

Delivering SAS® Expertise to Your Door

The Power of SAS® Remote Managed Software and Services



Contents

Introduction.....	1
Service models	2
Remote SAS installation with managed services.....	2
Hardware procurement and remote SAS installation with managed services.....	2
Remote managed services for an existing SAS implementation	3
Granting SAS access	3
Data privacy and security	4
Data privacy	4
Personnel security.....	5
Physical security	5
Logical security.....	5
Service operations management.....	5
Support options for SAS Remote Managed Software and Services	6
Proactive monitoring and support	6
Reactive support.....	7
System and software maintenance	7
Conclusion.....	8
Glossary of Terms.....	8

Introduction

The adoption or integration of a new technology can present many barriers within an organization. One barrier involves the significant expertise required to get the most from your investment. Another barrier is IT-focused, as many organizations struggle to define and meet service levels – and keep up with demands for an efficient and effective 24/7 infrastructure.

Still, organizations must make wise investments in systems and technology. They need solutions that provide the most value for the cost and are flexible enough to grow with the organization. So how does an organization select a management solution that meets both its current and future needs without breaking the budget? By choosing SAS Remote Managed Software and Services.

SAS Remote Managed Software and Services fulfills customers' application management needs when they require or prefer that the solution and data remain on-site. These customers still need application management and support to design, install, configure, support and maintain SAS platforms. For SAS Remote Managed Software and Services implementations, customers provide all the necessary infrastructure to operate and maintain the systems in their data center.¹

This includes:

- Servers.
- Operating systems.
- Storage.
- Account management.
- System security.
- Networking.
- Backup and recovery.
- Ongoing infrastructure support.

SAS Remote Managed Software and Services provides remote monitoring and management of SAS software and services for customers that deploy SAS solutions on-site or through a third-party cloud provider. This service allows customers to fully capitalize on the skill, knowledge and expertise of SAS experts. The offering may include service operations management; SAS application management; capacity planning; and event, incident and problem management; within the defined service level agreements. It also provides 24/7 support for SAS applications, which may include the following:

- Scheduled maintenance of the SAS solution.
- SAS platform monitoring and license monitoring.
- Data platform management, including the installation, configuration and maintenance of required SAS solution data stores (RDBMS and Hadoop instances).
- SAS administration, including the installation, configuration and maintenance of the SAS solution platform, the application of hot fixes and administration of user accounts within metadata.
- Architecture including documentation, deployment and maintenance planning.

¹ "Data center in a box" service model is an exception to this, where SAS provides the hardware and operating system, but the customer remains responsible for the ongoing maintenance and support of these elements.

- Technical account management, including the facilitation of ongoing service management activities, a fixed point of escalation for issues, and continual service improvement reviews.

This white paper describes the many advantages of SAS Remote Managed Software and Services and why it is the right fit and value to meet the demands on today's organizations.

Service models

SAS Remote Managed Software and Services provides a value-added service to customers by improving the management capabilities of SAS solutions. With over 40 years of experience, SAS has a proven track record in managing its solutions. In addition to supplying customers with continuous access to the required skills and expertise, SAS Remote Managed Software and Services also provides access to an extended global network of professional services and support experts.

There are three models of service offered under the banner of SAS Remote Managed Software and Services. Each offers a slightly different capability to meet customers' needs:

Remote SAS installation with managed services

This is the core deployment service model that includes full lifecycle management of the SAS platform. The customer provides and manages the network, hardware and operating systems. SAS implements connectivity to the customer site, deploys and tests the SAS platform, sets up monitoring for customers who opt for active monitoring, and provides ongoing support and maintenance.

To optimize performance, stability and security, SAS uses its expertise and best practices when installing SAS solutions. SAS retains the largest global resource pool of certified SAS administrators, with the support of project managers, IT support and other teams available to support the SAS application. When applicable to the SAS solution, the SAS database administration team works with the customer-provisioned RDBMS to support the SAS solution.

After deployment, the platform is transitioned across to management and support. All SAS software is installed according to a set of common documented standards. This helps ensure that 24/7 support is achievable from any of SAS' global authorized staff. Following a successful deployment, the SAS team maintains and manages the SAS solution.

Hardware procurement and remote SAS installation with managed services

In addition to the standard services offered in SAS Remote Managed Software and Services, customers have the option for SAS to supply and configure the hardware. While the primary focus is still the SAS platform, the provided hardware is specified to meet SAS' hosting requirements. After the hardware provisioning is complete, this service model follows the same process described in the previous section.

Remote managed services for an existing SAS implementation

In customer sites where the SAS Remote Managed Software and Services team has not deployed the SAS platform – but is asked to provide ongoing management of an existing implementation – the SAS team can perform a detailed review of the entire platform. In this model, the SAS team documents the architecture, the deployment model and any gaps perceived as nonstandard or against SAS best practices. A RACI matrix (a way of defining roles and responsibilities for a specific task or activity) is created for tasks and communication channels that are agreed upon with the customer. Before SAS assumes management of the platform, the following must occur:

- Any recommendations are discussed, prioritized and implemented.
- Any risks are mitigated or accepted by the customer.

Following a successful handover, the SAS Remote Managed Software and Services team maintains and manages the SAS platform.

Granting SAS access

Regardless of the selected service model type, the SAS Remote Managed Software and Services team must be able to access the SAS platform. This is achieved through a remote connection. Where possible, the team has a direct connection with the customer's environment, which enables them to gain access to the SAS applications to perform scheduled support and maintenance tasks. It also allows the SAS platform to communicate directly with the SAS Remote Managed Software and Services team to proactively send alerts when an event or an incident occurs.

The following list provides the ways that customers can grant SAS the required access to their systems in order to manage and maintain the SAS platform(s).

- For SAS Remote Managed Software and Services management, SAS requires a site-to-site VPN to provide proactive monitoring and alerting. When monitoring agents are installed onto the operating system of the SAS servers, alerts for significant events are sent back through the VPN to the SAS team, allowing them to respond (see Figure 1).
- For platform management, SAS installs a remote management server within the SAS Cary data center. The connection to the customer is limited and secured around this connection. All required SAS clients are installed on the customer's remote management server, enabling the SAS Remote Software and Services team to access and administer the SAS platform.

Each SAS Remote Managed Software and Services platform results in a multisite implementation. At the SAS Cary data center, monitoring and remote management servers are commissioned, along with a dedicated VPN connection to the customer's site. At the customer's site, the SAS servers that support the database servers are commissioned in combination with a dedicated VPN connection and a remote management client machine. Figure 1 depicts this architecture, assuming a default configuration where a VPN connection and active monitoring are in place.

Data privacy and security

For many years, customers have asked SAS to provide solutions and manage sensitive data for a wide variety of sectors globally. This includes sectors where data security, privacy and control are of paramount importance, such as government, banking/ financial services, pharmaceuticals and health care. This responsibility lies at the heart of the services that SAS offers around data protection. This section describes the privacy, security, and control for the service models described. In a majority of cases, the customer controls data within its own SAS platform, as defined by the customer's data security policies.

Data privacy

All data is treated as confidential and is made available only to authorized SAS personnel requiring access to perform their duties during installation or ongoing maintenance. Content cannot be used or disclosed by SAS personnel, other than what is required to perform the management services as authorized in customer agreements - or is required to comply with legal or regulatory requirements. Direct access to content is limited to what is necessary to perform management services or to fulfill any legal requirements.

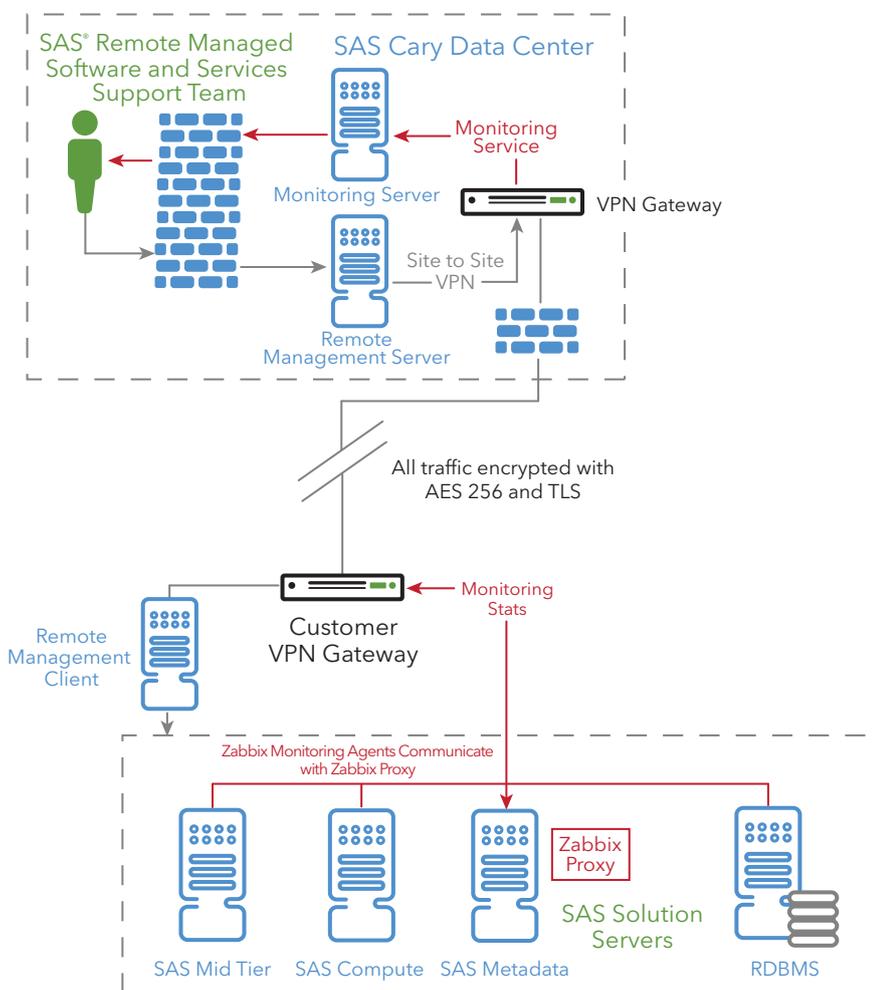


Figure 1: SAS Remote Managed Software and Services architecture with dedicated VPN.

Personnel security

SAS works with the customer to adopt the customer's existing security policies for gaining access to the remote systems. If these processes are not in place, SAS can work with the customer to define them based on previous experience and documented best practices. All SAS personnel are required to adhere to SAS policies and procedures at all times, including the SAS conduct policy. It is the customer's discretion to request further checks.

Physical security

Because all servers and data remain on the customer's site, physical security controls follow the customer's security policies and procedures. SAS servers reside in a SAS managed data center, which is audited annually by a third party.

Logical security

The customer is responsible for implementing all logical security controls and providing SAS personnel with access to the SAS platform, based on these controls.

Where continual access to the customer's platform is granted through a dedicated VPN to safeguard the customer's systems, SAS Remote Managed Software and Services system administrators take measures from within the SAS environment to protect the SAS remote management server from all known threats such as malware, viruses and unauthorized access. SAS uses two-factor authentication for appropriate SAS staff and SAS subcontractors to access systems hosted at the primary SAS data center if required by regulation or customer contract. Two-factor authentication is not required for customers to access SAS solutions. Other logical security policies include:

- All data transmissions to and from SAS are completed over secure and encrypted channels.
- Customer data or other content is not stored at SAS data center.
- All systems with a Microsoft operating system are configured with antivirus software.
- Access to the SAS remote management server is approved and logged.
- All connections must be made through a secure connection.

It is SAS policy that customer material be encrypted while in transit and at rest, whenever possible.

Service operations management

The SAS Remote Managed Software and Services team provides a single point of contact and customer liaison. This team may call upon a global resource pool of over 500 staff members to ensure the operational integrity of its customers' platforms.

This team uses ITIL and SAS best practices to provide event and incident management. Events are triggered when a process or element of SAS is not functioning correctly. Incident management is engaged to restore normal service operation as quickly as possible and minimize the adverse effect on business operations.

SAS' Remote Managed Software and Services team performs a root cause analysis of

identified incidents and works with the customer's support team if the issue involves the customer-provisioned elements of the platform. Resolving an incident can prevent further or related incidents from occurring in the future and allows these lessons to be shared for future prevention.

Support options for SAS Remote Managed Software and Services

For this offering, SAS provides two models for support:

1. Proactive monitoring and support.
2. Reactive support.

Proactive monitoring support is the recommended support model. The reactive model is an exception to the standard configuration and is used when the customers' restrictions prevent active monitoring of their environment.

Proactive monitoring and support

A team of experts actively monitors its customer's SAS platform from the SAS operations center on a 24/7/365 basis, responding to events and incidents and taking the lead in co-managing its customer's SAS platform and SAS solutions. Customers retain access and control and receive the added benefits of SAS' customer support, best practices and issue resolution processes.

This support model is only available to those customers who implement a site-to-site VPN as described in the "Remote managed services for an existing SAS implementation" section.

Active monitoring of the SAS environment involves SAS configuring the automatic creation of tickets based on monitoring triggers.²

Standard monitoring includes standard SAS software components, such as:

- SAS compute services.
- SAS mid-tier services and web applications.
- SAS metadata and/or microservices.
- SAS access engines.

Additional monitoring services are available and build upon standard monitoring:

- ETL and batch monitoring.
- Custom workload and grid workload monitoring.
- Capacity and health check reporting.

² Zabbix is used to provide the metrics near real-time over the SAS-to-site VPN. A Zabbix client is installed on all monitored servers. In addition, a Zabbix proxy is installed on a Linux server to communicate back to the Zabbix monitoring server in Cary. Linux is a requirement, as the Zabbix proxy cannot run on a Windows server.

Note: Some ancillary infrastructure information (e.g., CPU, memory, ports) may be collected and used to prescribe action if a pending or existing SAS software issue exists. Although the focus of monitoring is SAS software components.

- Capacity management, which includes a typical assessment based on capacity as the platform's metrics are recorded and extrapolated from the data collected.
- A direct line to SAS Technical Support, which triages to the SAS Remote Managed Software and Services desk. Customers can alternatively use the web-based ticketing system, which submits a request directly to the SAS Remote Managed Software and Services support team.
- The SAS support team works and manages the ticket and gains access to the customer's system, using the Cary-based remote management server to connect into the customer's on-site remote management client machine.

Reactive support

Reactive support is provided only when the customer does not permit sending monitoring data to the Cary data center. In these cases, there is no proactive monitoring of the platform, and the customer is responsible for informing SAS of any problems they encounter while using the platform.

Reactive support includes a direct line to SAS Technical Support, which triages to the SAS Remote Managed Software and Services desk. Customers can alternatively use the web-based ticketing system, which submits a request directly to the SAS Remote Managed Software and Services support team.

System and software maintenance

Best practices dictate that the operating system and SAS software receive updates on a regular basis, and in a controlled manner, to avoid data corruption or end-user disruption. The scheduling of these events is at the customer's discretion. When customers make changes to their infrastructure or software that could affect the SAS platform (for example, system updates, storage changes or network re-configuration), customers must notify SAS prior to any scheduled maintenance in accordance with a contracted notice period. SAS provides support by preparing the platform for such an event. In addition, SAS and the customer agree upon established maintenance windows to enable regular backup tasks or other scheduled tasks to be performed, without disrupting the end users or corrupting the platform.

The SAS Remote Managed Software and Services team ensures that its customers are using the latest SAS software updates, where appropriate. These software updates are installed and managed by experts, providing optimal uptime of the environment for the user community. SAS provides ongoing application support for licensed software, including installation of hot fixes and patches that may be required to address reported issues. Services for upgrades and migration from one set of hardware to another can be agreed upon and incorporated into a customer agreement.

Conclusion

With its combination of SAS best practices, customer-driven security and privacy settings, as well as industry standard incident and problem resolution procedures, SAS Remote Managed Software and Services is an excellent offering for SAS customers. The SAS Remote Managed Software and Services offering is the best fit for customers who require the level of expertise, governance and service operations management and monitoring of their SAS platforms, while ensuring the security and integrity of their data by keeping their solutions in-house.

For more information on SAS Remote Managed Software and Services, please contact your local SAS account executive.

Glossary of Terms

Term	Description
SAS application	The SAS application stack that is being managed by SAS, from the SAS servers to the RDBMS (if being managed as part of SAS Remote Managed Software and Services).
SAS platform	The SAS applications and services combined with associated third-party software.
ITIL	The information technology infrastructure library (ITIL) is a set of practices for IT service management that focuses on aligning IT services with the needs of business.
RACI matrix	RACI stands for responsible, accountable, consulted and informed. A responsibility assignment matrix describes the participation by various roles in completing tasks or deliverables for a project or business process.
TLS	Transport layer security is a cryptographic protocol that provides communication security over a computer network.
AES 256	The Advanced Encryption Standard is a specification for the encryption of electronic data established by the US National Institute of Standards and Technology (256 refers to the key length used).
Firewall	A technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts.

To contact your local SAS office, please visit: sas.com/offices

