SafeNet Authentication Service

PCE/SPE System Requirements Guide

gemalto
security to be free

Product Version: SafeNet Authentication Service 3.5.5 PCE/SPE

Document Part Number: 007-012948-005, Rev. A

Release Date: May 2017

Table of Contents

Document PN: 007-012948-005, Rev. A,

Preface

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS) - Service Provider Edition (SAS-SPE)**—Used by service providers to build an authentication service.
- **SafeNet Authentication Service (SAS) - Private Cloud Edition (SAS-PCE)**—Used to implement an authentication service on the customer premises.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet Authentication Service (SAS) users and security officers, key manager administrators, and network administrators. It is assumed that the users of this document are proficient with security concepts.

All products manufactured and distributed by Gemalto are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult the support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	**https://serviceportal.safenet-inc.com** Existing customers with a Technical Support Customer Portal account can login to manage incidents, get latest software upgrades, and access the Gemalto Knowledge Base.	
Documentation	All SAS documentation (Cloud, PCE, SPE, Token and Integration) can be found on the **SafeNet Knowledge Base** page. All SAS Agents documentation can be found on the **SafeNet Authentication Service Downloads** page.	

1
System Requirements

Environment

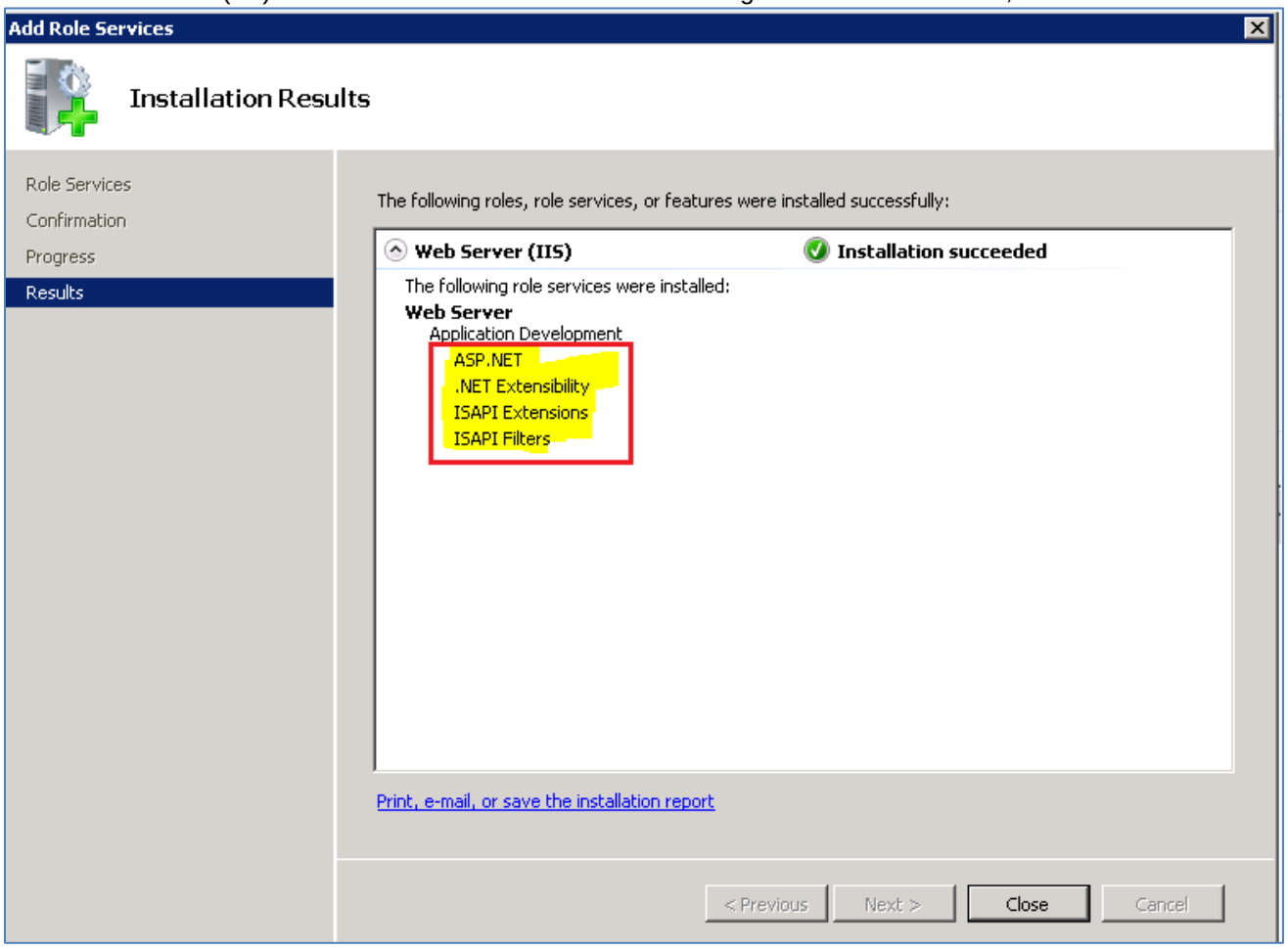
Description	
Supported Operating Systems	• Windows Server 2008 R2 SP1** • Windows Server 2012*** • Windows Server 2012 R2****
Supported Database Servers	• PostgreSQL 9.3 (default) **Note**: PostgreSQL should be used only for test and proof-of-concept installations. It is not supported in HA configurations. The default database shipped with SafeNet Authentication Service is PostgreSQL. Any other supported database must be purchased separately. • HA support requires MySQL 5.7 or later **Note**: In other words, MySQL versions prior to 5.7, are not be supported, and thus may not work with the SAS solution. • MS SQL 2008, MS SQL 2012, MS SQL 2014 **Notes**: For replication, an active/active (multi-master) configuration needs to be deployed. On MS SQL, this is transactional peer-to-peer replication. In addition, peer-to-peer replication (MS SQL 2014) is also supported. Only an MS internal (SQL only) user account needs to be used to connect SAS to the database. Also, MS SQL needs to be configured in the mixed mode. An MS SQL Windows User is not supported.
Supported LDAP Directories	• Active Directory • Novell eDirectory 8.x • SunOne 5.3
Supported Architecture	64-bit
Supported RADIUS Authentication Protocols	• PAP • MSCHAPv2

<table>
<tr><th>Description</th><th></th></tr>
<tr><td>Additional Software Components</td><td>• Internet Information Services (IIS) 8.5
• .NET 4.6.2 (Download, here)
• .NET Framework 3.5 Features
Note: IIS 6 compatibility roles and ASP.NET role services must be installed in order for the SAS website to appear.</td></tr>
<tr><td>MySQL Components</td><td>• MySQL Connector 6.4.4 (Download, here)
Note: The MySQL Connector is required only if the database in use is MySQL.</td></tr>
<tr><td>Processor</td><td>2.6 GHz processor (or above)</td></tr>
<tr><td>Memory</td><td>16 GB RAM (or greater)
<table>
<tr><th>Number of Users Range</th><th>Recommended RAM</th><th>Number of Processor Core (v2.60 GHz or above)</th></tr>
<tr><td>Till 10000</td><td>16 GB</td><td>2</td></tr>
<tr><td>10000-20000</td><td>32 GB</td><td>4</td></tr>
<tr><td>20000+</td><td>64 GB</td><td>6</td></tr>
</table></td></tr>
<tr><td>Disk Space</td><td>300 MB
Note: Minimum disk space required for installation is 300MB; additional disk space would be required if logging is enabled.</td></tr>
<tr><td>Display</td><td>SVGA (1280 x 1024), 24-bit color or higher</td></tr>
</table>

**Windows Server 2008 R2 SP1 – Installing Microsoft Root Certificate

For a smooth installation of SAS with .NET 4.6.2 Framework, the administrators have to install the Microsoft Root certificate manually, prior to running the setup.

a. Install Web Server (IIS) and select additional Role Services using **Add Roles Services**, as illustrated below:



b. Download and import the Microsoft Root certificate (Download **here**).

c. Initiate the SAS installer to continue with .NET 4.6.2 Framework installation, followed by SAS installation.

Note: After .NET installation, a prompt to restart the system will be displayed. After the restart, the installation process will resume to complete the SAS installation.

***Windows Server 2012 – Installing Server Manager Roles

For a smooth installation of SAS with .NET 4.6.2 Framework, the administrators have to install the required server manager roles:

a. Install .NET Framework 3.5 Features.

b. Install Web Server (IIS) and select additional Role Services using **Server Manager Roles and Features**, as illustrated in the **Internet Information Services Role Services Required** section on page 9.

c. Initiate the SAS installer to continue with .NET 4.6.2 Framework installation, followed by SAS installation.

Note: After .NET installation, a prompt to restart the system will be displayed. After the restart, the installation process will resume to complete the SAS installation.

****Windows Server 2012 R2 – Installing Microsoft Updates

For a smooth installation of SAS with .NET 4.6.2 Framework, the administrators have to install the following Microsoft updates.

a. Install .NET Framework 3.5 Features.

b. Install Web Server (IIS) and select additional Role Services using **Server Manager Roles and Features**, as illustrated in the **Internet Information Services Role Services Required** section on page 9.

c. Install the following Windows updates, in the following order:

   i. **Windows8.1-KB2919442-x64.msu** (64-bits) (Download **here**)

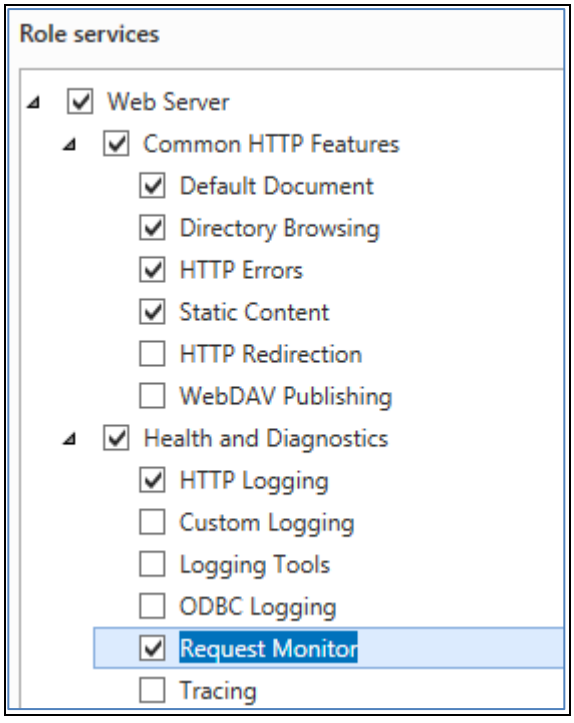
   ii. **Windows8.1-KB2919355-x64.msu** (64-bits) (Download **here**)

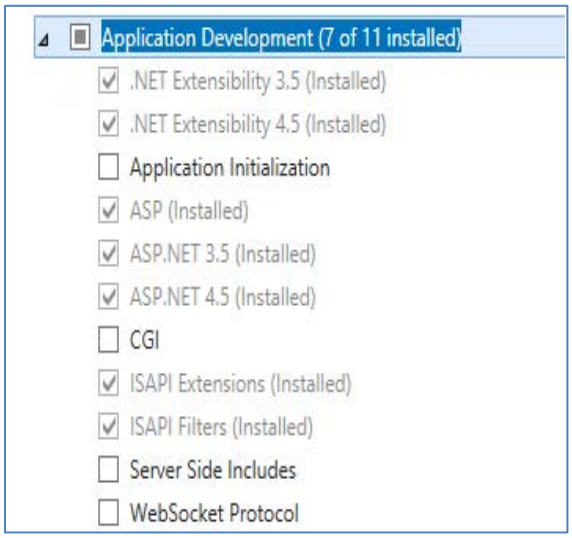
d. Initiate the SAS installer to continue with .NET 4.6.2 Framework installation, followed by SAS installation.

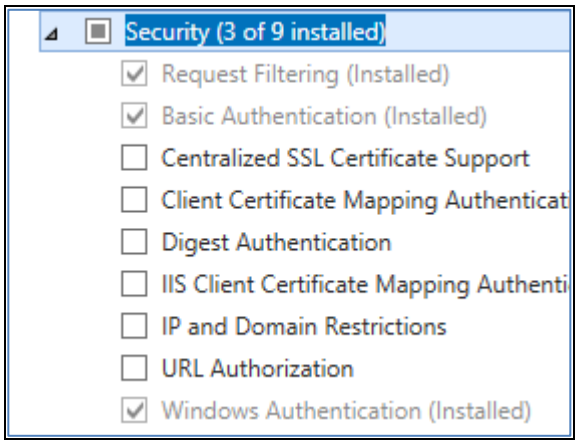
   Note: After .NET installation, a prompt to restart the system will be displayed. After the restart, the installation process will resume to complete the SAS installation.

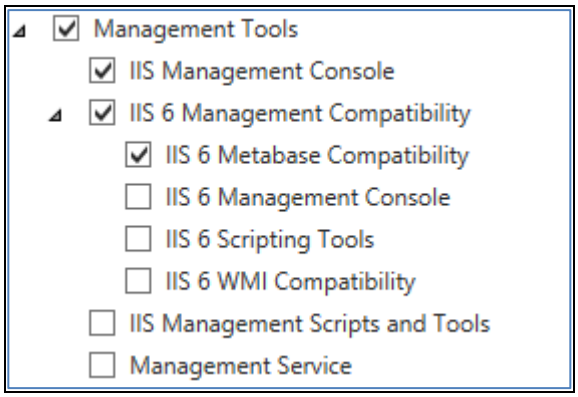
Internet Information Services Role Services Required

To successfully install and run SAS 3.5.5 on Windows Server 2012 and Windows Server 2012 R2, include the IIS role services as specified in the images below:









System Sizing

NOTE: The system sizing information is provided as a general guide. It is strongly recommended that you make an assessment of your specific requirements based on your infrastructure setup before implementation.

Minimum Recommended Configuration

The information in the table below is based on the following minimum recommended configuration (for up to 5000 users):

- CPU: Intel® Xeon(R) Processor CPU E5-2650 v2.60GHz (2 core)
- RAM: 16 GB
- Primary measurement: Authentications per second

Under stable testing conditions, the average time to complete one authentication successfully is 15 milliseconds. Below are the comparative performance metrics differentiated on various RAM and Processor Core sizes.

	16 GB RAM (Minimum Recommended)	**32 GB RAM**	**16 GB RAM**	**32 GB RAM**
Number of processor Cores	2 Core	2 Core	4 Core	4 Core
Maximum number of authentications per second	80	87	90	102
Maximum CPU utilization	90%	85%	40%	38%
Average number of authentications per second	70	73	82	88
RAM Memory Utilization				
% of available RAM used	1%	1%	~1%	~1%
Available RAM	16220 MB	32440 MB	16220 MB	32440 MB
Physical Disk				
Average latency *	16ms	14ms	10ms	10ms
Throughput *	174 MB/sec	188 MB/sec	342 MB/sec	348 MB/sec
Maximum CPU utilization by MySQL process	34%	30%	20%	10%
Network I/O activity	6 Mbps	6.5 Mbps	6 Mbps	7 Mbps
Physical memory used	196 MB	232 MB	210 MB	245 MB
Users loaded	5000	5000	5000	5000

* Average latency – It is the latency between start and completion of server read/write request on the physical disk, and is measured in milliseconds.

* Throughput – It is the amount of data that the physical disk has received from the server at any given second, and is measured in megabytes.

Additional Requirements

- The system administrator installing SAS must have administrative privileges on the local system.

- If migrating to SAS, refer the specific SAS migration guide at the following link: **http://www2.safenet-inc.com/sas/implementation-guides.html**

SafeNet Authentication Service Ports

SAS may require the use of several ports, depending upon the location of external directories, databases, or RADIUS servers. The following is a list of default port values. SAS can be configured to use alternate ports. SSL requires that a valid certificate is installed on the SAS server.

Port (TCP/UDP)	Usage
80/443	Port 80 and/or 443 can be used for management sessions, provisioning, self-enrollment, self-service, and for servicing of encrypted authentication requests from configured agents. For security purposes, port 443 (SSL) is recommended.
1812/1813	Ports 1812/1813 are standard ports for RADIUS authentication and RADIUS accounting respectively.
389/636	Ports 389/636 are standard ports for LDAP and LDAPs connections respectively. For security purposes, port 636 (SSL) is recommended.
5432	The port number for connection to the default PostgreSQL database.
1433	The default port number for connection to an MS SQL database.
25	The default port for SMTP email.
8456	The default port number for LDAP synchronization traffic to/from SAS and LDAP.
8458 (Inbound)	The default incoming port number for the Logging Agent.
8459 (Outbound)	The default outgoing port number for the Logging Agent.
11012	The default port for communication between SAS and SAS HA Controller Service.

SAS Synchronization Agent Ports

- TCP Port 8456 – Incoming on the SAS server
- TCP Port 389
- TCP Port 636 (optional) – Outgoing from the SAS Synchronization Agent

SAS Logging Agent Ports

- Agent > SAS TCP Port 8459
- SAS > Agent TCP Port 8458
- Agent -> Syslog UDP Port 514

Virtualization

SAS is designed for virtualization and has been extensively tested with VMWare®.

Internal Database

The internal database contains all system configuration, application and policy data, token information, and history and activity information used by SAS. User-specific information, such as user IDs and coordinates are also stored in the database (possibly synchronized from an original user source).

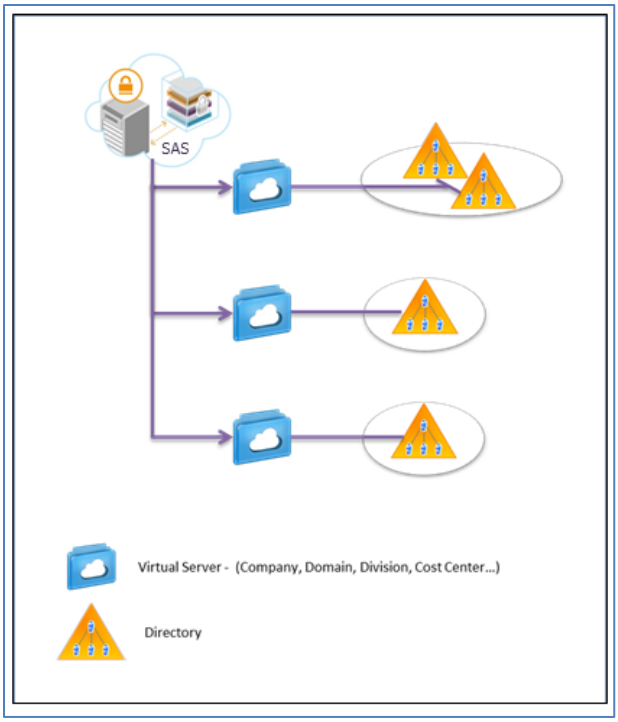
Where LDAP/AD integration is configured, the unique **GUID** property of the LDAP user account is stored in the database, providing a consistent link between the user's LDAP account and tokens associated with the user in SAS. The **UserID** is stored with authentication activity for reporting purposes. This allows SAS to provide audit trails and authentication activity reports even after a user (and therefore the GUID) has been deleted from LDAP.

The database can be installed on the machine hosting SAS, on a separate machine, or as a cluster. Every SAS implementation can be configured for a primary database instance with failover to an alternate instance. In addition, multiple SAS servers can use the same database.

LDAP External User Sources

SAS supports the use of one or more LDAP directories for the user, account status, and group membership data. Each LDAP must be configured for a specific virtual server. Alternatively, an LDAP forest can be connected to one virtual server if needed. When there are multiple domains within one virtual server, SAS must be able to read the LDAP forest via the Global Catalog Server (port 3268), and all domains in a forest must be fully trusted (AD only).

LDAP External User Sources



Supported Browsers

A browser is the standard interface for use with SAS or components such as self-enrollment or user self-service.

The following browsers are supported:

- Chrome 33 and later
- Firefox 3.5 and later
- Internet Explorer 8 and later
- Microsoft Edge

Certain functions may require ActiveX controls and/or JavaScript.

Maintaining Accurate Time Settings

SAS operation and authentication services are not dependent on accurate time settings. However, it is recommended to maintain accurate time to enable reliable and consistent reporting and audit trails. In some cases, SAS licensing may restrict certain functions based on dates or date ranges. Modifying the server date after license installation may cause these functions to become unavailable.

It is recommended that the SAS time is set to the local time zone and that the server time is UTC coordinated. For more information, visit **http://www.time.gov**.

Installation Types

An SAS site is defined as an instance of the SAS authentication engine. The number of sites and configuration options are determined by licensing, redundancy, and performance requirements. Assuming that SAS is installed on the recommended hardware, the factor that has the largest bearing on performance is the database I/O, primarily determined by the amount and frequency by which authentication history is written. In most cases, it is acceptable to have SAS and the database installed on the same server.

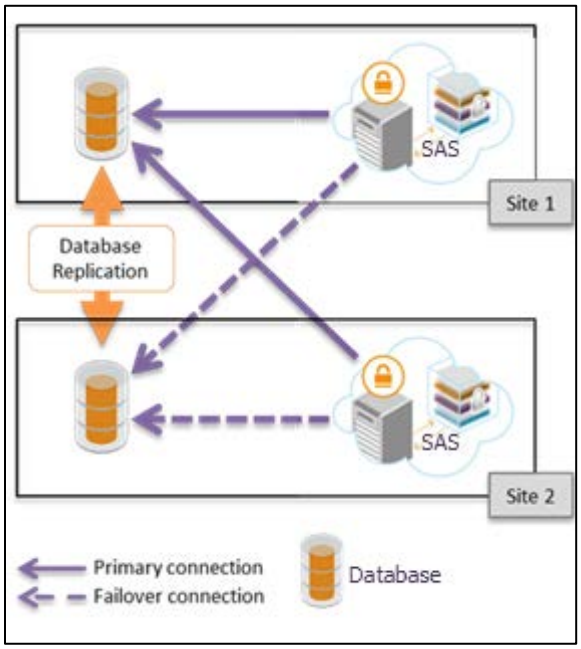
The scenarios described in the following sections are provided as guidelines and examples. Many different configurations are possible. For example, it is perfectly acceptable to install the database, enrollment, self-service, and directory components on separate computers.

NOTE: In the following diagrams, “site” refers to an SAS instance that connects to the same database or database cluster. This can be at the same physical location or spread across different data centers.

Small, Single-Site Deployments

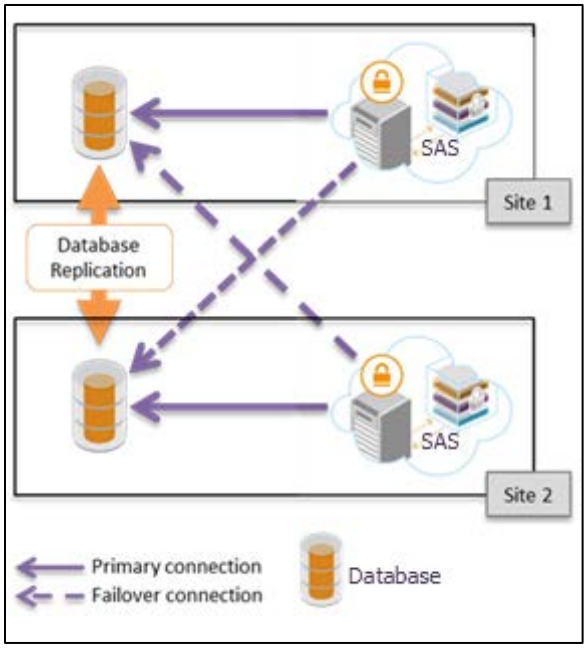
You may choose to install all SAS components on a single server, with a secondary instance providing redundancy and failover.

Small Deployments with Failover



You may choose to install all SAS components on a single server, with a secondary instance providing redundancy and failover.

Small Deployments with Failover and Site Specific Database

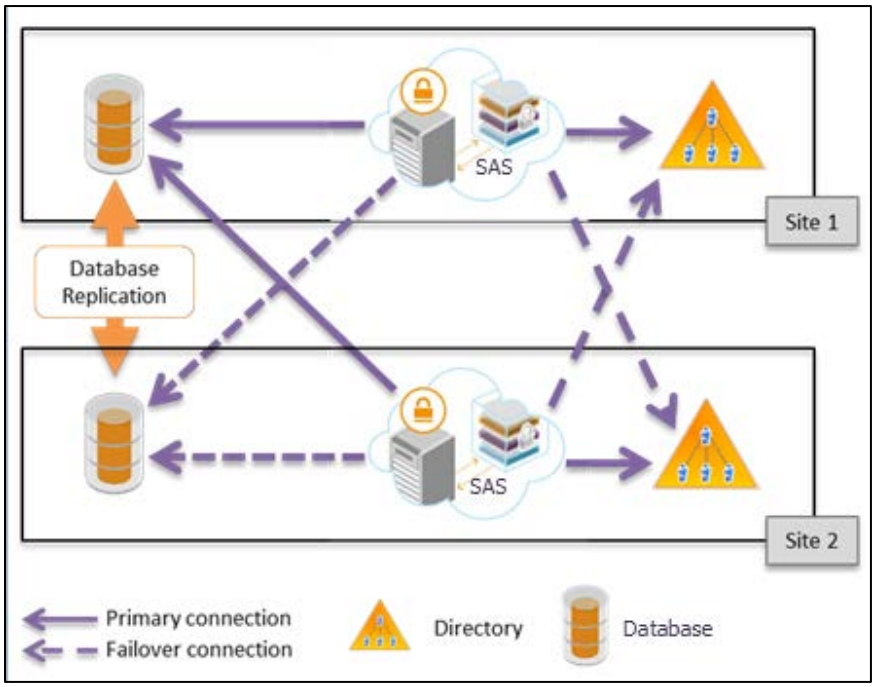


Authentication and management functions can be distributed across sites if necessary. SAS agents can failover to the alternate site. The connections between LDAP and SAS can be local or remote. If there is a primary and secondary LDAP server, each SAS instance would typically be configured for LDAP failover.

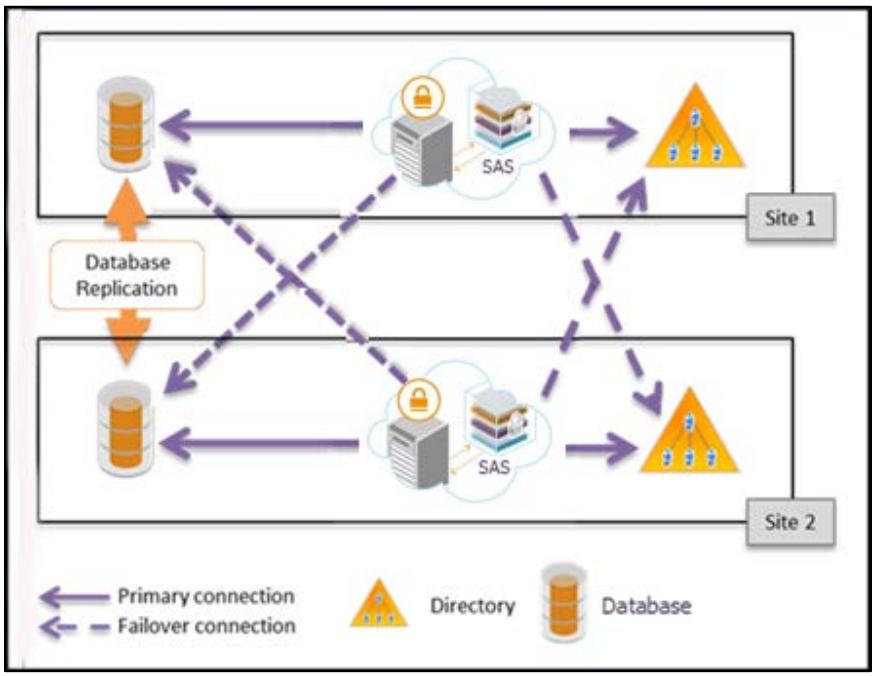
Medium Site Deployments

Medium site deployments are typically required for organizations with dedicated LDAP, web, and RADIUS servers.

Medium Deployments with Failover



Medium Deployments with Failover and Site Specific Database



Large Deployments

For sites requiring support for up to 250,000 users and several hundred authentications per second, a database cluster fronted by multiple SAS sites is recommended.

Large Deployments with Failover