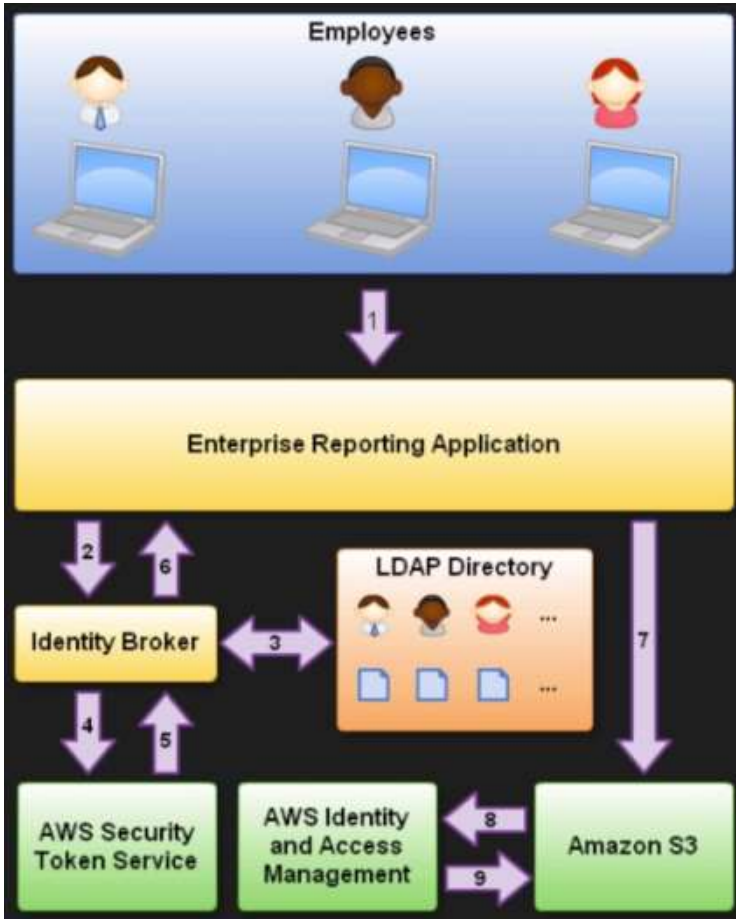
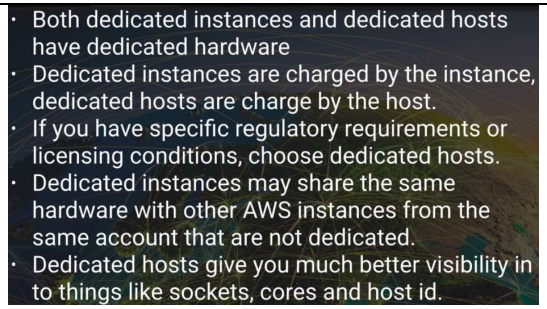
AWS Best Practices for DDoS	https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf Remember the technologies you can use to mitigate a DDoS attack: ▪ CloudFront ▪ Route53 ▪ ELB's ▪ WAFs ▪ Autoscaling (Use for both WAFs and Web Servers) ▪ CloudWatch
AWS IAM	▪ You can create custom policies using the visual editor or using JSON. ▪ You can now attach roles to EC2 instances at any time using the command line or AWS Console. ▪ Once attached the role takes effect immediately. ▪ Any policy change also takes effect immediately.
MFA Reporting & IAM	You can enable MFA using the command line and by using the console. MFA can be enabled on both the root account and user accounts. You can report on who's using MFA on a per user basis using credential reports.
Security Token Service (STS)	**Grants users limited and temporary access to AWS resources.** Users can come from three sources: ▪ Federation (Typically Active Directory) Grants temporary access based off the users AD credentials. Does not need to be a user in IAM. SSO allows users to log in to AWS console without assigning IAM credentials. ▪ Federation with Mobile Apps Use FB/Amazon/Google or other OpenID providers to log in. ▪ Cross Account Access Let's users from one AWS account access resources in another. **Federation:** *Combining or joining a list of users in one domain (such as IAM) with a list of users in another domain (such as AD, FB etc.).* **Identity Broker:** A service that allow you to take an identity from point A and joint it (federate it) to point B. **Identity Store:** Service like AD, FB, Google etc. **Identities:** A user of a service like FB etc.



1. Employee enter their username and password.
2. The application calls an Identity Broker. The broker captures the username and password.
3. The Identity Broker uses the organization's LDAP directory to validate the employee's identity.
4. The Identity Broker calls the new GetFederationToken function using IAM credentials. The call must include an IAM policy and a duration (1 to 36 hours), along with a policy that specifies the permissions to be granted to the temporary security credentials.
5. The Security Token Service confirms that the policy of the IAM user making the call to GetFederationToken gives permission to create new tokens and then returns four values to the applications:
   a) Access key
   b) Secret access key
   c) Token
   d) Duration (the token's lifetime)
6. The Identity Broker returns the temporary security credentials to the reporting application.
7. The data storage application uses the temporary security credentials (including the token) to make requests to AWS S3.
8. AWS S3 uses IAM to verify that the credentials allow the requested operation on the given S3 bucket and key.
9. IAM provides S3 with the go-head to perform the requested operation.

Logging	**Services:** ▪ AWS CloudTrail

	▪ AWS Config ▪ AWS CloudWatch Logs ▪ VPC Flow Logs
CloudWatch vs CloudTrail vs Config	**CloudWatch** monitors performance. **CloudTrail** monitors API calls in the AWS platform. **AWS Config** records the state of your AWS environment and can notify you of changes.
AWS Hypervisors	**Exam Tips:** Choose HVM over PV where possible PV is isolated by layers, Guest OS sits on Layer 1, Applications Layer 3. Only AWS Administrator have access to hypervisors. AWS staffs do not have access to EC2, that is your responsibility as a customer. All storage memory and RAM memory is scrubbed before it's delivered to you.
EC2 Dedicated Instances Vs Dedicated Hosts	
AWS Systems Manager Run Command	▪ Commands can be applied to a group of systems based on AWS instances tags or by selecting manually. ▪ SSM agent needs to be installed on all your managed instances ▪ Commands can be issued using AWS Console, AWS CLI, AWS Tools for Windows PowerShell, System Manager API or Amazon SDKs ▪ You can use this service with your on-premise systems as well as EC2 instances.
AWS Systems Manager Parameter Store	▪ Confidential information such as passwords, database connection strings, and license codes can be stored in SSM Parameter Store. ▪ You can store values as plain text or you can encrypt the data. ▪ You can then reference these values by using their names. ▪ You can use this service with EC2, CloudFormation, Lambda, EC2 Run Command etc.
AWS Config Rules With S3	▪ No Public Read Access ▪ No Public Write Access
Shared Responsibility	**AWS manages security of the cloud.**

	AWS Responsibilities are.. 1. Global infrastructure 2. Hardware, Software, Networking, and Facilities. 3. Manged Services. **Security in the cloud is the responsibiltiy of the customer**. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks. Customer Security Responsibilities are … 1. Infrastructure as a Service (IaaS). 2. Including updates and security patches. 3. Configuration of the AWS provided firewall **Exam Tips:** ▪ You are responsible for things like EC2 OS Patching, Antivirus, Security Groups etc. ▪ You are not responsible for things like RDS OS Updates, RDS Database Updates, PHP updates with Elasticbeanstalk etc.