Welcome back and in the last lesson, I step through the architecture of Identity Federation. So all of the technical components, as well as the differences between SAML 2.0 Identity Federation and Web Identity Federation. In this lesson, I want to focus on when you would use Identity Federation because the Solutions Architect Associate exam tends to feature questions which test your understanding of when it's appropriate to use Identity Federation and perhaps just as important are the restrictions on various AWS services which would require you to use Identity Federation. So that's two things I want to get across in this lesson.



So some of the situations why you might use Identity Federation, maybe you're within an enterprise and you're wanting to allow access to AWS resources so if you are in an enterprise, you'll probably have your own internal identity provider, so users and staff will have access to an existing pool of identities. You might need those identities to be used across all enterprise systems, including AWS. So you want to access AWS resources using single sign on, and you might have tens or hundreds of thousands of users the important part to remember for the exam is that IAM which handles the internal AWS identities does have a limit on the number of users that it can cope with. Now there are various different, important IAM limits, and I covered those earlier in the course but keep them in mind that if you do have any situations where you're dealing with tens of thousands or hundreds of thousands or even millions of identities, then you won't be able to use IAM and that's a perfect situation for considering either SAML 2.0 Federation or Web Identity Federation. Another component of this is you might have an existing identity team inside your business, and they might control identities from a security and a data sovereignty perspective and so you want to give them the responsibility to manage identities. So by creating an ID Federation, you grant them the ability to control the creation, modification, and deletion of identities, roles, groups, and you just configure the integration with AWS. Now, you might also be a mobile or web application developer, and you need to grant access from your application users to AWS resources that are used by your application. This might be a mobile game. It might be a fitness application or any other application which needs to store data in AWS services maybe S3 or DynamoDB. You might want to grant a certain level of guest access that a user can access using an unauthenticated or an anonymous identity, but then you want to grant further access based on them being logged into your application. When using Incognito, you're able to create that Federation relationship. Allow them to log in with Twitter, Facebook, Google, Amazon, and many other external identity providers. You're able to create a guest role so that they can use your application without being logged in and still access AWS services but then another role where they can authenticate with the ID provider, get a token in response to logging in, and exchange that for AWS credentials. Now, from a development perspective, the benefit of this is you do not have to store any credentials in your application. You're essentially using their external ID and the swap of that ID internally inside AWS to get credentials that they can use. So you don't have to worry about credential leakage because they're not using identities that you manage, it's much safer. You don't have to worry about coding a login infrastructure that's already done by the identity provider, so there's lots of benefits to doing Web Identity Federation. Now again, many popular mobile or web applications do have millions of users, and so you couldn't go ahead and create individual IAM accounts for each of those users. So by using ID Federation and exploiting the fact that they already have an external identity, maybe even more than one external identity. You can bypass that limit of IAM and swap that identity for temporary credentials, and they can be used to access AWS. Now another common scenario that I see is you might be a large organization with tens, hundreds, or even more AWS accounts in an organization. You might have one central account that manages identities, and you might want to allow that one account to access other accounts using role switching. Now you can just use internal IAM accounts or internal IAM identities and allow those to role shift to every one of your member accounts, but you could also federate the account is used for that jumping point, use their existing enterprise credentials, to access that account and then role switch into your other accounts. So you get the benefit of AWS Organizations but also you can use your existing corporate identities. So the key thing to understand when it comes to any ID Federation questions in the exam is look for any keywords. Look for large user accounts. Look for situations where there are existing identity providers and you want to use them. Look for answers that mention STS or Cognito. Look for answers that talk about using roles. Any of those keywords will point you in the direction of the correct answer. Now this is the solutions architect associate exam, I don't expect it to feature heavily on this exam or feature in very much detail. You might get a question on it and the things that we've covered in the last two lessons will allow you to answer any of those questions. So I what would suggest is just become really comfortable with exactly the type of situations that you will use Identity Federation in and then make sure that you understand the flow across these two different federation architecture's So SAML 2.0 and Web Identity and once you've done that, you should be good to answer any questions in this area on the exam. Now that is everything that I wanted to cover about Identity Federation in this lesson. Coming up next is a hands on lab where you'll get practical exposure to how to use Identity Federation. Now, if you don't see this hands on lab at this point, it could be because the course is still in preview. It is coming very soon. We just need to finish up doing any of our quality assurance checks, and then it will be available for you to take. So at this point, go ahead, mark this lesson as complete. You can go ahead and take the hands on lab if it is available, and regardless next, we're moving on to the next section of the course, which is section eight. The last section of the course where we'll be looking application integration, analytics, and various operational services. So go ahead and mark this lesson as complete and I'll see you in the next.