SAP Afaria, Cloud Edition
SAP Partner Organization

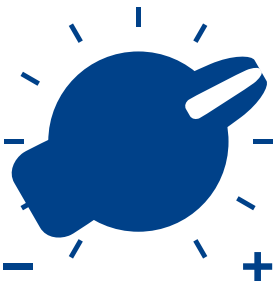
SAP® Afaria®, Cloud Edition

A By-the-Numbers Approach to Security

The Best-Run Businesses Run SAP™

The software-as-a-service (SaaS) approach to software delivery is rapidly gaining popularity in the enterprise software marketplace. Many companies have found that adopting software "on demand" has become not just a viable option but a necessary cornerstone of their IT strategy. The benefits are obvious: drastically reduced start-up costs and no need for a physical infrastructure or the ongoing maintenance for either the operating system or the applications that run on top of it.

Outsourcing part of the IT infrastructure does come with some perceived risk, however, usually in the area of security. The purpose of this technical paper is to describe SAP's approach to maintaining confidentiality, data integrity, and system availability for the SAP® Afaria®, cloud edition, set of solutions. We will take a by-the-numbers approach to security, starting with a solution diagram and describing security features at various points in the solution. SAP believes that we have taken a differentiating approach to enterprise mobility management in the cloud. By the end of this paper, you will too.



Horizontal scaling is fundamental to the SAP Afaria, cloud edition, architecture and allows an enterprise to have a much more private cloud experience than would otherwise be possible.

SAP Afaria Cloud Security

ARCHITECTURAL APPROACH

SAP has taken a unique approach to implementing the SaaS edition of the SAP Afaria mobile device management solution. Historically, software providers offering an on-demand solution have relied heavily on multitenancy in order to scale. Multitenancy has been around for quite some time, and all cloud providers leverage it in some way.[1] This is true of SAP Afaria as well, but SAP's relationship with Amazon allows us to share resources less and dedicate more resources to each individual enterprise.

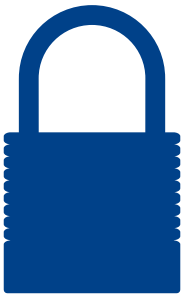
Multitenancy as a concept was born out of the idea of hardware optimization. Often, software applications underutilize hardware, but once it's allocated, it's allocated. Allowing multiple tenants within a single application allows for more efficient use of hardware. But in a shared environment, competition for resources can cause real performance issues and make it difficult to meet demanding corporate service-level agreements.

SAP Afaria, cloud edition, does use this concept. In a trial environment, a shared reporting server, database server (with separate database schemas per customer), and certificate authority (CA) server are used. That same could hold true in a production environment, but more likely an enterprise's on-premise active directory and certificate authority systems would be leveraged.

What isn't shared, what isn't multitenant, is the SAP Afaria server itself. Every customer receives a dedicated server for SAP Afaria. This is true both in the trial environment as well as in production. The server itself performs the vast majority of the work, and SAP didn't consider it appropriate to share this resource among customers.

The adoption of this "horizontal scaling" architectural pattern is possible due to the singular infrastructure expertise provided by Amazon. In short, the Amazon infrastructure is highly elastic.[2] Rather than dedicate a large amount of resources to a single instance, Amazon elasticity allows resources to start small and then automatically grow over time as enterprise adoption grows. Using this approach allows the solution to be run at a much lower cost than if large amounts of dedicated resources had to be allocated up front.

Horizontal scaling is fundamental to the SAP Afaria, cloud edition, architecture and allows an enterprise to have a much more private cloud experience than would otherwise be possible. Combining the horizontal scale approach with dedicated database schemas eliminates the risk of cross-enterprise data leakage and is just one of the many security features of this solution.



SAP Afaria provides a spectrum of security policies that can be applied to mobile devices.

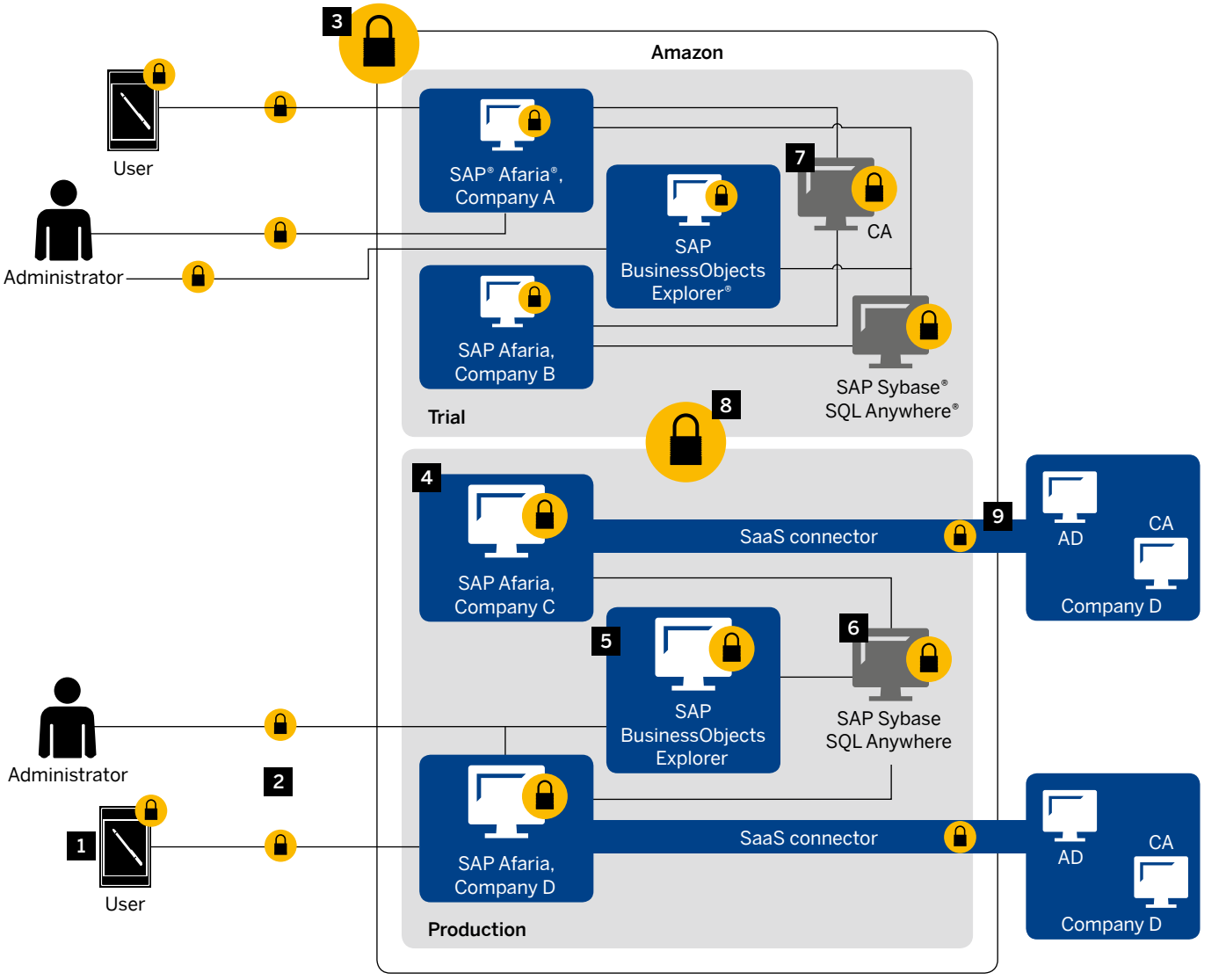
FOOTNOTES

1. http://blogs.forrester.com/john_r_rymer/12-03-20-understanding_clouds_multitenancy
2. http://aws.amazon.com/ec2

ARCHITECTURE DIAGRAM

In understanding the security features of SAP Afaria, cloud edition, it's helpful to understand the components of the solution and how they communicate with one another. Figure 1 shows a logical architecture of the solution. Each number in the diagram will be discussed separately in the details that follow.

Figure 1: SAP Afaria Solution Architecture – Security, by the Numbers



Amazon Web Services delivers a highly scalable cloud computing platform with **high availability and reliability,** and the flexibility to enable customers to build a wide range of applications.

Device Management: Components
The management of device security is fundamental to SAP Afaria, so it's a logical place to start. However, by default SAP doesn't enforce any level of security on mobile devices that enroll in the solution. Why? It's simple. Enterprises are different. Some companies support bring-your-own-device (BYOD) policies; others don't. Some companies are satisfied with a four-digit PIN, others require something more complex, and some forgo a device password altogether and simply force a password on an e-mail container. Many enforce device encryption where possible, but not all. Some enterprises will enforce application blacklisting and whitelisting; others will not.

For that reason, it's not appropriate for SAP to enforce a predefined level of security on a mobile device. That is the enterprise administrator's task to perform. What SAP does provide is a robust set of capabilities that are made available to the enterprise administrator to extend corporate security policies onto mobile devices.

The only exception to this policy is the underlying storage used by the SAP Afaria client itself. In all cases where a client exists on the mobile device, the data is encrypted using OpenSSL crypt libraries.

The rest is up to the enterprise administrator. SAP Afaria provides a spectrum of security policies that can be applied to mobile devices. Examples of some of those security policies are:

- **Password and encryption controls** – Password enforcement is completely under administrative controls, along with the ability to enforce encryption on devices that support the feature.
- **Peripheral controls** – SAP Afaria has the ability to lock down device peripherals, including camera, Bluetooth, SD Card, USB, and Wi-Fi access for devices that provide support.
- **Application blacklisting and whitelisting** – SAP Afaria covers blacklisting and whitelisting from two different angles. For devices that provide API support, SAP Afaria can enforce true blacklisting and whitelisting of applications, allowing administrators to specify which applications are permitted to run and be installed on a mobile device. For devices where API access is not available, SAP Afaria can react to the existence of blacklisted applications and immediately quarantine devices through the remediation mechanism.
- **E-mail, VPN, and Wi-Fi configuration** – SAP Afaria has the ability to automate the configuration of many connectivity elements, including virtual private network (VPN) and Wi-Fi. SAP Afaria can also bind certificates to VPN, Wi-Fi, and e-mail policies, enabling existing security infrastructure to be maintained and extended to mobile devices.
- **Remediation** – SAP Afaria enables the monitoring of remote devices for compliance. Devices that are compliant continue to function normally, and the user is able to access all enterprise functions made available to them. Devices that are deemed noncompliant can automatically be quarantined away from the corporate environment and have e-mail and other enterprise features disabled. Users are notified visually when the device becomes noncompliant and can be notified again once the device has complied with the corporate profile.
- **E-mail access control** – SAP Afaria supports the ability to limit access to either on-premise Microsoft Exchange or Exchange 365 e-mail systems only to compliant devices. Once an administrator has defined the policies that should be applied to a device, SAP Afaria can automatically block devices that do not currently have the policies installed on their devices. E-mail access control also enables immediately blocking access to e-mail for compromised devices. Once the device is brought into compliance, e-mail will be permitted.
- **NitroDesk TouchDown integration** – The NitroDesk TouchDown client provides a containerized ActiveSync e-mail experience for both iOS and Android without requiring a full third-party e-mail infrastructure. SAP Afaria can automate the configuration of both the iOS and Android container and remove the container automatically in the event of a security action.
- **Samsung SAFE support** – SAP Afaria fully supports the advanced security features offered by Samsung SAFE controls.
- **Enhanced LG Electronics support** – SAP Afaria fully supports the advanced security features offered by next-generation LG devices.

Data in Transit

No unencrypted traffic is permitted to pass into the SAP Afaria, cloud edition, environment. This is applicable to both device users as well as enterprise administrators.

Enterprise administrators – Access to the SAP Afaria administrative console is done through an authenticated HTTPS connection. In a trial environment, that user name and password are defined by the enterprise administrator during system initiation. In a production environment, the authentication process can be handled similarly, or more likely, the administrative credentials to be used would be the user's Active Directory credentials.

Access to SAP Afaria reporting is also done through an authenticated HTTPS connection. This is true whether the reports are accessed through a Web browser or through SAP BusinessObjects Explorer® or SAP BusinessObjects™ Mobile software.

Device users – Device users access various parts of the SAP Afaria solution. First, in order to enroll, they will likely access the "/Me" enrollment site. This will be done through an HTTPS connection that is authenticated prior to allowing access. During the enrollment process, a one-time use code will be generated that must be supplied to the SAP Afaria client in order to complete the process. This code is populated into the client automatically; the user does not have to type it in. The user is then authenticated again to ensure that the code is being used by a valid user. Only then is the user permitted to enroll in mobile device management through a secure protocol. This protocol is also used for policy and software delivery, for a secure connection from start to finish.

Hosting Security

General certifications – Amazon Web Services (AWS) delivers a highly scalable cloud computing platform with high availability and reliability and the flexibility to enable customers to build a wide range of applications. In order to provide end-to-end security and end-to-end privacy, AWS builds services in accordance with security best practices, provides appropriate security features in those services, and documents how to use those features. In addition, AWS customers must use those features and best practices to architect an appropriately secure application environment. Enabling customers to ensure the confidentiality, integrity, and availability of their data is of the utmost importance to AWS, as is maintaining trust and confidence.

AWS provides a wide range of information regarding its IT control environment to customers through white papers, reports, certifications, and other third-party attestations. This information assists customers in understanding the controls in place relevant to the AWS services they use and how those controls have been validated by independent auditors. This information also assists customers in their efforts to account for and to validate that controls are operating effectively in their extended IT environment. Below, please find a brief summary of the various certifications and third-party attestations with which AWS is compliant. [3] These include:

- ✓ **SAS70 Type II** – This report includes detailed controls that AWS operates, along with an independent auditor opinion about the effective operation of those controls.
- ✓ **PCI DSS Level 1** – AWS has been independently validated to comply with the PCI Data Security Standard (DSS) as a shared host service provider.
- ✓ **ISO 27001** – AWS has achieved ISO 27001 certification of the Information Security Management System (ISMS) covering infrastructure, data centers, and services.
- ✓ **FISMA** – AWS enables government agency customers to achieve and sustain compliance with the Federal Information Security Management Act (FISMA). AWS has been awarded an approval to operate at the FISMA-Low level. It has also completed the control implementation and successfully passed the independent security testing and evaluation required to operate at the FISMA-Moderate level. AWS is currently pursuing an approval to operate at the FISMA-Moderate level from government agencies.

AWS Identity and Access Management (IAM) – This enables you to create multiple users and manage the permissions for each user within your AWS account. A "user" is an identity (within a customer AWS account) with unique security credentials that can be used to access AWS resources. IAM eliminates the need to share passwords or access keys and makes it easy to enable or disable a user's access as appropriate.

IAM enables you to implement security best practices, such as least privilege, by assigning unique credentials to every user within your AWS account and granting only the permissions users need to access the AWS resources required for them to perform their jobs. IAM is secure by default; new users have no access to AWS until permissions are explicitly granted.

FOOTNOTE

3. http://aws.amazon.com/security

IAM allows you to minimize the use of your AWS account credentials. Instead, all interactions with AWS resources should occur in the context of IAM user security credentials. To learn more about AWS IAM, visit our IAM page.

AWS Multi-Factor Authentication (AWS MFA) – AWS MFA is an additional layer of security that offers enhanced control over your AWS account settings and the management of the AWS resources to which the account has subscribed. When you enable this opt-in feature, you'll need to provide a six-digit single-use code in addition to your standard user name and password credentials before access is granted.

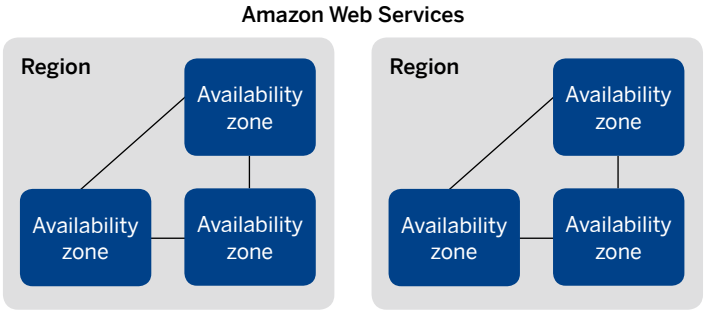
It is easy to obtain an authentication device from a participating third-party provider or download and install appropriate software on your mobile phone and then set it up for use through the AWS Web site. More information about Multi-Factor Authentication is available here.

Key rotation – For the same reasons that it is important to change your password frequently, AWS recommends that you rotate your access keys and certificates on a regular basis. To let you do this without potential impact to your applications' availability, AWS supports multiple concurrent access keys and certificates. With this feature, you can rotate keys and certificates into and out of operation on a regular basis without any downtime to your application. This can help to mitigate risk from lost or compromised access keys or certificates. The IAM APIs enable you to rotate the access keys of your AWS account as well as for users created under your AWS account.

To learn more about this feature or to begin using key rotation, click here.

Availability zones and regions – AWS infrastructure services are hosted in a number of regions, including locations in the United States, Europe, and Asia Pacific. This article lists the Web service API end points needed to make API requests and manage infrastructure in each region. AWS infrastructure services are hosted in multiple locations worldwide. These regions are logically isolated from each other, so, for example, you won't be able to access U.S. East resources when communicating with the EU West end point (see Figure 2). You might choose a region to optimize latency, minimize costs, or address regulatory requirements. For more information on how services operate in each region, see the service *Developer Guide* at http://aws.amazon.com/documentation.

Figure 2: Logical Isolation of Amazon Zones and Regions



To reduce data latency in your applications, most Amazon Web Services products allow you to select a regional end point to make your requests. An end point is a URL that is the entry point for a Web service.

For information about which regions are supported, see the specific region information for your product. For information about the AWS products and end points available in the AWS GovCloud (U.S.) region, see AWS GovCloud (US) Region.[4]

Regions are dispersed and located in separate geographic areas (see Figure 3). Availability zones are distinct locations within a region that are engineered to be isolated from failures in other availability zones and provide inexpensive, low-latency network connectivity to other availability zones in the same region.

Each Amazon EC2 region is designed to be completely isolated from the other Amazon EC2 regions. This achieves the greatest possible failure independence and stability, and it makes the locality of each EC2 resource unambiguous.

Security groups – When launching an Amazon EC2 instance, you need to specify its security group. The security group acts as a firewall allowing you to choose which protocols and ports are open to computers over the Internet. You can choose to use the default security group and then customize it, or you can create your own security group. The protocols to configure are TCP, UDP, and ICMP. There is also a range of ports for each protocol.[5]

Lastly, the source allows you to open the protocols and ports to either a range of IP addresses or to members of some security group. The default security group described above may be a little confusing. It appears that everything is wide open when, in fact, everything is closed. Most likely, you'll need to open some protocols and ports to the outside world. There are a number of common services preconfigured in the *Connection Method* drop-down as shown in the table in Figure 4.

As an example, if you are configuring an EC2 instance to be a Web server, you'll need to allow the HTTP and HTTPS protocols. When you select them from the list, the security group would be altered as shown in Figure 5.

Figure 3: AWS Regions

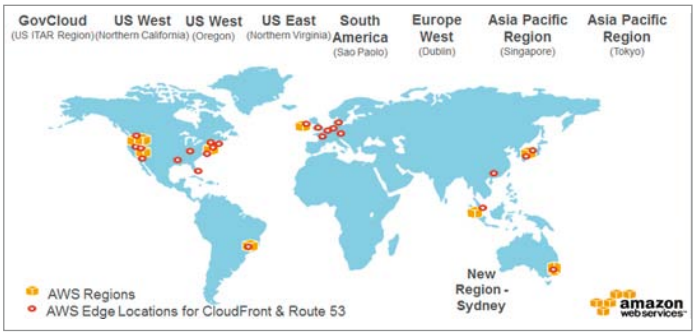


Figure 4: Connection Method

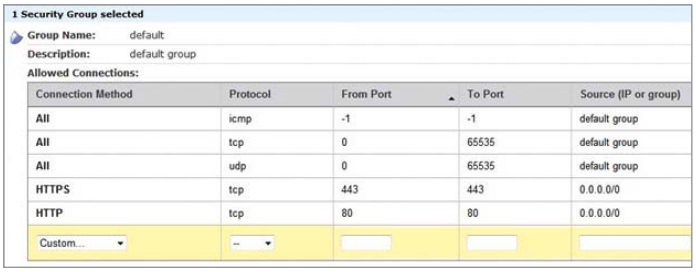
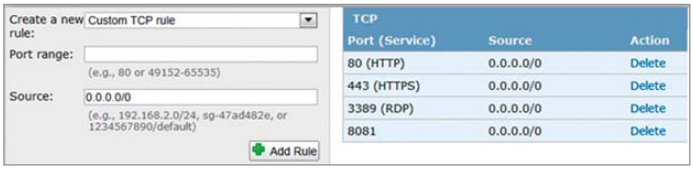


Figure 5: Altering the Security Group



FOOTNOTES

4. http://docs.aws.amazon.com/general/latest/gr/rande.html#govcloud_region
5. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

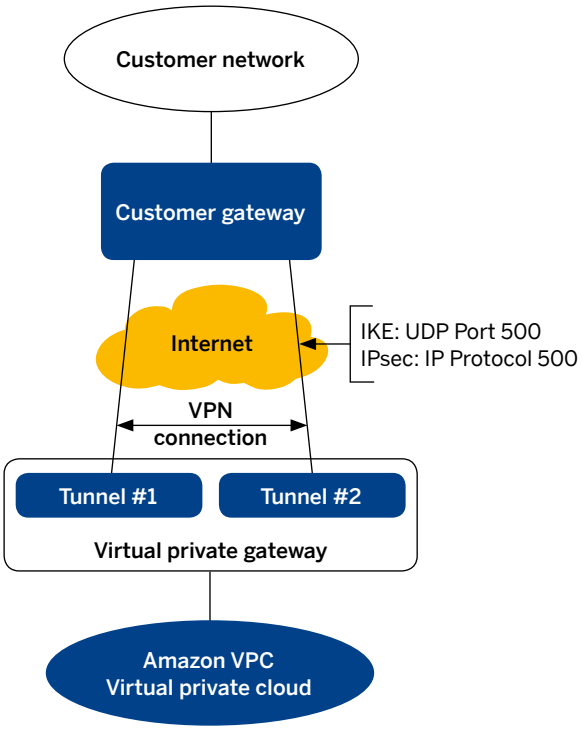
Each Amazon EC2 region is designed to be completely isolated from the other Amazon EC2 regions. This achieves the greatest possible **failure independence and stability,** and it makes the locality of each EC2 resource unambiguous.

The most important thing to note is the source IP. When you specify "0.0.0.0/0," that really means you're allowing every IP address access to the specified protocol and port range. So in the example, TCP ports 80 and 443 are open to every computer on the Internet.

VPCs – To ensure the highest level of security, SAP Afaria, cloud edition, leverages Amazon's virtual private cloud (VPC) VPN technology architecture. We chose this design to provide increased availability for the Amazon VPC service. If there's a device failure within AWS, your VPN connection will automatically fail over to the second tunnel so your access isn't interrupted.

Figure 6 shows your network, the customer gateway, the VPN connection that goes to the virtual private gateway, and the VPC. There are two lines between the customer gateway and virtual private gateway because the VPN connection consists of two tunnels to deliver high availability.

Figure 6: Amazon's VPC VPN Technology Architecture

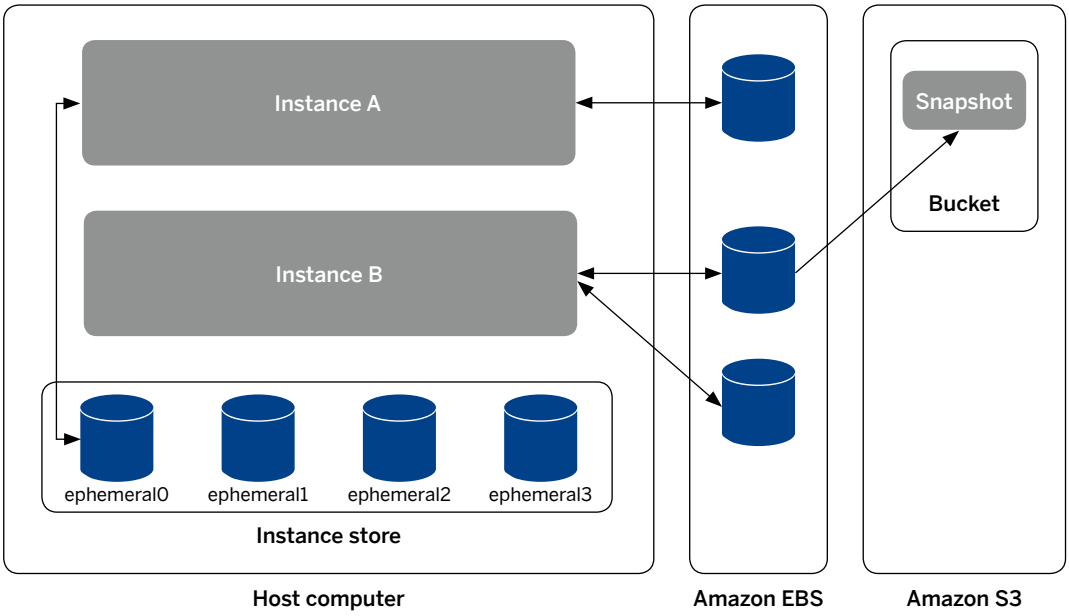


EC2 storage – Amazon EC2 provides you with flexible, cost-effective, and easy-to-use data storage options for your instances. Each option has a unique combination of performance and durability. These storage options can be used independently or in combination to suit your requirements. These storage options include the following:

- Amazon Elastic Block Store (Amazon EBS)
- Amazon EC2 instance store
- Amazon Simple Storage Service (Amazon S3)

Figure 7 shows the relationship between these types of storage.

Figure 7: Storage Types



Amazon EBS – Amazon EBS is a durable, block-level storage volume that you can attach to a single running Amazon EC2 instance. You can use Amazon EBS as a primary storage device for data that requires frequent and granular updates. For example, Amazon EBS is the recommended storage option when you run a database on an instance.

Amazon EBS volumes behave like raw, unformatted, external block devices that you can attach to your instances. They persist independently from the running life of an Amazon EC2 instance. After an Amazon EBS volume is attached to an instance, you can use it as you would any other physical hard drive. For more information, see Amazon Elastic Block Store (Amazon EBS).

Amazon EC2 Instance Store – Each Amazon EC2 instance, unless it's a microinstance, can access storage from disks that are physically attached to the host computer. This disk storage is referred to as "instance store." Instance store provides temporary block-level storage for Amazon EC2 instances. The data on an instance store volume persists only during the life of the associated Amazon EC2 instance. For more information, see Amazon EC2 Instance Store.

Amazon S3 – Amazon S3 is a repository for Internet data. Amazon S3 provides access to reliable and inexpensive data storage infrastructure. It is designed to make Web-scale computing easier by enabling you to store and retrieve any amount of data, at any time, from within Amazon EC2 or anywhere on the Web. For example, you can use Amazon S3 to store backup copies of your data and applications. For more information, see Amazon Simple Storage Service (Amazon S3).

Adding storage – Every time you launch an instance from an advanced metering infrastructure (AMI), a root storage device is created for that instance. The root storage device contains all the information necessary to boot the instance. For more information, see Amazon EC2 Root Device Volume. You can specify storage volumes in addition to the root device volume when you create an AMI or launch an instance using block device mapping. For more information, see Block Device Mapping.

Snapshots – Amazon EBS provides the ability to back up point-in-time snapshots of your data to Amazon S3 for durable recovery.[6] Amazon EBS snapshots are incremental backups, meaning that only the blocks on the device that have changed since your last snapshot will be saved. If you have a device with 100 GBs of data, functionality can be used as a way to increase the size of an existing volume or to create duplicate volumes in new availability zones. If you choose to use snapshots to resize your volume, you need to be sure your file system or application supports resizing a device.

New volumes created from existing Amazon S3 snapshots load lazily in the background. This means that once a volume is created from a snapshot, there is no need to wait for all of the data to transfer from Amazon S3 to your Amazon EBS volume before your attached instance can start accessing the volume and all of its data. If your instance accesses a piece of data that hasn't yet been loaded, the volume will immediately download the requested data from Amazon S3 and then will continue loading the rest of the volume's data in the background.

Amazon EBS allows you to share these snapshots, making it easy for you to share this data with your co-workers or others in the AWS community. With this feature, users whom you have authorized can quickly use your Amazon EBS shared snapshots as the basis for creating their own Amazon EBS volumes. If you choose, you can also make your data available publicly to all AWS users. Users to whom you have granted access can create their own EBS volumes based on your snapshot; your original snapshot will remain intact. This is a great way for developers to easily share data with the rest of the Amazon EC2 community, and it makes it easy for new customers to create Amazon EBS volumes from an existing snapshot. For more information on how to share snapshots, refer to the Amazon EC2 User Guide's EBS section.

Amazon EBS also provides the ability to copy snapshots across AWS regions, making it easier to leverage multiple AWS regions for geographical expansion, data center migration, and disaster recovery. Customers can copy any accessible snapshots that are in the "available" status. This includes snapshots that they created, snapshots that were shared with them, and also snapshots from the AWS Marketplace, VM Import/Export, and Storage Gateway. For more information on how to use EBS snapshot copy, refer to Amazon EBS Documentation.

FOOTNOTE

6. http://aws.amazon.com/ebs

Amazon EC2 provides you with flexible, cost-effective, and easy-to-use data storage options for your instances. Each option has a unique combination of **performance and durability.**

Snapshots can also be used to instantiate multiple new volumes, expand the size of a volume, or move volumes across availability zones. When a new volume is created, there is the option to create it based on an existing Amazon S3 snapshot. In that scenario, the new volume begins as an exact replica of the original volume.

SAP Afaria Application Instance

As mentioned in the "Architectural Approach" section, each customer receives a dedicated server for SAP Afaria. SAP started with a hardened Windows 2008 R2 instance in order to create a gold image to be used for each customer. Unnecessary services were shut down, firewalls enabled, and other security controls were added for adequate protection. Physical access to this server is restricted to SAP personnel. Network access is permitted only through a standard Web browser over secure authenticated protocols. Storage, while network based, is dedicated to each customer.

Detailed monitoring features were added to the server to ensure that it is adequately sized in order to handle load. Amazon elasticity is leveraged to vertically increase the size of the instance as load grows over time, ensuring availability of the system.

The entire system is "snapshotted" (backed up) before and after any upgrade. Instance storage is snapshotted once a day, as very little information is actually saved in file storage. Combined with the database backups (described in the SAP Sybase SQL Anywhere® solutions server), a system can be recovered rapidly, minimizing any outage.

SAP BusinessObjects Explorer

As mentioned in the "Architectural Approach" section, the server for SAP BusinessObjects Explorer represents one of the shared elements both for production as well as for trial environments. The server itself is monitored by SAP to determine if additional resources are required.

SAP started with a hardened Windows 2008 R2 instance in order to create a gold image to be used for this server. Unnecessary services were shut down, firewalls enabled, and other security controls were added for adequate protection. Physical access to this server is restricted to SAP personnel.

Network access to the server for SAP BusinessObjects solutions is provided through two mechanisms: first, through a standard HTTPS Web interface, and second, through an on-device native client called SAP BusinessObjects Explorer and SAP BusinessObjects Mobile. In all cases, the traffic is encrypted over HTTPS, and a user name and password generated by the end user is used as authentication credentials. The user name selected is required to be unique across all instances of SAP Afaria and SAP BusinessObjects solutions and is restricted to enable access to information only for that customer data.

SAP Sybase SQL Anywhere Solutions

As mentioned in the "Architectural Approach" section, SAP Sybase SQL Anywhere solutions represent one of the shared elements both for production as well as for trial environments. The database server itself is monitored by SAP to determine if additional resources are required.

SAP started with a hardened Red Hat Enterprise Linux 5.8 instance in order to create a gold image to be used for each SAP Sybase SQL Anywhere server. Unnecessary services were shut down, firewalls enabled, and other security controls were added for adequate protection. Physical access to this server is restricted to SAP personnel. The customer never directly accesses this server. Network access is granted only to the SAP Afaria server service and the server for SAP BusinessObjects Web Intelligence® software used for reporting. This server is not accessible to the Internet.

While the same database server is used, each customer has its database encrypted using AES encryption, with a separate database encryption key and distinct user name and password. Each database is backed up fully once a day during low transaction times. Incremental backups of the transaction log are done once per hour and offloaded to S3 or EC2 storage. This ensures that a system using SAP Afaria can be brought back up quickly in the case of an outage.

Microsoft Certificate Authority

As stated, the Microsoft Certificate Authority server represents one of the shared elements for trial environments. Depending on whether an enterprise is integrating with an on-premise CA, it may also be leveraged in a production environment. This would likely be the case if the CA isn't used for generating certificates for binding to Exchange, VPN, or Wi-Fi policies. The server itself is monitored by SAP to determine if additional resources are required.

SAP started with a hardened Windows 2008 R2 instance in order to create a gold image to be used for the CA. Unnecessary services were shut down, firewalls enabled, and other security controls were added for adequate protection. Physical access to this server is restricted to SAP personnel. The customer never directly accesses this server. Network access is granted only to the SAP Afaria server service. This server is not accessible to the Internet.

Trial–Production Boundary

SAP strongly believes that trial customers should be kept completely separate from production customers. This does add some effort on SAP's part during the trial to migration, but we believe that this helps ensure stability for both trial and production systems. Leveraging Amazon's VPC capabilities, trial customers are in a different private subnet than production customers. During the migration, components that need to be transitioned from trial to production are physically moved by SAP as part of the production landscape setup.

SaaS Connector

The SaaS connector plays a crucial role in the SAP Afaria solution. It serves as the secure tunnel between the SAP Afaria server and an enterprise authentication system or certificate authority. As such, specific attention has been paid to the security of this aspect of the solution.

Installation – The secure tunnel requires two components. One component, the SaaS connector server, is installed on the SAP Afaria server. Only SAP can perform this installation. The other component, the SaaS connector client, is installed within the customer's environment. Until this is installed and configured appropriately, the SAP Afaria server has no access to any back-end systems other than those that are installed in the SAP Afaria solution.

Communication initialization – While traffic flow within the SaaS connector is bidirectional, it is always initiated by the SaaS connector client. This gives complete control to the enterprise if there is a desire to terminate the connection. An additional benefit of this approach is that it typically does not require any firewall modifications.

Mutual authentication – During the initial setup of the SaaS connector, both the SaaS connector server and client are assigned unique certificates with a key length of at least 2,048 bits. These certificates have to be manually inserted into the installation directories of both the client and the server. During session initialization (and periodically during an established connection), the client and server mutually authenticate their certificates, and the validity of the certificates is checked against the revocation list of the CA that issued them. If the certificates are expired, have been revoked, or are invalid in any other way, the connection is refused. This guarantees mutual authentication and eliminates risk of man-in-the-middle attacks.

Transport encryption – Once the client and server end points have been authenticated, the connection switches to a secure Transport Layer Security (TLS) encryption stream, ensuring confidentiality of data transfer.

End-point control – The SaaS connector is not intended to act as a VPN, but rather as an application layer tunnel for SAP Afaria. As such, it will generally only be permitted to communicate with predefined end points within the enterprise environment. Those end points are configured by SAP with a heavy customer environment during the installation process and remain under control of the customer after installation is complete. Only those end points defined within the system configuration will be available for routing.

SUMMARY

SAP has made security its top priority when designing SAP Afaria, cloud edition. In doing so, we believe we have realized a solution that allows for security without unnecessarily impinging on ease of use.

CMP26599 (13/06)

SAP

The Best-Run Businesses Run SAP™