the implementation details available in the SAP Analytics and Reporting Standards.

Communication Security

This is described in the Application Architecture SAP BTP document.

Data Security

Platform level data security is described in the Application Architecture SAP BTP document.

At an application level, data security is part and parcel of the authorisation approach. As with the authorisations, additional information can be found in the Security Approach and Security Approach For Analytics documents, with further implementation details available in the SAP Analytics and Reporting Standards.

The majority of data will be held in Datasphere. This includes planning data which uses seamless planning. Here, the Datasphere data security will apply.

If data needs to be read from S/4 directly (to satisfy Export Control Data (EAR or ITAR) reporting), the connectivity will be via the Cross-origin resource sharing (CORS) approach.

- N.B. with CORS, all data stays within the remote (customer) landscape. The data is not replicated to SAP Analytics Cloud, instead, results are sent directly to the end user's device. Modelling and model security is managed on the source system meaning NextLabs security is applied.

  blocked URL

Other Controls

This is described in the Application Architecture SAP BTP document.

System Landscape

The system landscape is described at a high level in the Application Architecture SAP BTP document and in more detail in the SyWay Analytics Approach document.

Operation Architecture

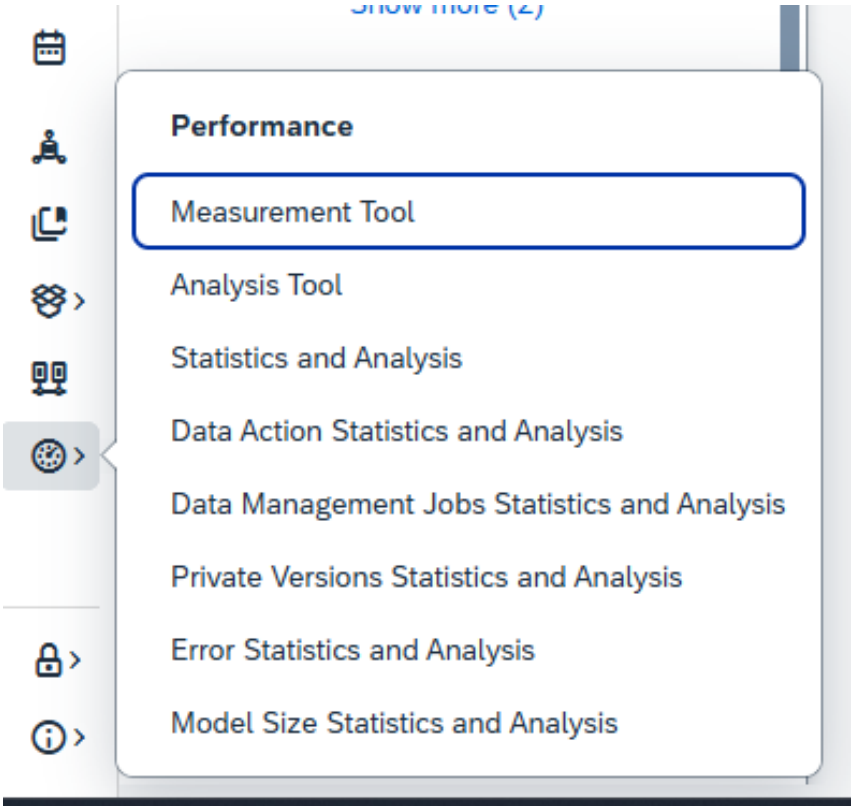
Transport Management

Transports are moved between environment tiers using Cloud TMS. Please see DD-TEC-170 Transport Management for Release 4 for more details.

Monitoring

Application Monitoring

SAP provide access to the system monitoring views available through the System menu path. These can be accessed with the system administrator role.



The monitoring capabilities update regularly with the quarterly releases and it is recommended to look at the latest SAP help documentation on the subject.

System Monitoring

As per the 'Shared Responsibility Model' section, system monitoring is the responsibility of SAP.

Sizing

Sizing has been performed based on an estimation of 500 users with 100 performing planning.

High Availability

SAC uses the same financially-backed System Availability SLA as other public cloud services from SAP, which is **99.7%**. At the time of writing, there is no mechanism available to increase this availability SLA.

As a SaaS application, the mechanisms and processes used to achieve High Availability are not visible to the customer.

Disaster Recovery

SAC has a DR approach where there is a full back-up done once a day. On top of this, there are log backups that are being done every 15 minutes. Achievable RPO is therefore 15 minutes (please see note 3026603 - Backup & Restoration for SAP Analytics Cloud).

There is no guaranteed RTO SLA for SAC.

Backup/Restore

SAP performs a back-up of SAC tenants every 15 minutes. There is also no guaranteed RTO for SAC but it is leveraging the SAP HANA Cloud service resiliency layer. Please see OSS Note 3026603 - Backup & Restoration for SAP Analytics Cloud.

Maintenance Plan - Release Management

- Major functionality is bundled into **Quarterly Release Cycle (QRC)** updates. Feb, May, Aug and Nov.
- SAP recommend to review upcoming changes before they are released. This can be done via the SAP roadmap, or through a dedicated 'Test Service' instance. There is no test service in the SyWay landscape.
- Updates include **new features, fixes, and security patches** , and they're applied automatically by SAP in the background.
- No customer-side installation or downtime planning is needed.

Shared Responsibility Model

As SAC is a SAAS service, there is shared responsibility between SAP and Syensqo. The details of this responsibility sharing are set out in the document ' Hyperscalers: Securing SAP Environments '.

As of 12 Nov 2025 the details are as follows:

Party	Service	Responsibility
Syensqo	Customization & Configuration	Customers must configure and customize the application per their business requirements
	Management of identity and access	Customers must manage the complete identity lifecycle, including onboarding and offboarding users, creating and assigning roles, forming user groups, granting and restricting privilege access, and similar functions for their application
	Data Integrity Requirements	Customers must define proper data classification, storage, and deletion requirements. Although SAP will execute processes on data, defining data requirements is a big part of the customer's responsibility. Protection for data at rest will be assigned by SAP based on the data classification
	Application Audit logs	Customers are responsible for capturing, monitoring, and analysing the application audit logs
	Application compliance	Customers are responsible for industry-specific certification and compliance for data used by or within the application.
SAP	Deploying and configuring Resources	SAP is responsible for deploying and configuring VMs, databases, container images, and the VM operating system.
	Securing VM and images	SAP is responsible for securing and patching operating systems and container images, as well as hardening configurable items on servers and databases
	Logical separation	SAP is responsible for logically segregating applications and data within various environments and between various tenants and customers
	Protecting data	SAP is responsible for implementing data protection, backup, and restoration, based on the data classification. The data retention policy is defined by customer but can be executed by SAP
	Monitoring and incident reporting	SAP logs all the security and infrastructure events. Logs will be aggregated in a system information and event management (SIEM) tool, and an alert will be generated based on the predetermined trigger. SAP will also monitor for incidents and will follow SAP's incident response plan as and when needed.
	Audit and compliance	SAP is responsible for maintaining and providing certification and compliance for the application and related infrastructure.
	Change management	SAP is responsible for managing the maintenance window and other administrative tasks regarding change management
	Availability	SAP is responsible for deploying and maintaining the availability and meeting the SLA
	IaaS	SAP maintains responsibility for the IaaS that the hyperscaler provides on SAP's behalf, and for ensuring each hyperscaler performs as per the contractual agreement
Hyperscaler	Physical security	The hyperscaler is responsible for the physical data centre and the safety and security of people in the data centre. This includes the responsibility for background checks of the people who work in the data center and in connection with other hyperscaler- provided services
	Resiliency	The hyperscaler is responsible for providing the capability of a resilient network and infrastructure across multiple regions and availability zones.
	Physical infrastructure	The hyperscaler is responsible for providing a secure network and infrastructure, including hypervisors
	Audit and compliance	The hyperscaler is responsible for IaaS compliance with industry standards.

Additional SAP responsibilities:

Application security	Application security is the heart of the overall security strategy. Application development at SAP follows the secure development lifecycle. The process starts with planning and assessment, which includes a very important security measure: threat modelling. SAP uses the well-known STRIDE threat modelling technique from Microsoft. Developers follow the secure coding guidelines during the development process. The developed code is reviewed under the "Secure code review" step as a part of the process. Next, a static vulnerability scan is performed on any code developed in-house. Any vulnerability found during the review or scan is mitigated – or documented, if not mitigated – before the release. Software is next scanned for open source vulnerabilities, if any open source libraries or components are used. Dynamic application security testing is performed after software is fully developed and compiled. The last step in the application security is unit testing of the security-related functionality to address issues like invalid input parameters. Once the software is developed and the application is deployed in production, vulnerability scanning is performed at regular intervals and after each new release. Vulnerabilities found during the scanning are managed based on their Common Vulnerabilities and Exposures (CVE) score. SAP does not report or disclose vulnerabilities, but a Service Organization Control 2 (SOC 2) audit report lists any unmitigated vulnerabilities. The SOC 2 report can be obtained from SAP.

Data Security	The customer defines the data protection, retention, backup, and deletion requirements. SAP is responsible for making sure that tenant data is logically segregated. SAP also makes sure that data is segregated between nonproduction and production environments. **Encryption** As per the SAP security policy, data in transit and data at rest should always be encrypted. Any communication between the hyperscaler and client uses Transport Layer Security (TLS) with HTTPS. Data at rest is encrypted using disk encryption to prevent data exposure in case of a physical theft of the drive. Other encryption methods, such as volume, backup, or in-application encryption, are used based on the technical, functional, and business requirements of the application and customer. **Encryption Key Management** SAP does not utilize default keys provided by hyperscalers. SAP is responsible for creating, rotating, and deleting the encryption keys. SAP also manages access to the key. One of the "key" differences between an application hosted by SAP versus third-party hyperscalers is the key storage. When an SAP application is hosted by a third-party hyperscaler, the key is stored with the hyperscaler using the hardware security module (HSM) or other secret management storage that the hyperscaler provides. This key storage or HSM is always FIPS 140-2 compliant. Any access to this storage is logged and audited by SAP. The encryption key is always managed by SAP, regardless of where the key is stored. **Retention, Deletion, and Backup** Data retention with most SAP applications is automated and customer driven. Customers can create policies or rules in the application stating how long the data should be retained based on their requirements. Data will be deleted at the end of the retention period. Customers can also delete their data at any time they have access. Data backup and deletion processes and schedules are not impacted by the migration to hyperscaler. These processes remain unchanged. It is important to note that SAP and hyperscalers will maintain compliance with laws and requirements around personal data, such as EU access, the General Data Protection Regulation, and other industry and geographic regulations.
Infrastructure and Network Security	SAP creates virtual resources using cloud APIs and is responsible for everything between and including virtual resources and the application. SAP will deploy and manage everything from the virtual machine up. This means that SAP has responsibility for managing infrastructure, creating and managing various virtual private clouds, and creating and managing security groups and firewalls. SAP is also responsible for managing and patching the operating system and middleware. SAP will regularly scan the environment for operating system and middleware vulnerabilities. SAP will deploy patches to operating systems and middleware based on the vendors' specifications. SAP's architecture blueprint dictates that database servers and application servers are isolated from each other and from the public-facing Web server. DB server and application servers are hosted within a private subnet, while Web servers are in the public subnets behind the Web application firewall (WAF) and security groups. SAP's strategy is to provide database clusters. High availability will not change as a result of migration to a hyperscaler. Hyperscalers are responsible for providing overall network and infrastructure protection against DDoS and network- or infrastructure-based attacks to the data centres, but it is SAP's responsibility to provide anti-DDoS, IPS/IDS, WAF, and network monitoring of the resources created by SAP. It is SAP's responsibility to perform regular penetration testing, and SAP will work with the hyperscaler for network penetration testing. The physical security of the data centres and vetting of the workforce who are working in and around data centres are responsibilities of the hyperscaler.
Logging, Monitoring, and Incident Response	The customer has full access to application and audit logs. SAP is responsible for collecting, storing, and analysing infrastructure and security logs. SAP manages the threat triggers and generates alerts from the logs. SAP does not share infrastructure and security logs with customers. SAP aggregates the logs into the SIEM tool and automates the process of analysing and generating alerts. Monitoring various logs and generating alerts when there is a deviation from the baseline is a very time-consuming but essential part of the security – and SAP handles that for you, so you can focus on your customers. The team of seasoned SAP professionals perform infrastructure monitoring, database monitoring, security incident management, secure admin access, regular backups, security scanning and remediation 24x7 to secure the environment for customers. Hyperscaler landscapes pose unique challenges, and SAP's security incident response team works closely together with GCS multi-cloud security operations to continuously improve security incident response process and automation for SAP's multi-cloud landscape. Although SAP does not notify customers of every incident, we will provide breach notification report and root cause analysis to customers for any incident that is classified as a personal data breach.
Identity and Access Management	The customer is responsible for identity and access management (IAM). SAP provides single sign-on and other IAM-related services as needed. SAP offers solutions that can manage the complete identity lifecycle, integrate on-premise and cloud solutions, work with multi-factor authentication, and simplify the access management process for you. The customer has complete control over who can access the data and to what extent. Most important, the customer has the ability to provide admin or privileged access to the application. This access should be granted only as needed and must be monitored. SAP has access to cloud accounts as well as privileged access to the application and SAP environment within the hyperscaler environment. SAP employees or partners do not have any access to customer's data or information.
Connectivity to Cloud	Azure ExpressRoute allows you to extend your corporate or personal network into the Microsoft cloud over a private connection. Azure ExpressRoute provides Layer 3 connectivity between your site and Microsoft cloud. Azure ExpressRoute provides redundancy for the network connection as well as a guaranteed uptime SLA for connectivity.

Additional information can be found at SAP's Cloud Services Service Level Agreement , specifically the document ' Service Level Agreement for Private Cloud Edition Services and Tailored Option Services'.

Exceptions

See also

SAC Connections

File	Modified
PDF File Approval by Frank Bolata.pdf	Apr 30, 2026 by WENNINGER-ext, Sascha
File SAC Application Architecture draw.io diagram	Apr 14, 2026 by WENNINGER-ext, Sascha
PDF File Deemed endorsement.pdf	Jan 19, 2026 by WENNINGER-ext, Sascha
PDF File Endorsement - Francois Ruffinoni.pdf	Jan 15, 2026 by WENNINGER-ext, Sascha
File SAC Connections draw.io diagram	Oct 01, 2025 by SHEPHERD-ext, Robert
File SAC Authorisations draw.io diagram	Sept 19, 2025 by BARROW-ext, ian
File Tunnel draw.io diagram	Sept 18, 2025 by BARROW-ext, ian
File CORS draw.io diagram	Sept 18, 2025 by BARROW-ext, ian

Download All

Change log

Version	Published	Changed By	Comment
CURRENT (v. 94)	**Apr 14, 2026 13:57**	**WENNINGER-ext, Sascha**	
v. 93	Apr 02, 2026 14:05	**SHEPHERD-ext, Robert**	
v. 92	Apr 02, 2026 12:32	**WENNINGER-ext, Sascha**	
v. 91	Apr 02, 2026 11:55	**SHEPHERD-ext, Robert**	
v. 90	Apr 02, 2026 11:54	**SHEPHERD-ext, Robert**	
v. 89	Apr 02, 2026 11:50	**SHEPHERD-ext, Robert**	
v. 88	Apr 02, 2026 11:45	**SHEPHERD-ext, Robert**	
v. 87	Apr 02, 2026 11:43	**SHEPHERD-ext, Robert**	
v. 86	Apr 02, 2026 11:34	**SHEPHERD-ext, Robert**	
v. 85	Apr 01, 2026 17:20	**WENNINGER-ext, Sascha**	

Go to Page History