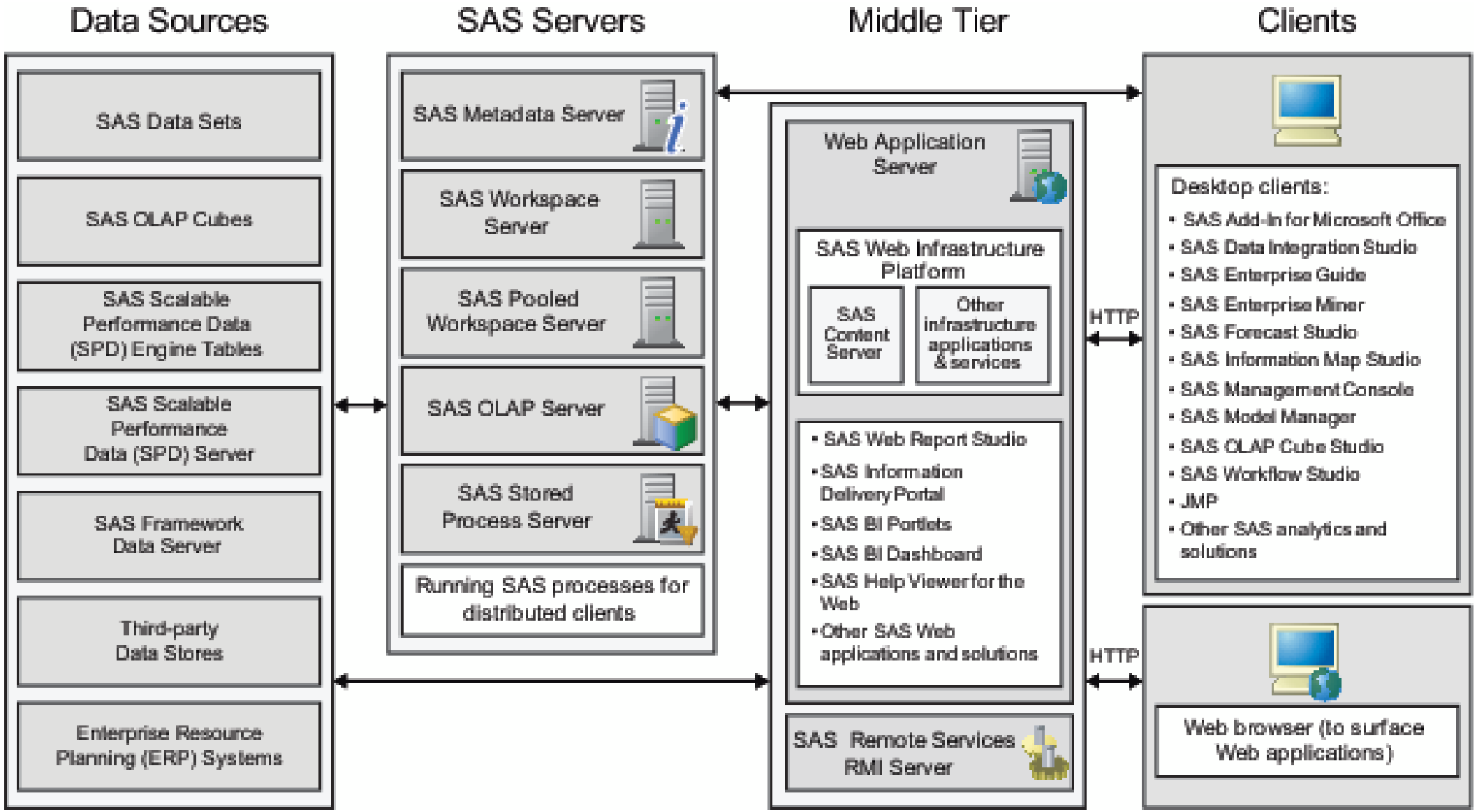
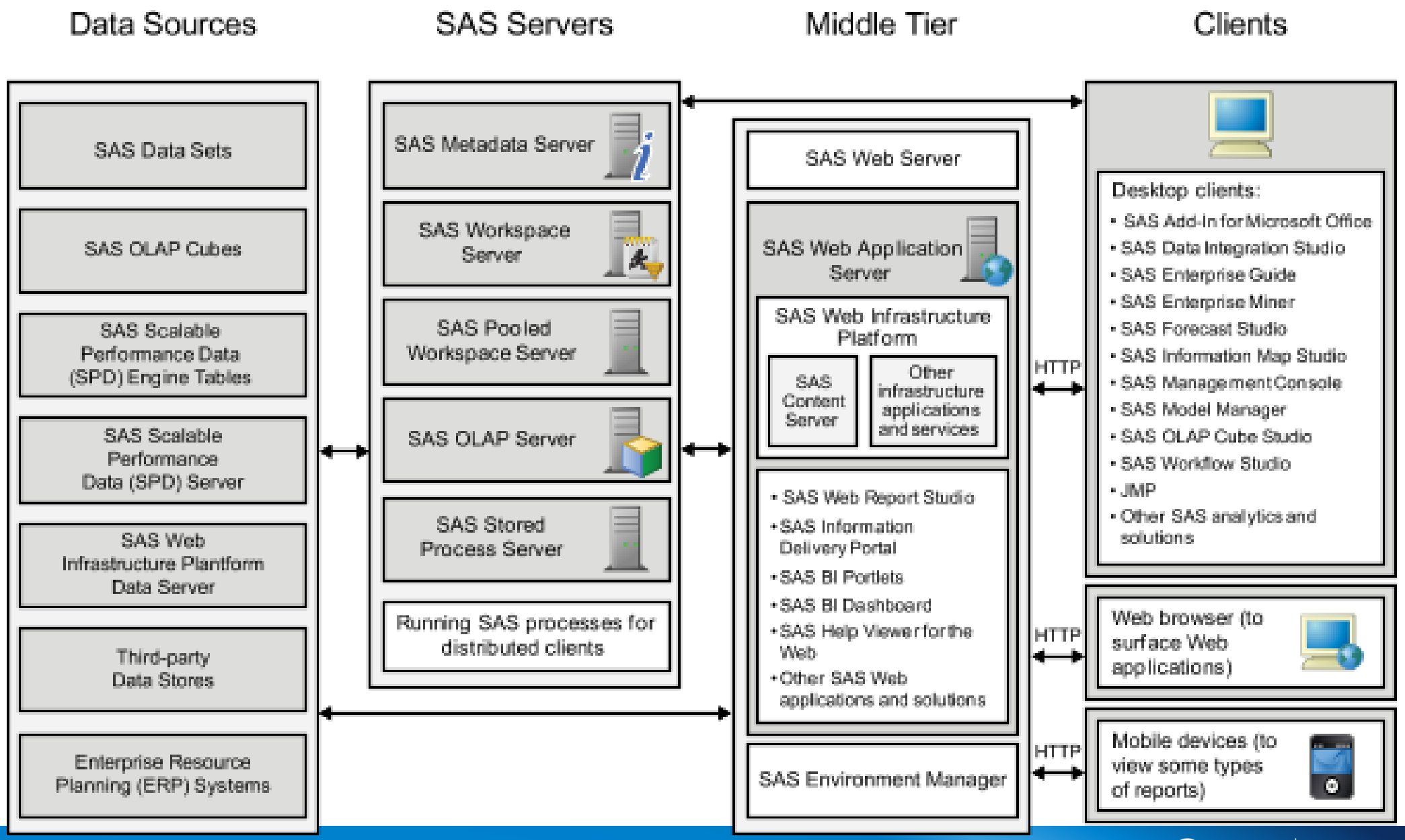
9.3 AND 9.4 MID TIER

PETER HOBART
SAS UK

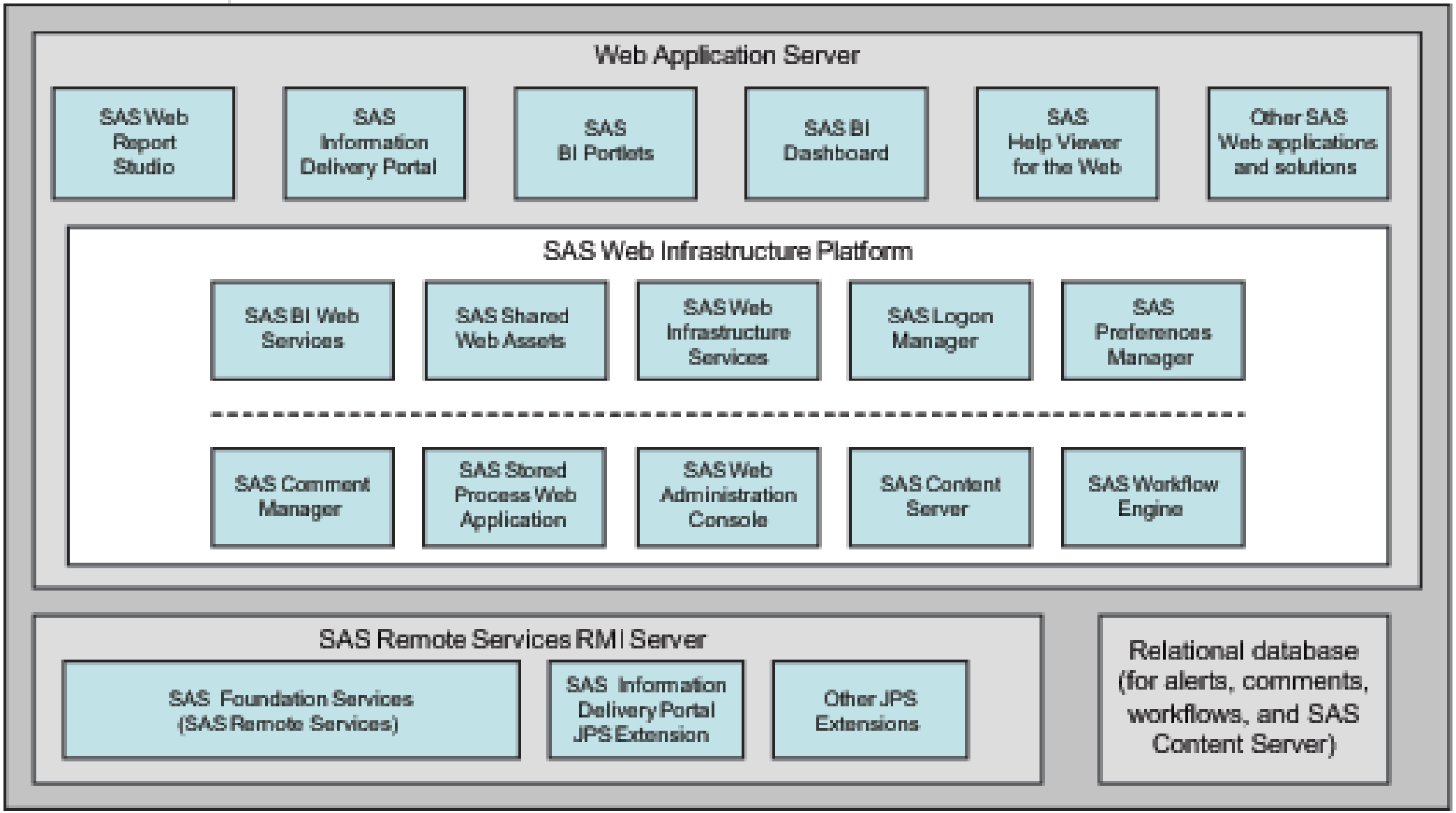
9.3



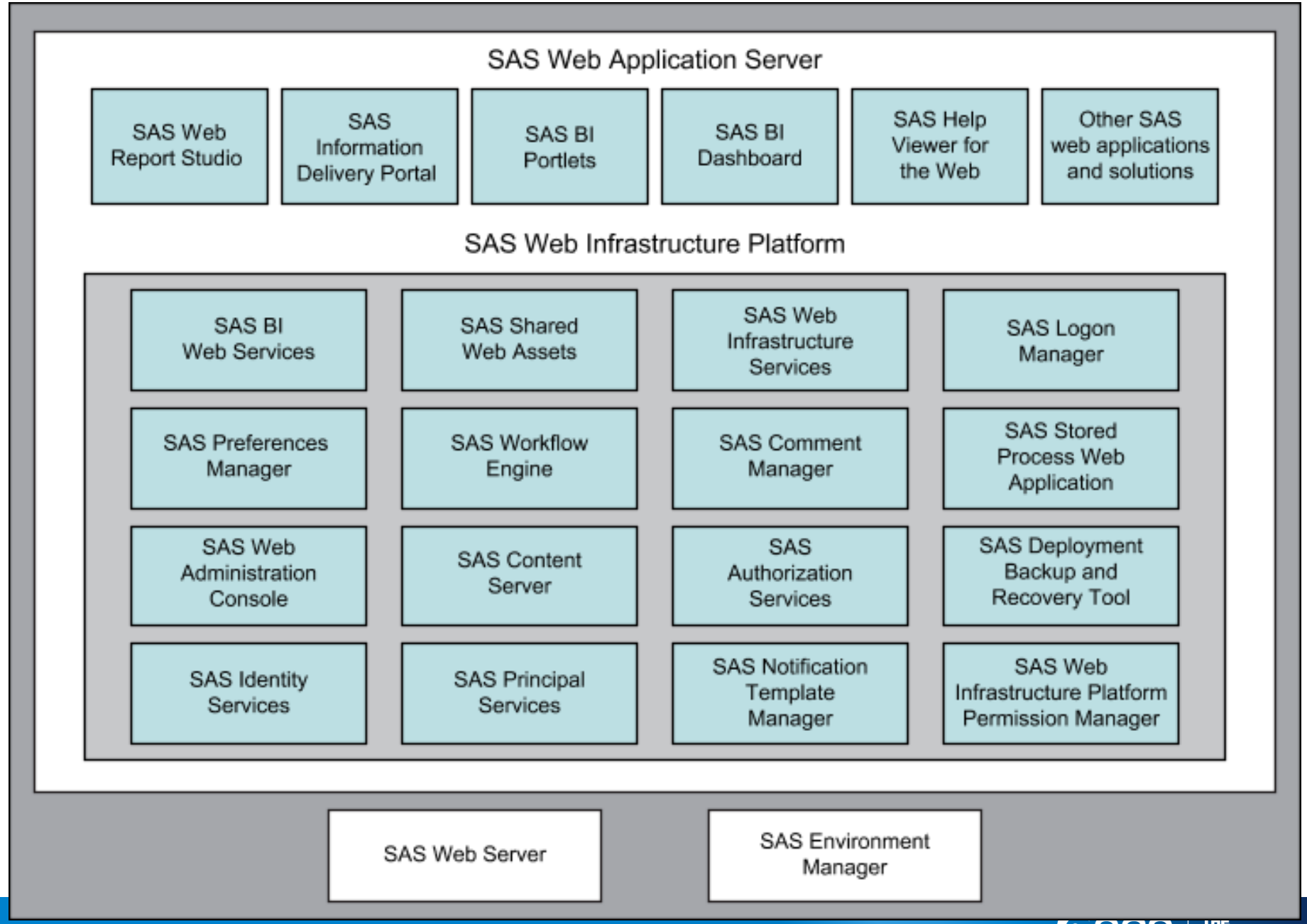
9.4



9.3



9.4



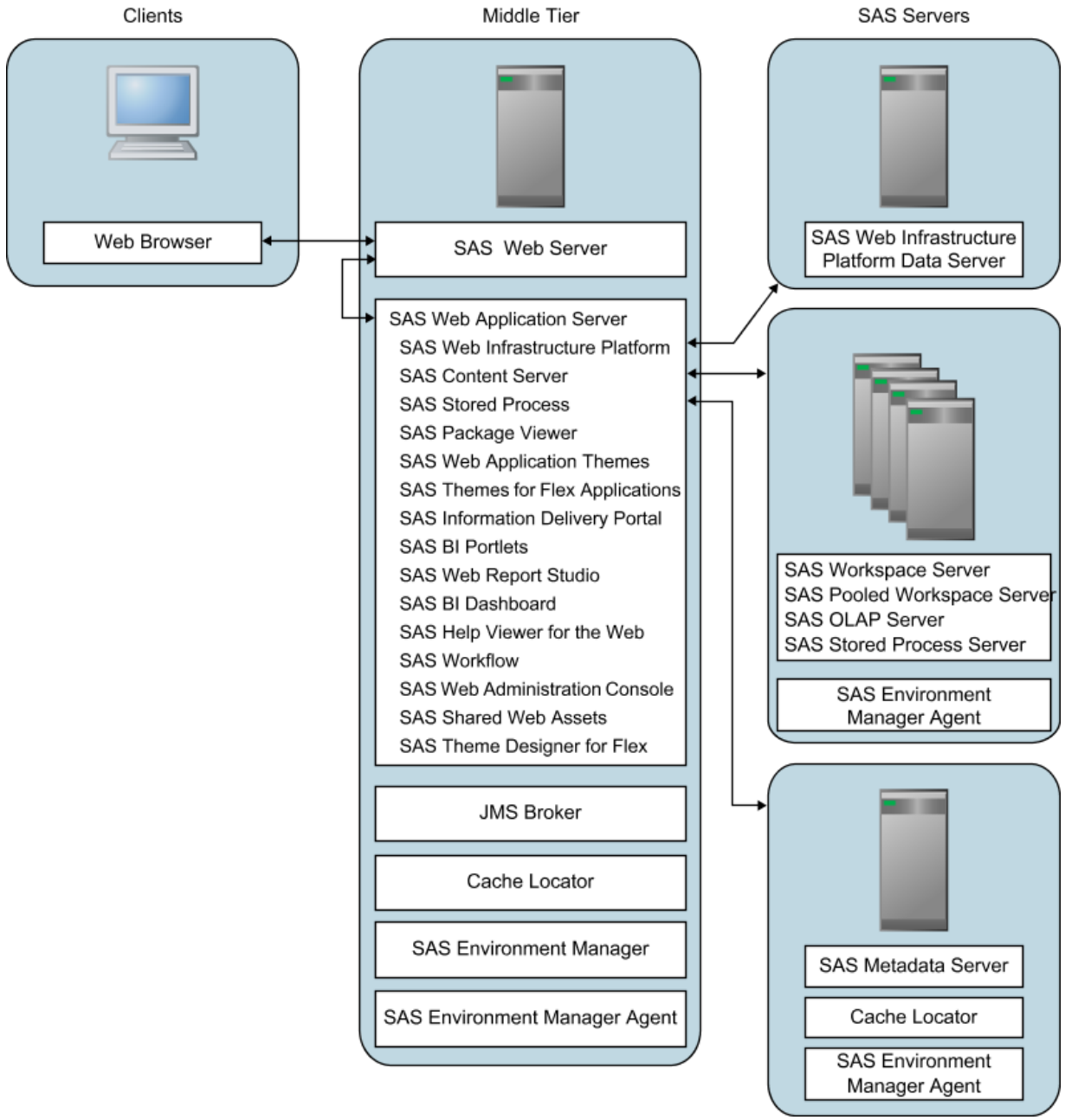
MID - TIER COMPONENT COMPARISON

9.3	9.4
SAS BI Web Services for Java	SAS BI Web Services for Java
SAS Content Server	SAS Content Server
SAS Logon Manager	SAS Logon Manager
SAS Preferences Manager	SAS Preferences Manager
SAS Shared Web Assets	SAS Shared Web Assets
SAS Stored Process Web Application	SAS Stored Process Web Application
SAS Web Administration Console	SAS Web Administration Console
SAS Web Infrastructure Platform Services	SAS Web Infrastructure Platform Services
SAS Workflow	SAS Workflow
SAS Foundation Services	SAS Foundation Services
	SAS Authorisation Service
	SAS Deployment Backup and Recovery Tool
	SAS Identity Services
	SAS Principal Services
	SAS Notification Template Editor
	SAS Web Infrastructure Platform Permission Manager
SAS Remote Services	SAS Remote Services (optional, not required)

DESIGN PATTERNS

- Trade - off between
  - Security
  - Resilience
  - Complexity
  - Hardware Costs
  - Installation effort

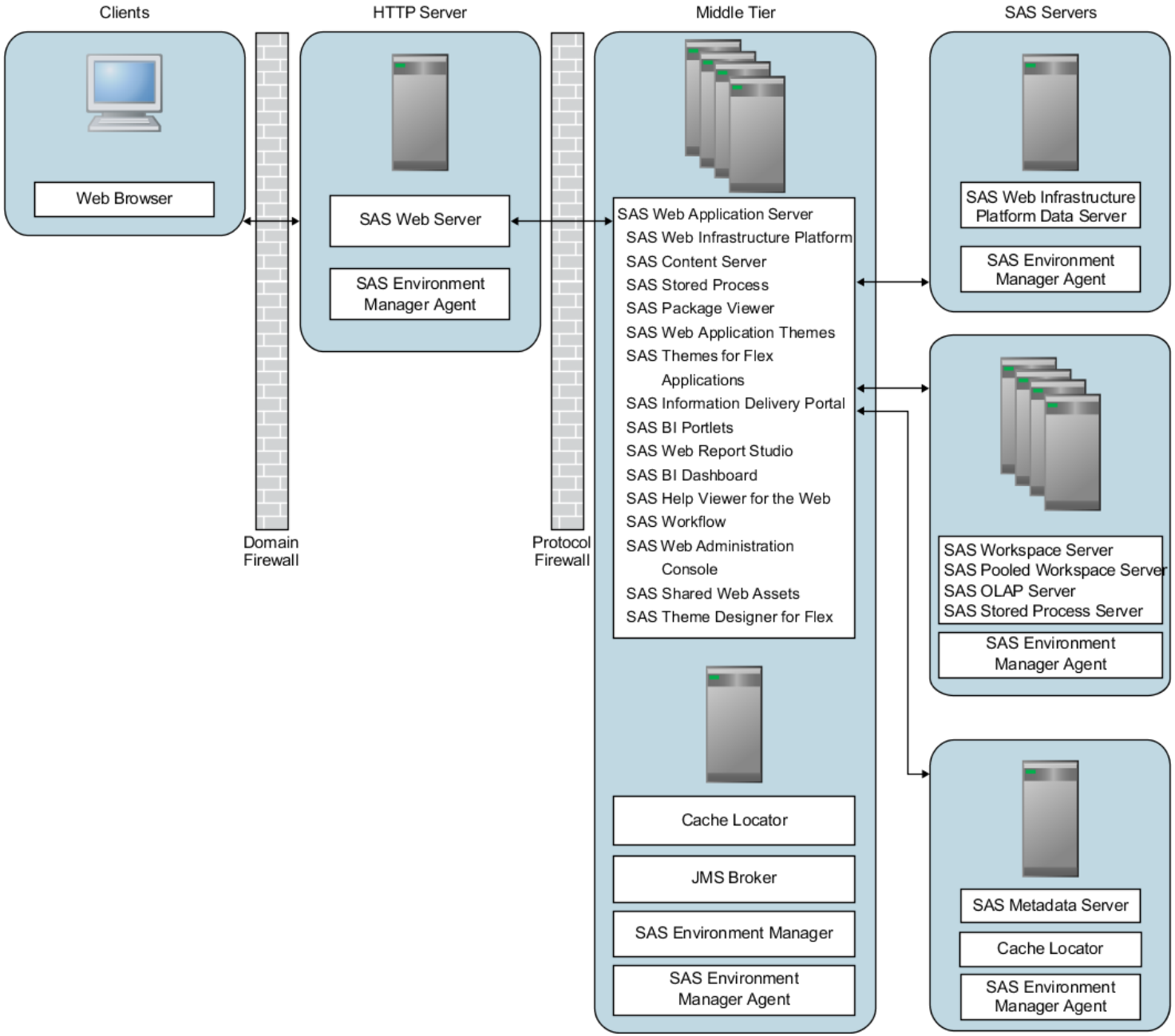
SCENARIO 1: SIMPLE



SCENARIO 1: SIMPLE

Topic	+	-
Security	Reverse proxy provides a layer of security. Network on the middle-tier server can be configured to reject HTTP packets that do not originate from the reverse proxy. SSL can be enabled on the client side of the reverse proxy without affecting the work load on the WAS or the performance of the SAS Web applications. Web app server and SAS Web applications can perform Web authentication for SSO to SAS Web applications and other Web resources in the network.	Adding firewalls to the network is a good next step
Performance	Response time is improved because processing static content is offloaded from the Web application server to the reverse proxy.	As with (1) all SAS Web appls are deployed to a single WAS instance. However, a second managed server instance can be configured, as mentioned in the scenario 1 section.
Scalability	There are no advantages in this scenario, but the topology provides an upward path to clustering Web application servers.	This topology does not support hundreds of concurrent users
Availability	None	This topology has no provision for planned or unplanned down time
Maintainability	SAS Deployment Wizard can still automate configuration & deployment of the WAS and SAS Web applications.	After manual or automatic installation and configuration with the SAS Deployment Wizard, there are manual steps to perform. The reverse proxy must be configured with the connection information for the SAS Web applications.

SCENARIO 2 : SCALABLE / SECURE



SCENARIO 2

Topic	+	-
Security	The SAS Web applications and the Web application server cluster are protected by the DMZ. The Web application server and SAS Web applications can be configured to perform Web authentication for single sign-on to SAS Web applications and other Web resources in the network.	None
Performance	Response time is improved because processing static content performed by the reverse proxy and because of the greater computing capacity of the Web application server cluster.	None
Scalability	Once the cluster of Web application servers is established, additional managed servers can be added to the cluster to support larger numbers of concurrent users.	None
Availability	Clustering provides fault isolation that is not possible with a single Web application server. If a node in the cluster fails, then only the users with active sessions on that node are affected. You can plan downtime for maintenance by taking managed servers offline. New requests are then directed to the SAS Web applications deployed on the remaining nodes while maintenance is performed.	None
Maintainability	Configuration and deployment of the first Web application server and the SAS Web applications can still be automated with the SAS Deployment Wizard. This first Web application server can be cloned to speed the creation of the cluster.	None

LOAD BALANCING

- The SAS 9.4 **Web Application servers** can be load - balanced by the SAS HTTP server, improving scalability and resilience.
  - Session affinity is handled by the SAS HTTP server
  - The HTTP server represents a "single point of failure"
- Load balancing the **SAS HTTP server** requires third - party components e.g. f5 BIG_IP

  See more at http://support.sas.com/documentation/cdl/en/bimtag/66823/HTML/default/viewer.htm#n0axzi2o0wubxan1cgaovjqqjfho.htm

WEB INFRASTRUCTURE PLATFORM DATABASE OPTIONS

- The SAS WIP Data Server and SAS Content Server in 9.4 use a database as a persistent store
  - PostgreSQL 9.1.9. (supplied by default)
  - The WIP can be configured to use a third-party vendor database
    - Oracle
    - MySQL
    - DB2
    - SQL Server
    - PostgreSQL

MULTICAST

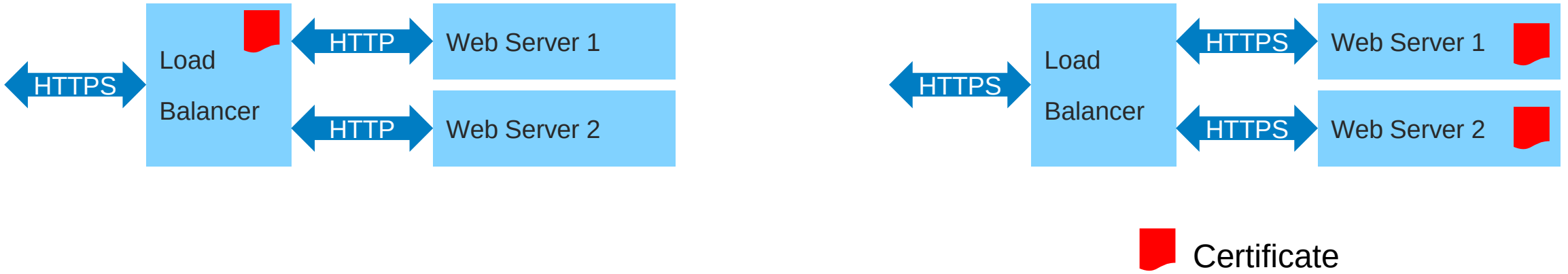
- SAS 9.2 and 9.3 require multicast for the mid - tier components to communicate
- Multicast communication is no longer used to communicate among SAS 9.4 middle-tier applications in a single SAS deployment (the set of applications connected to the same SAS Metadata Server)
- In SAS 9.4 multicast is turned off by default but is available if any customer - created custom applications require it

SECURITY

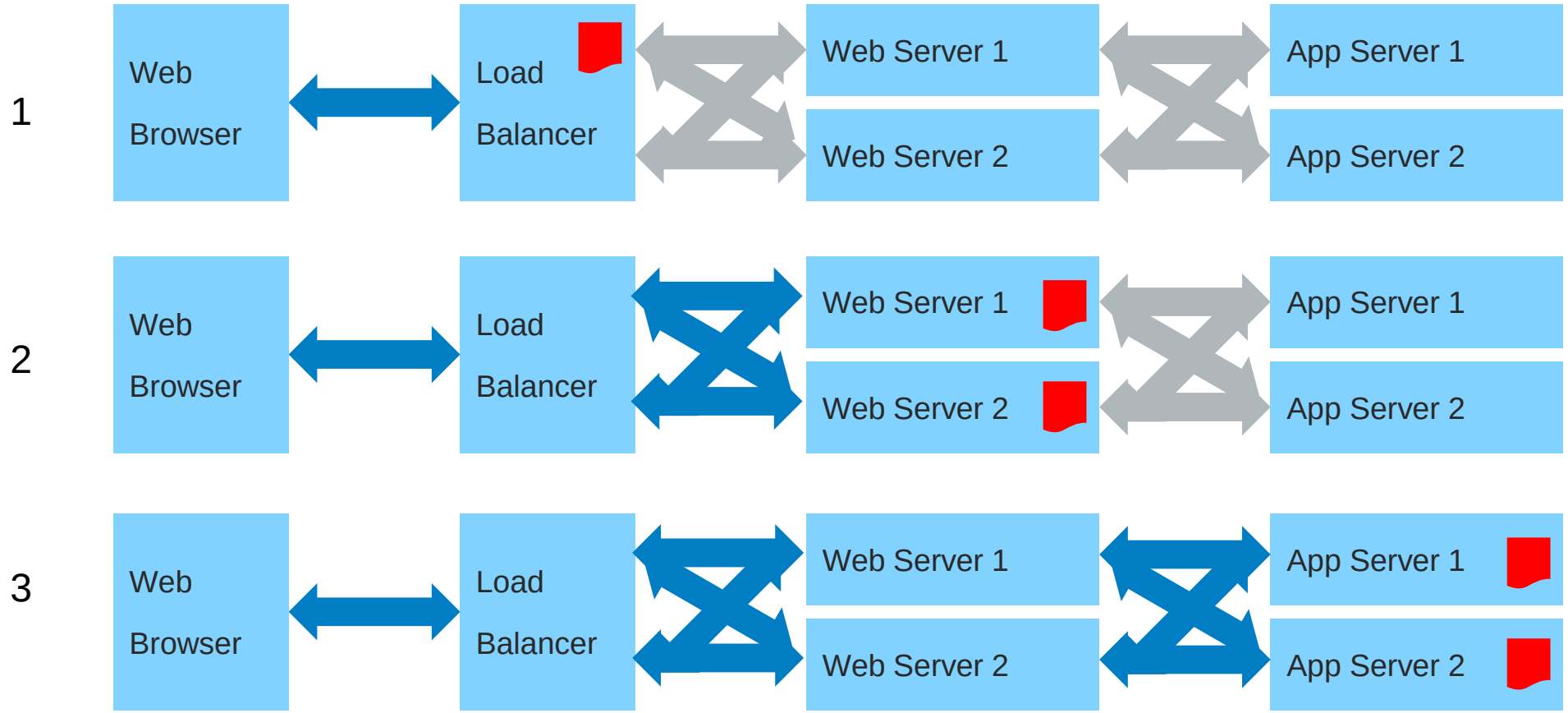
- Passwords in configuration files and metadata are encrypted or encoded
- Passwords in transit to and from SAS servers are encrypted or encoded. You can choose to encrypt all such traffic, instead of encrypting only credentials.
- SAS HTTP server can be configured to use HTTPS/TLS (1-way SSL)
  - Automatically during installation
  - Manually post - installation
- SAS WAS can be manually configured to use HTTPS/TLS (2-way SSL)

SECURITY AND LOAD - BALANCING

- If HTTPS is to be used, certificates must be available for the installation to proceed.
- If a load - balancer is to be used with HTTPS then the termination point for HTTPS (and therefore the location of certificates) must be defined.



POSSIBLE CONFIGURATIONS IN DETAIL



Configurations 1 and 3 are preferred

AGENDA

- Authentication
  - Inbound authentication
  - Outbound authentication
- Single Sign-on

DEFINITIONS

Stage	Process	Method	Physical world
Authentication	Verifying a person's identity	ID/Password Security Token	ID card, passport
Identification	Matching identity to a SAS metadata identity	Text - based comparison	Check person against a "guest list"
Authorisation	Allowing actions based on identity	Grant or deny of an action	Door unlocked, gate opened

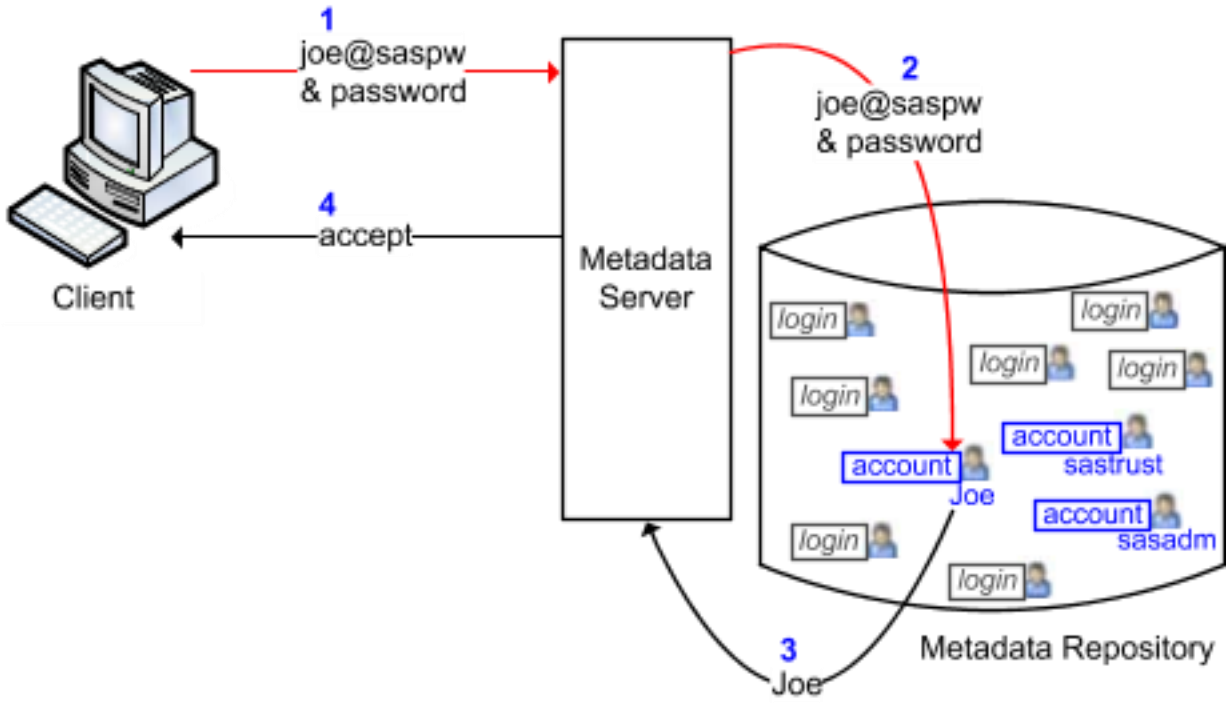
A user will go through all three phases when using SAS
We will only deal with authentication today

AUTHENTICATION

AUTHENTICATION

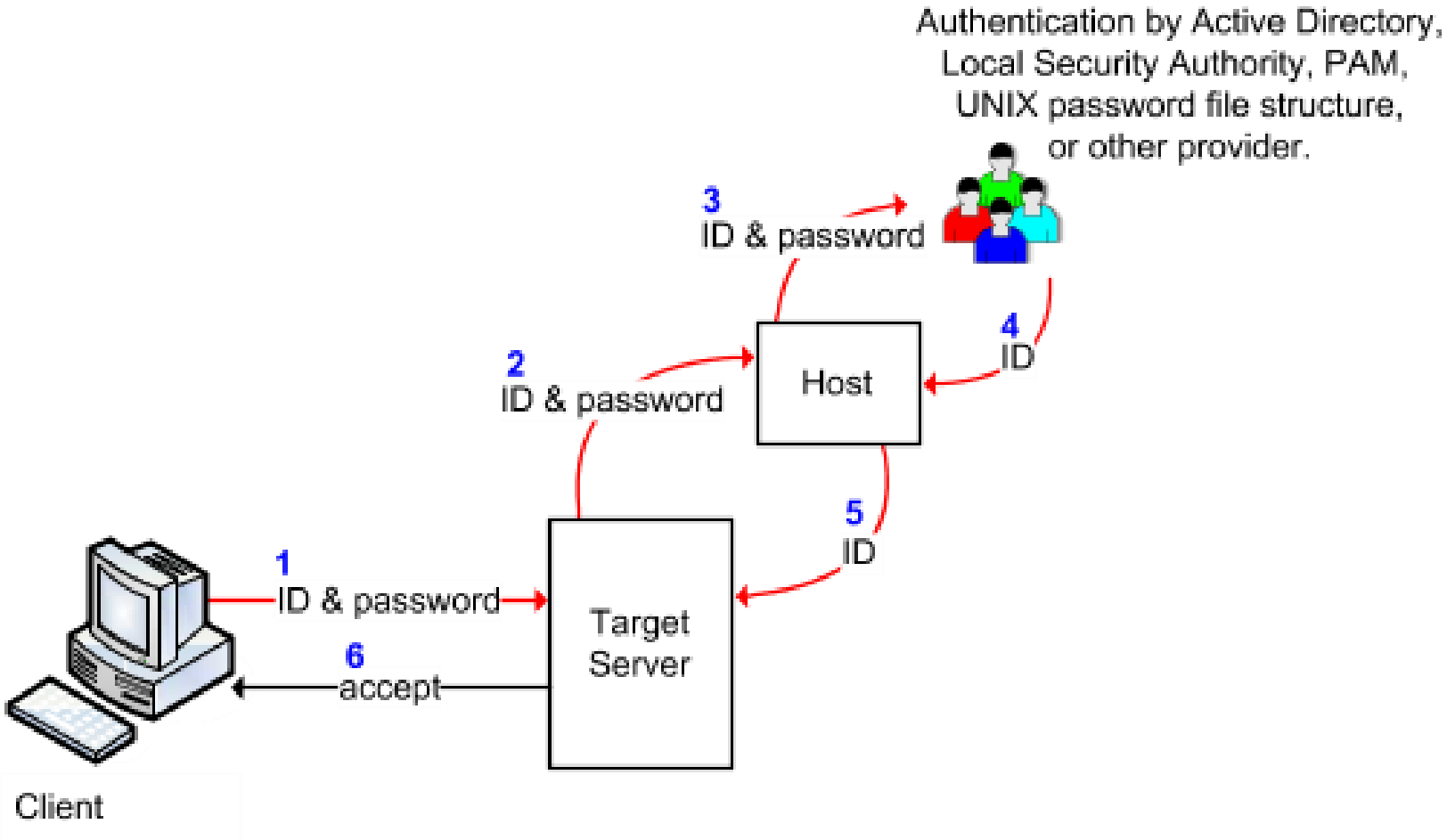
INBOUND AUTHENTICATION: INITIAL CONNECTION TO A METADATA SERVER

SAS INTERNAL AUTHENTICATION

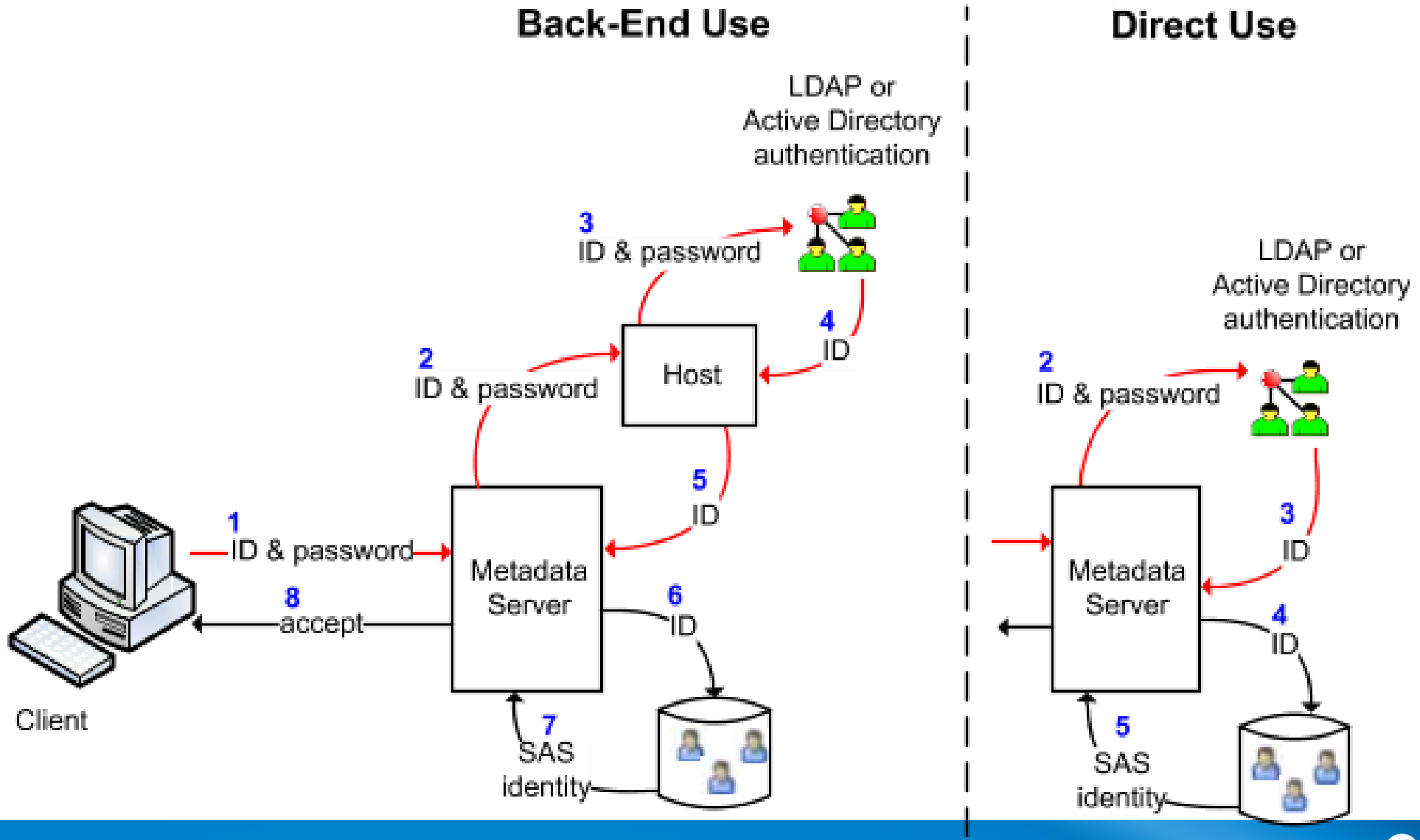


Internally authenticated SAS accounts are special purpose accounts. They cannot launch OS processes such as Workspace servers under their own identity. Examples of internal accounts are
sasadm@saspw - Used for SAS metadata administration
sastrust@saspw -Used for SAS server to SAS server communication

INBOUN
CRE



DIRECT AUTHENTICATION



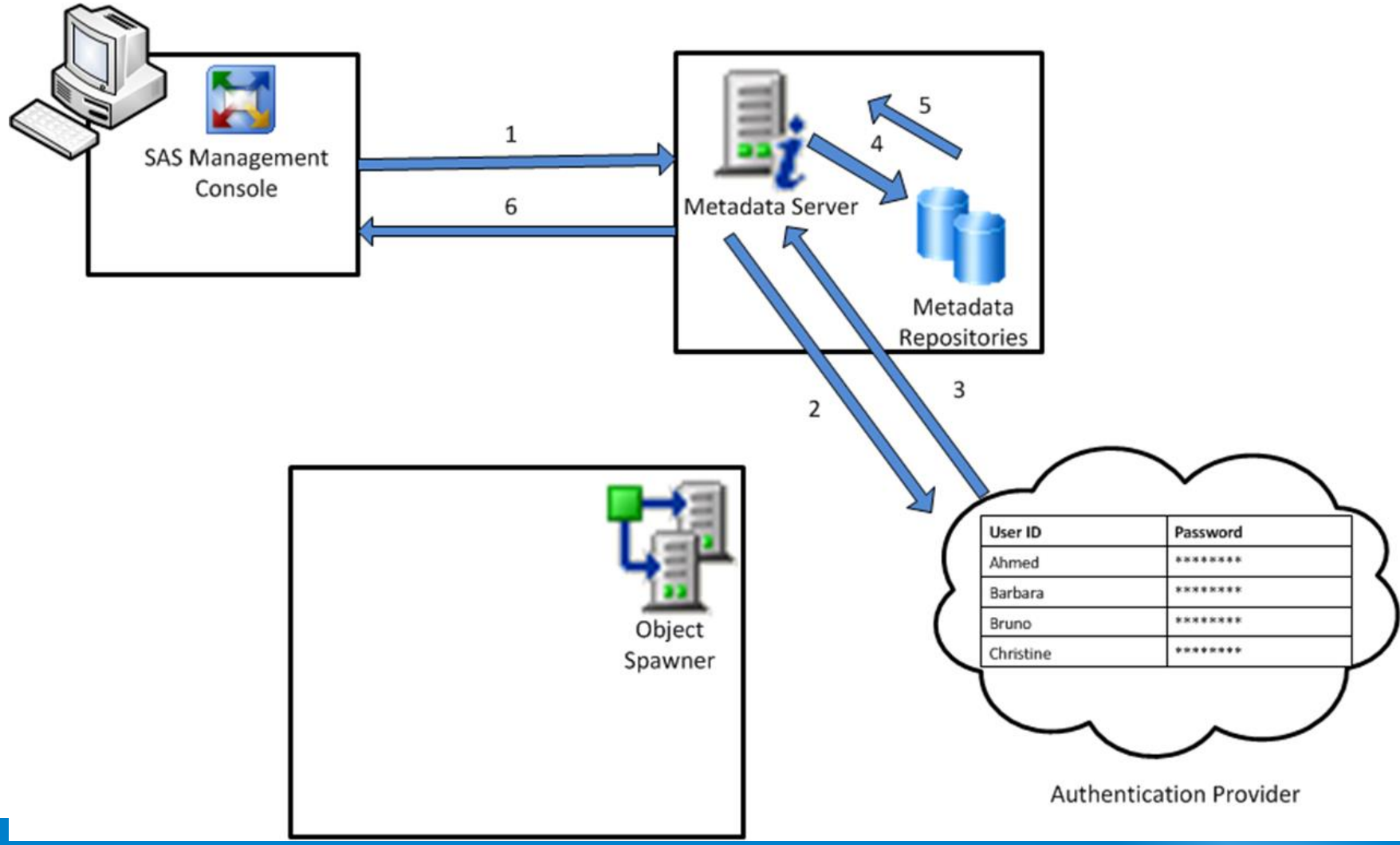
AUTHENTICATION

OUTBOUND AUTHENTICATION: CONNECTING TO A RESOURCE IN THE SAS ENVIRONMENT

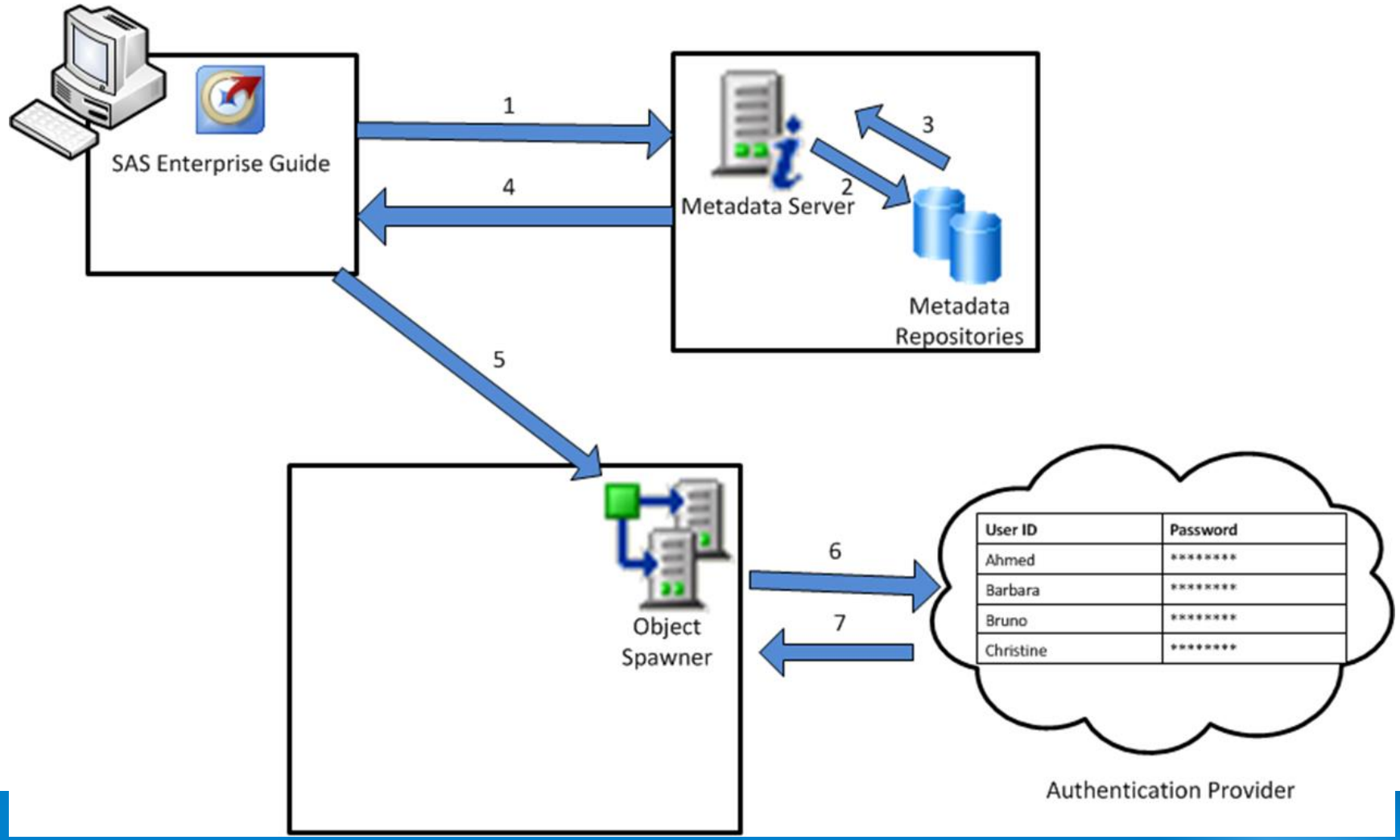
OUTBOUND AUTHENTICATION

- Outbound authentication is establishing a connection to a server after initial authentication to the metadata server
- Inbound authentication is a pre-requisite of outbound authentication.

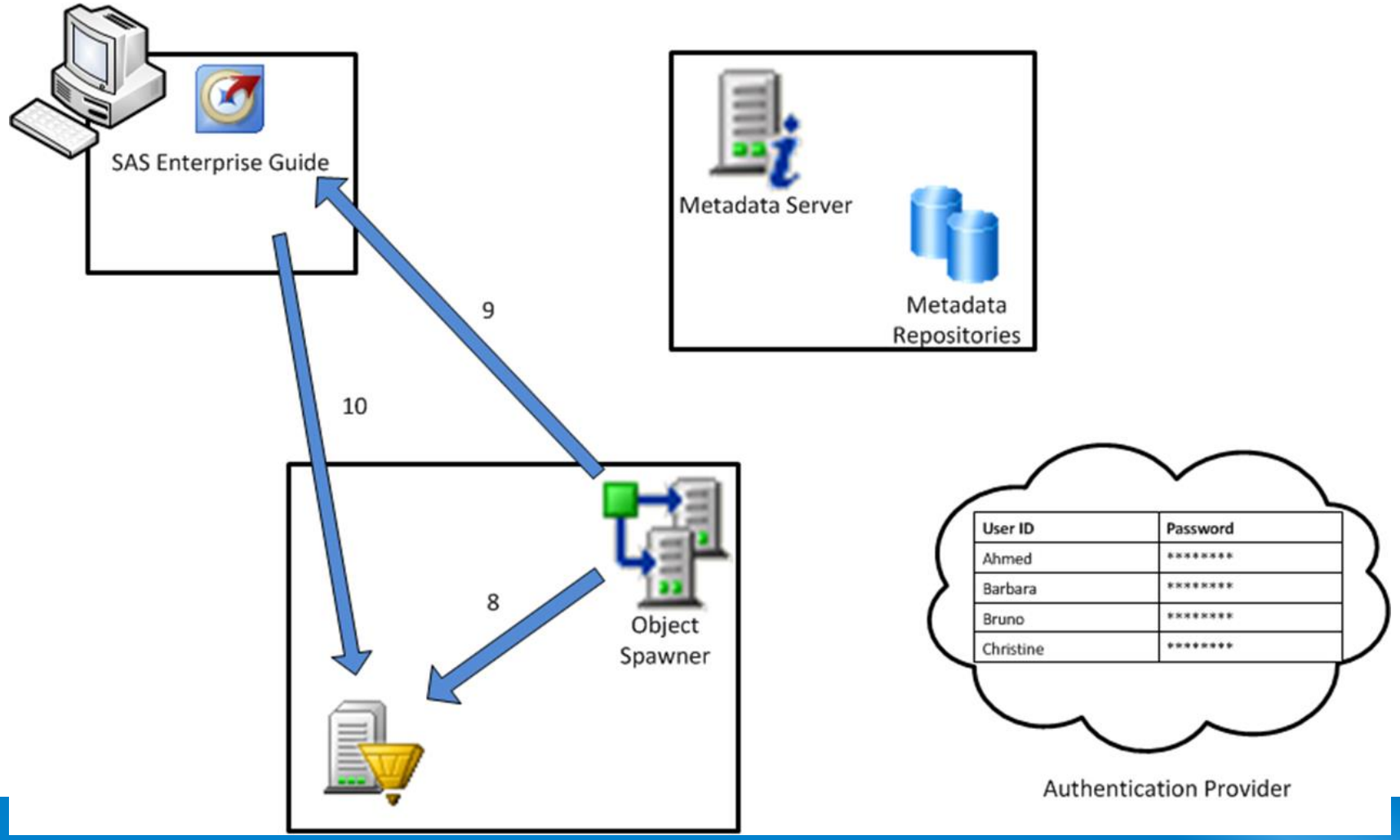
RECAP: INBOUND AUTHENTICATION



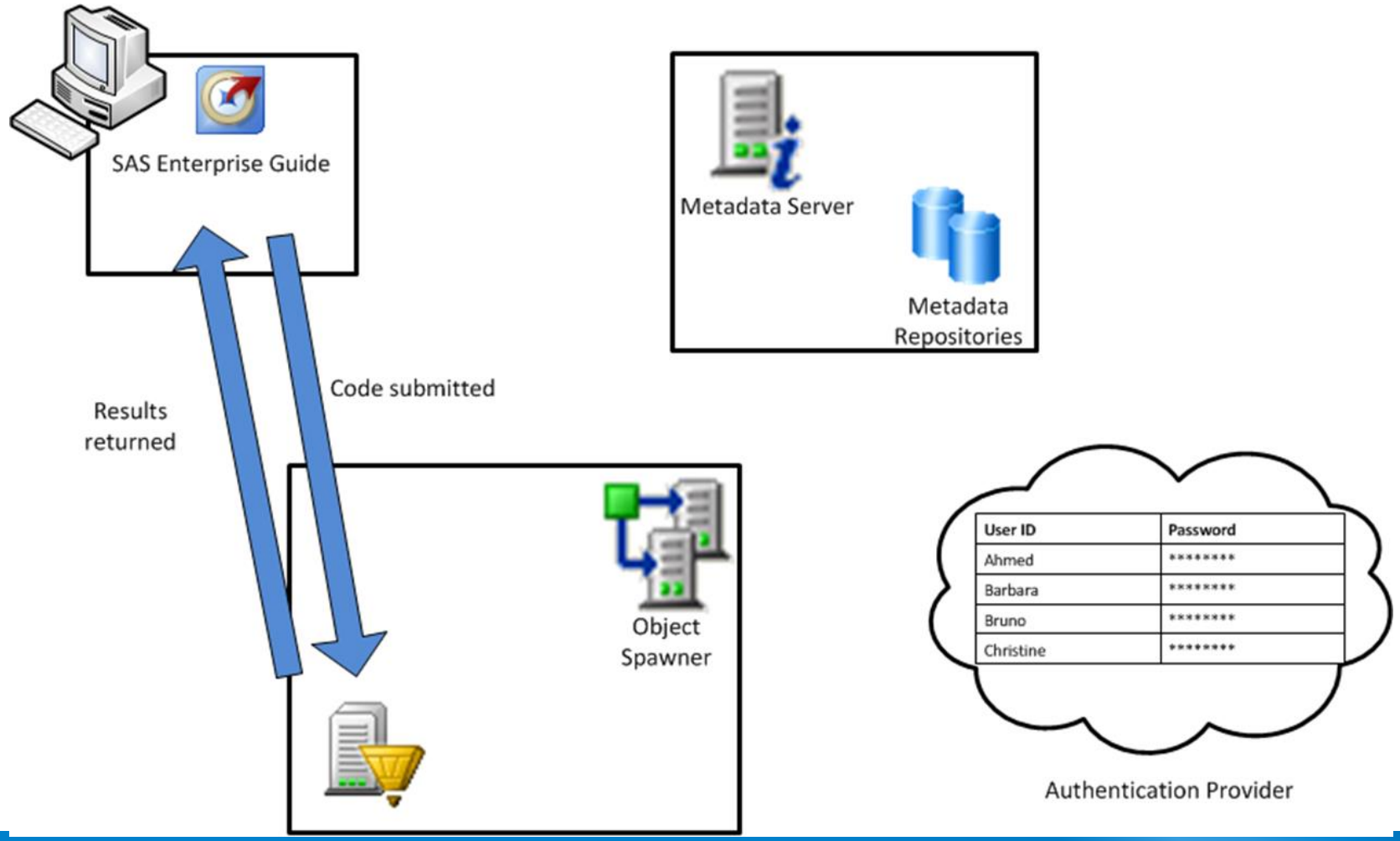
OUTBOUND AUTHENTICATION TO A STANDARD WORKSPACE SERVER



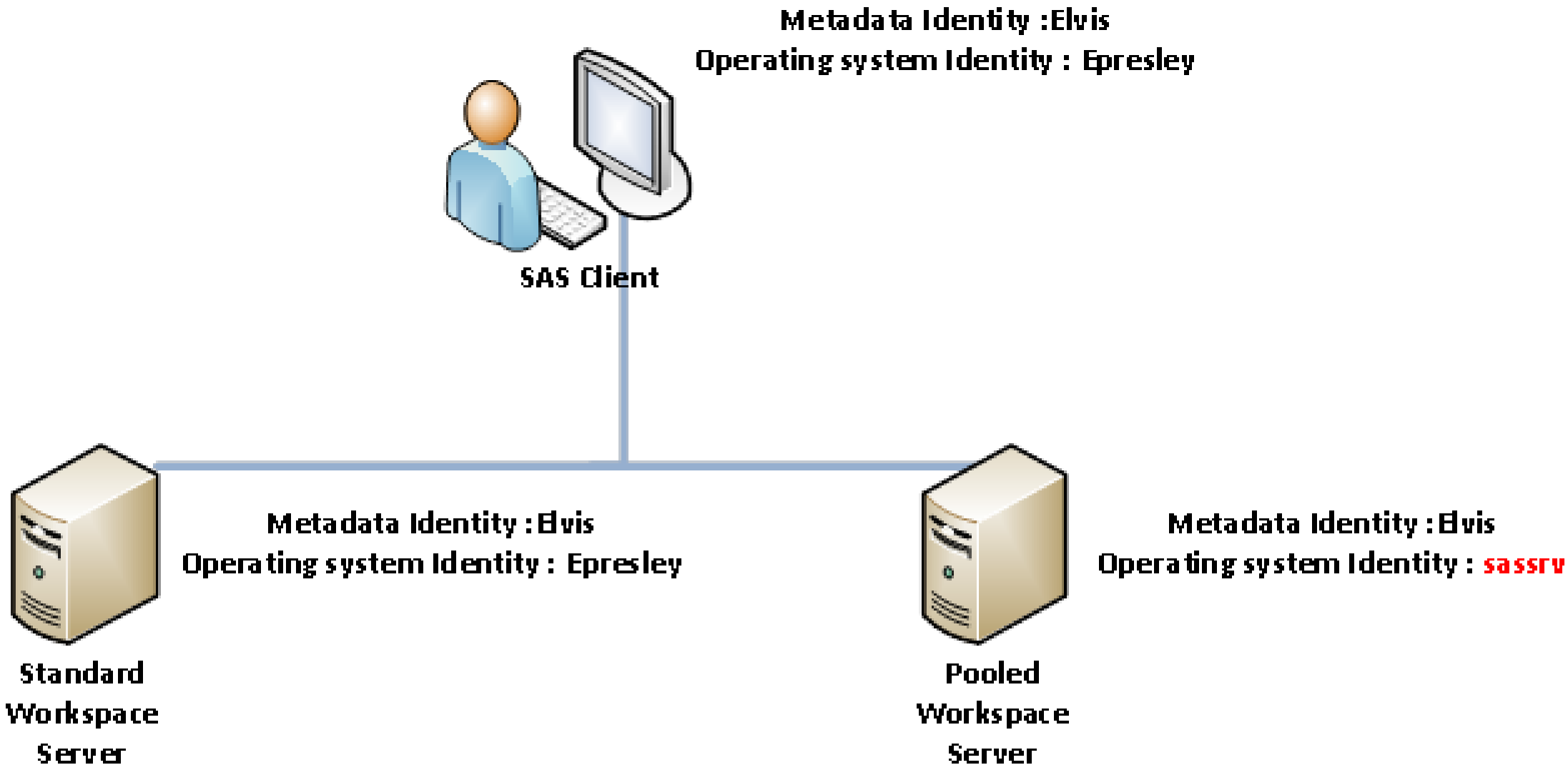
OUTBOUND AUTHENTICATION TO A STANDARD WORKSPACE SERVER



OUTBOUND AUTHENTICATION TO A STANDARD WORKSPACE SERVER



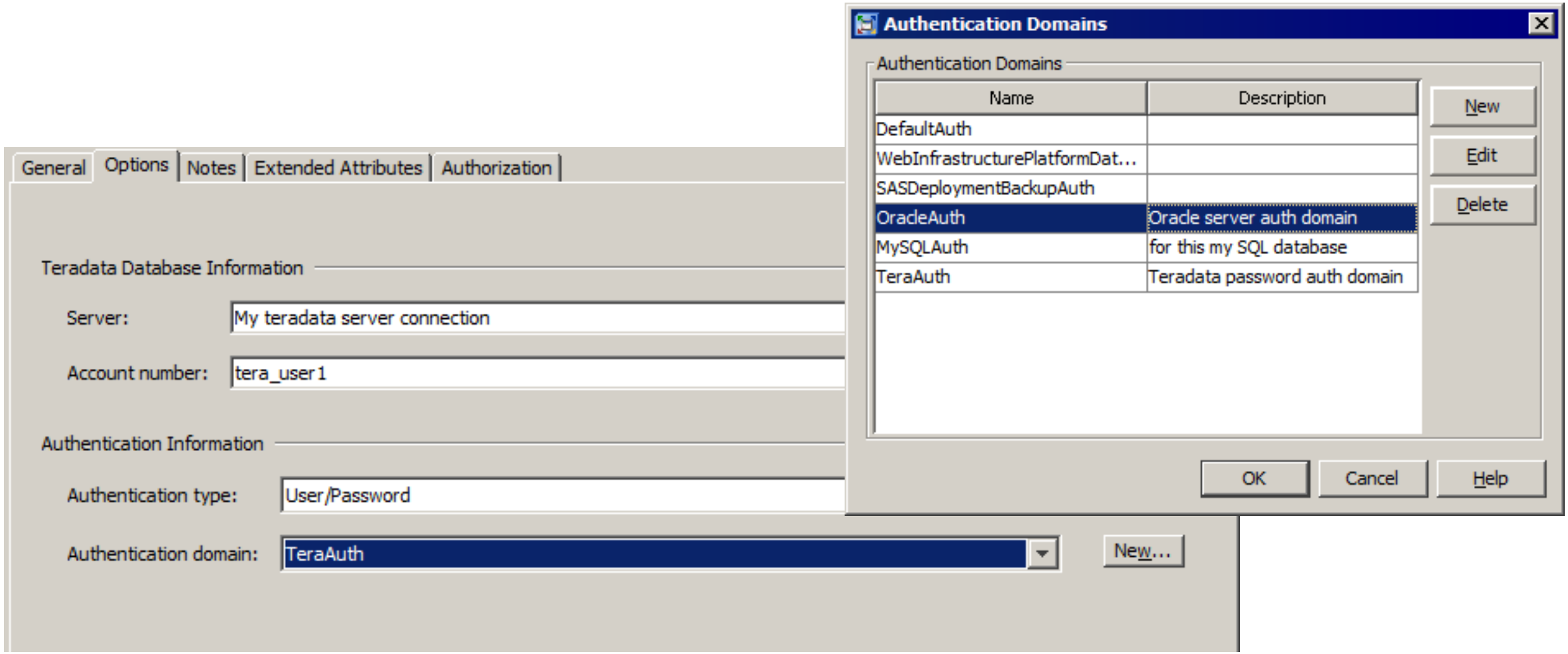
WHAT IS A "STANDARD" WORKSPACE SERVER?



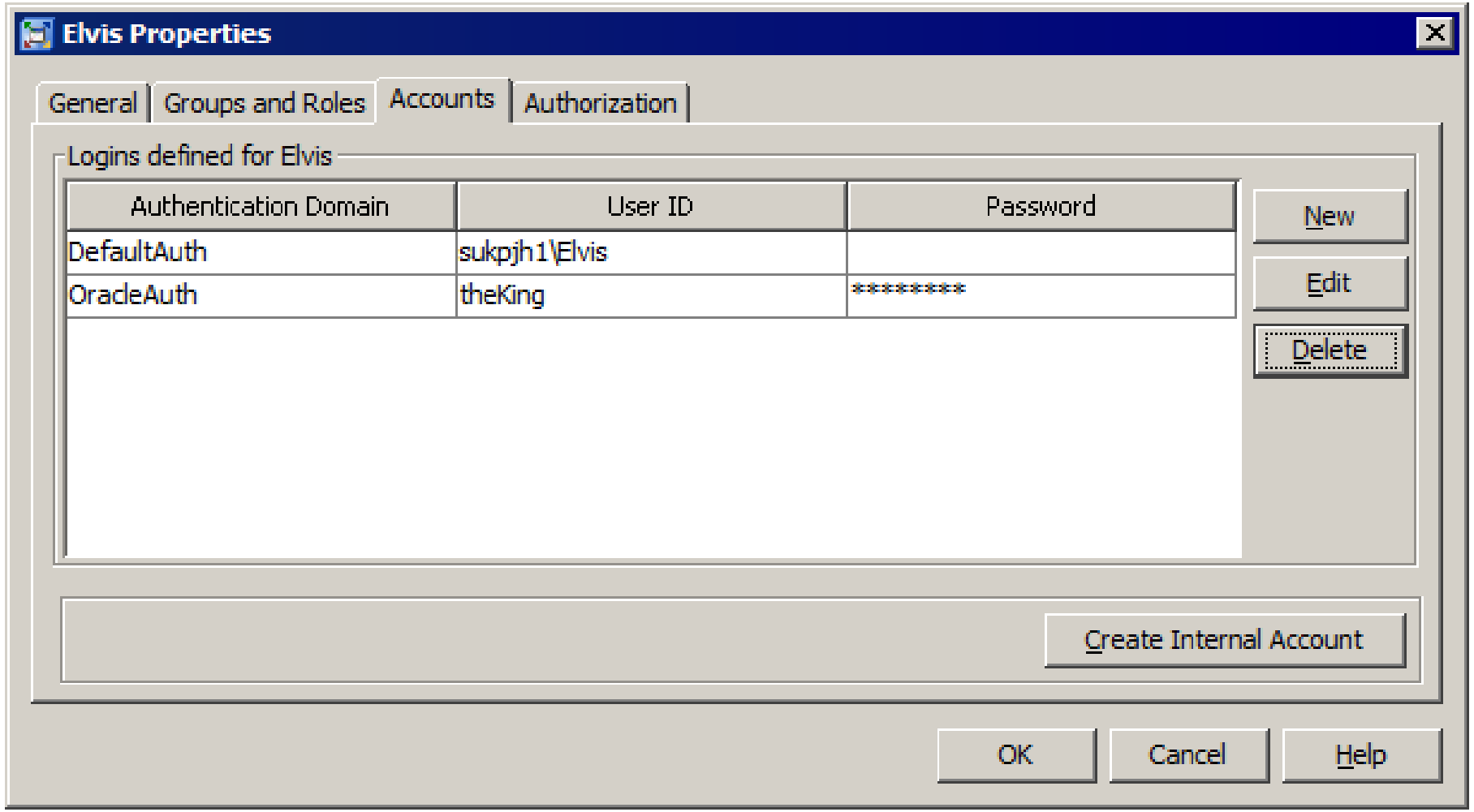
CREDENTIAL MANAGEMENT

Method	
Re-use (credential caching)	The credentials used to authenticate to the metadata server are presented to the new server
Retrieve	Credentials associated with - The user or a user's groups - The server's authentication domain Are retrieved from the metadata server and presented to the new server
Request	The user is presented with a prompt and asked to provide a user ID and password

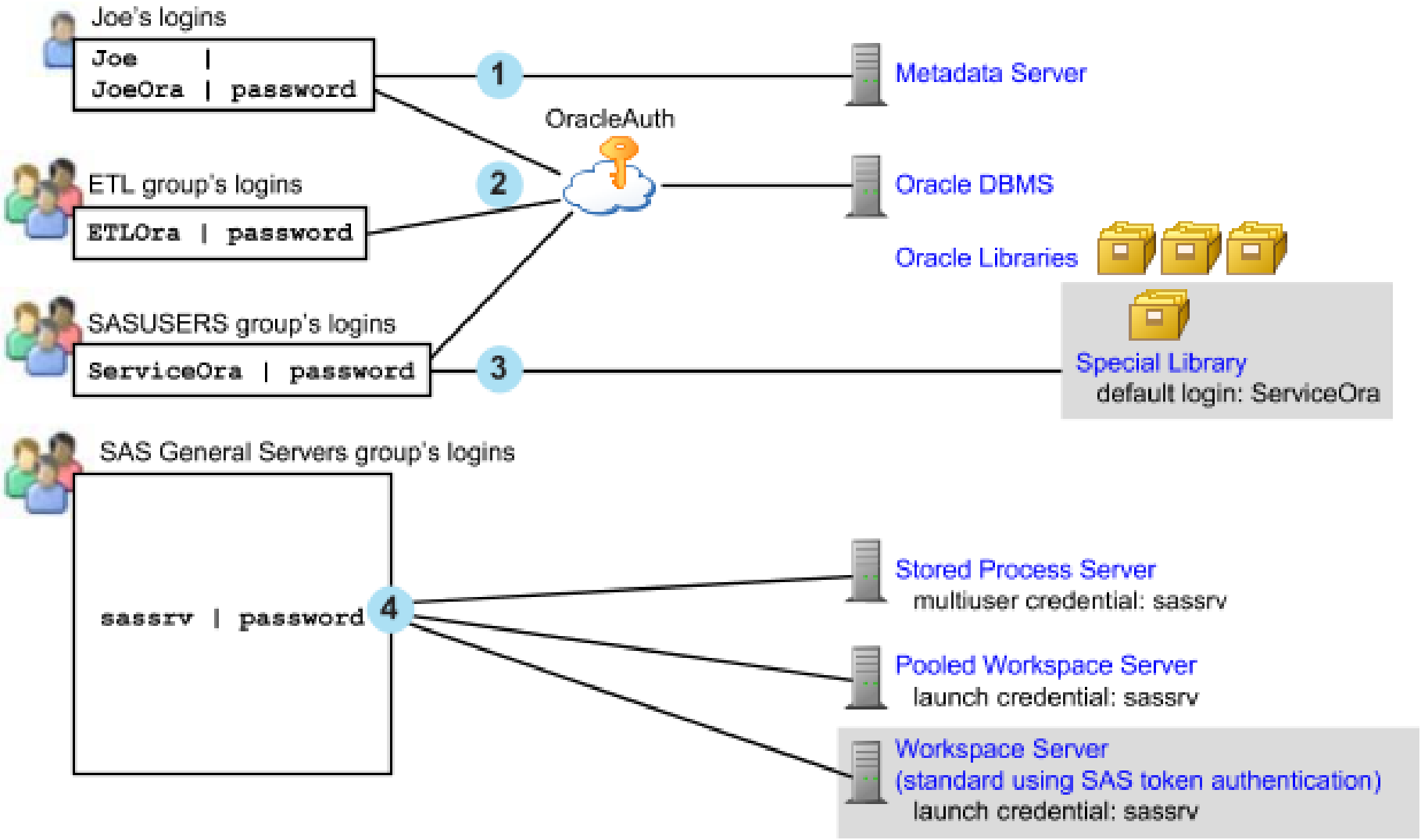
SAS AUTHENTICATION DOMAINS



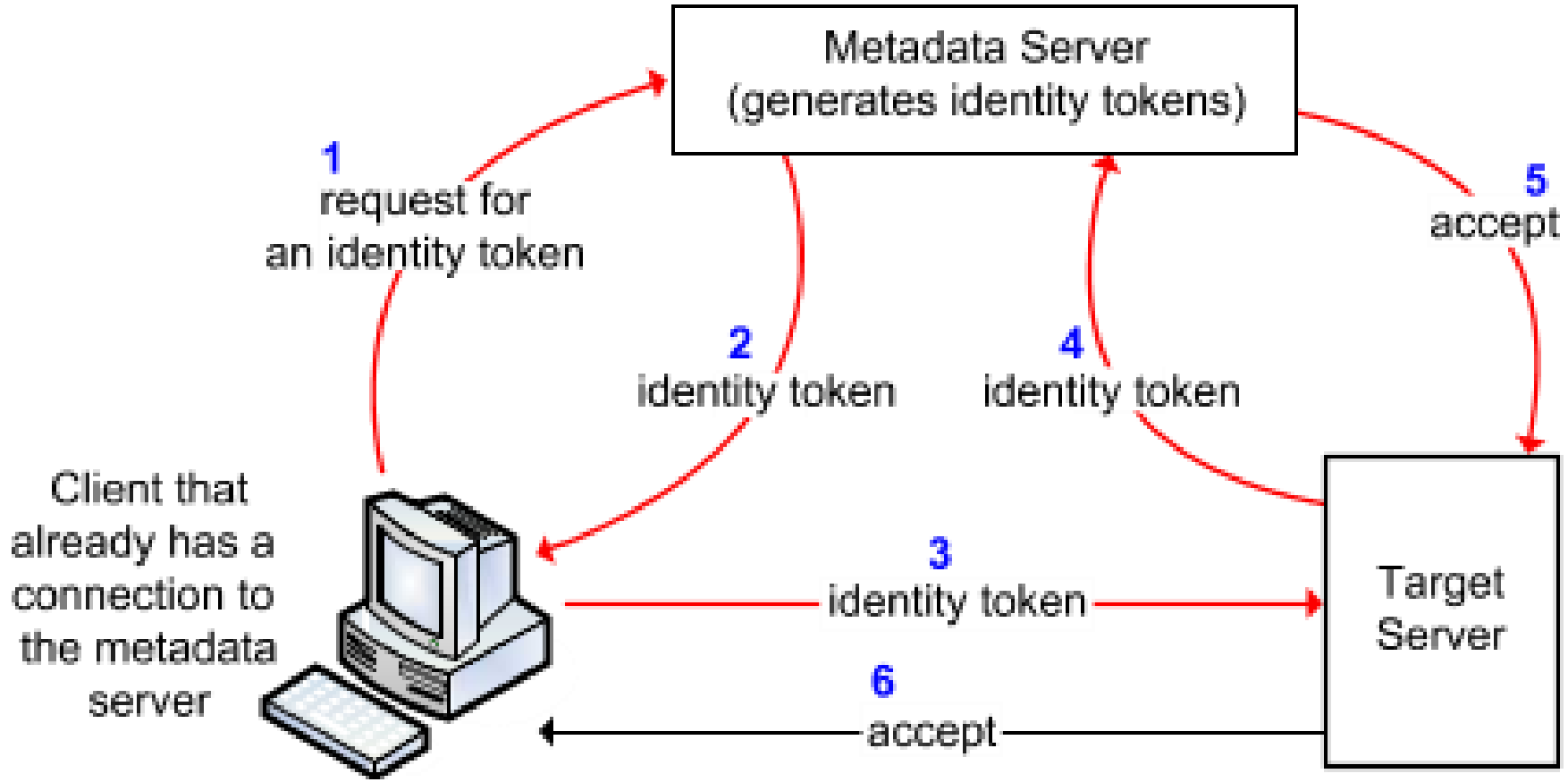
SAS AUTHENTICATION DOMAINS



CREDENTIAL MANAGEMENT



SAS TOKEN AUTHENTICATION

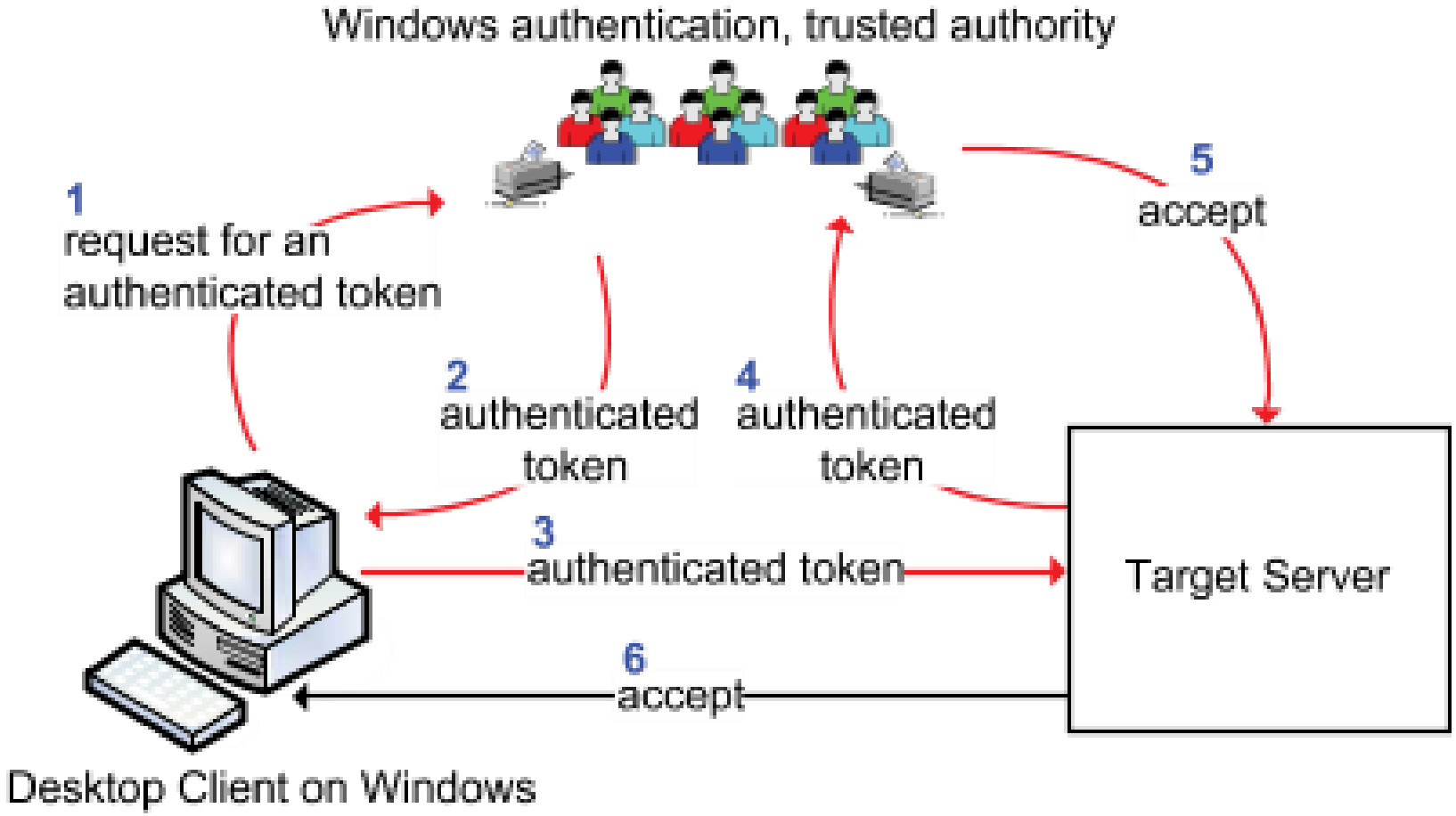


The metadata server generates and validates a single-use identity token for each authentication event. This has the effect of causing participating SAS servers to accept users who are connected to the metadata server.

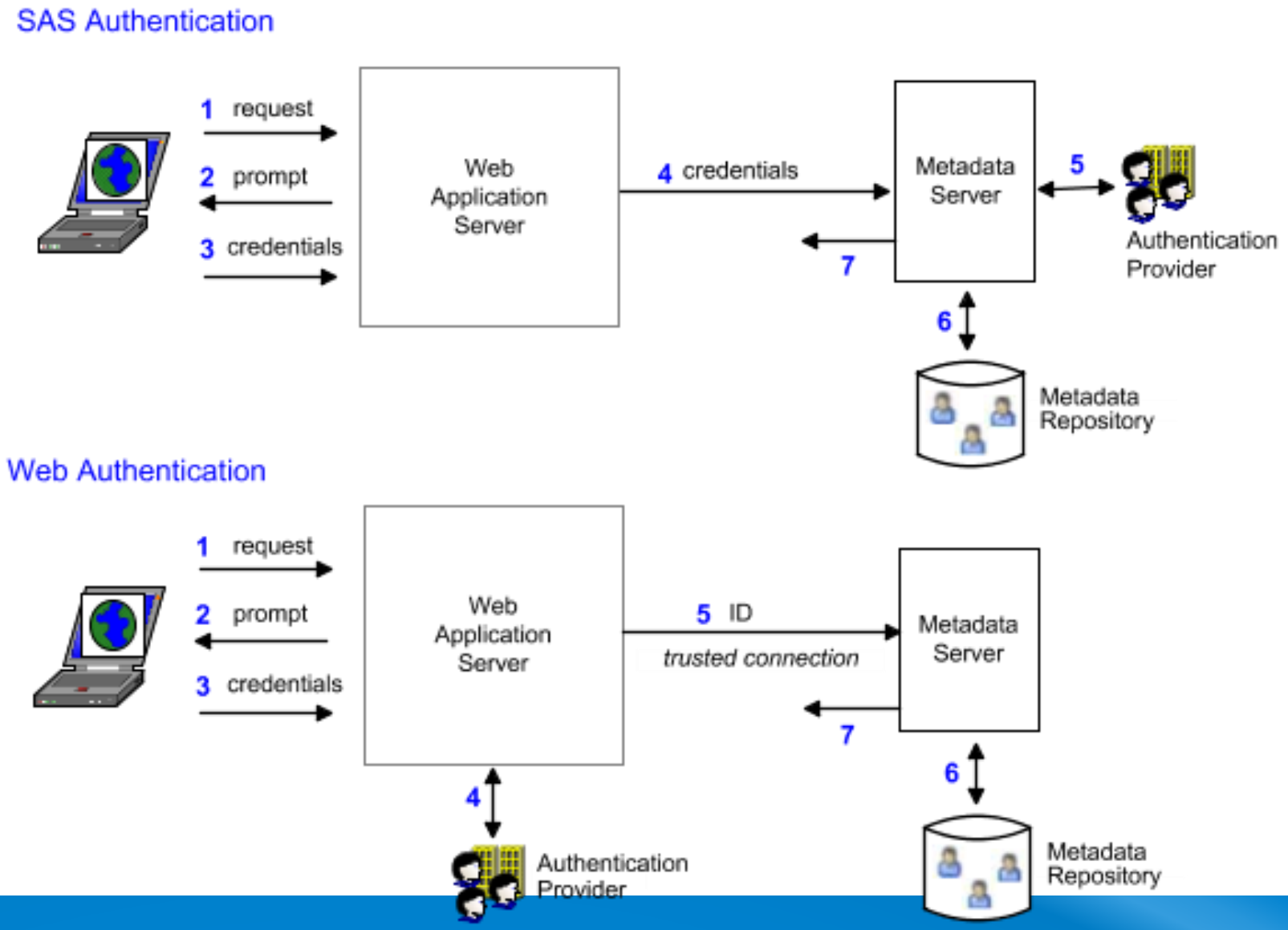
SAS TOKEN AUTHENTICATION

Scope	Primarily used for metadata-aware connections to the stored process server, the server-side pooled workspace server, the OLAP server, the content server, and (in a specialized configuration) the standard workspace server. Also used by launched servers to connect back to the metadata server (for example, from the workspace server to the metadata server for library pre-assignment).
Benefits	Preserves client identity for metadata layer access control and auditing purposes. No individual external accounts are required, no user passwords are stored in the metadata, and no reusable credentials are transmitted.
Limits	On the workspace server, reduces granularity of host access. Supported only for metadata-aware connections (in which the client learns about the target server by reading the server's metadata definition).
Use	Optional for the workspace server, otherwise mandatory in certain configurations

INTEGRATED WINDOWS AUTHENTICATION



WEB AUTHENTICATION VS. SAS AUTHENTICATION



SINGLE SIGN-ON

SINGLE SIGN - ON TWO DEFINITIONS

- 1. Challenged access, but one password which works everywhere
- 2. Unchallenged access to resources *
  - Thick Client (Java, .Net)
  - Thin client (browser)
  - External data (Oracle, Teradata, Hadoop….)

*This is the default definition used in a SAS architecture design

SUMMARY FOR SINGLE SIGN ON

Feature	Notes
Internal authentication	An internal account cannot participate in IWA or web authentication and cannot launch any OS processes (e.g. standard workspace servers)
SAS token authentication	Facilitates SSO to most SAS servers
IWA	Facilitates silent launch of desktop applications. If not fully configured, prevents SSO to a standard workspace server. Requires a Kerberos implementation.
Web authentication	Facilitates silent launch of web applications. Prevents SSO to a standard workspace server (as the user is not required to have have an OS account on SAS servers).
Direct LDAP authentication	Not compatible with silent launch. Prevents SSO to a standard workspace server
PAM	Can help unify authentication
Credential Management	Facilitates SSO to third-party servers and (in some configurations) workspace servers.

SINGLE SIGN-ON

1. Install / configure effort

	Challenged		Unchallenged using IWA ("Single sign - on")	
Client	**Customer effort**	**SAS effort**	**Customer effort**	**SAS effort**
"FAT"(.NET, Java)	**Configure AD**	**None**	**Configure Kerberos**	**Low**
"THIN" (Browser)	**Configure AD**		**Configure Kerberos**	**Moderate**

2. Will the user have to type their password?

	"Challenged" No credential storage	"Challenged" Credentials stored in SAS profiles	IWA
"FAT" (.NET, Java)	**YES**	**NO (If credentials are stored in the default SAS profile for that user)**	**NO**
"THIN"	**Depends on browser credential caching policy**		**NO**