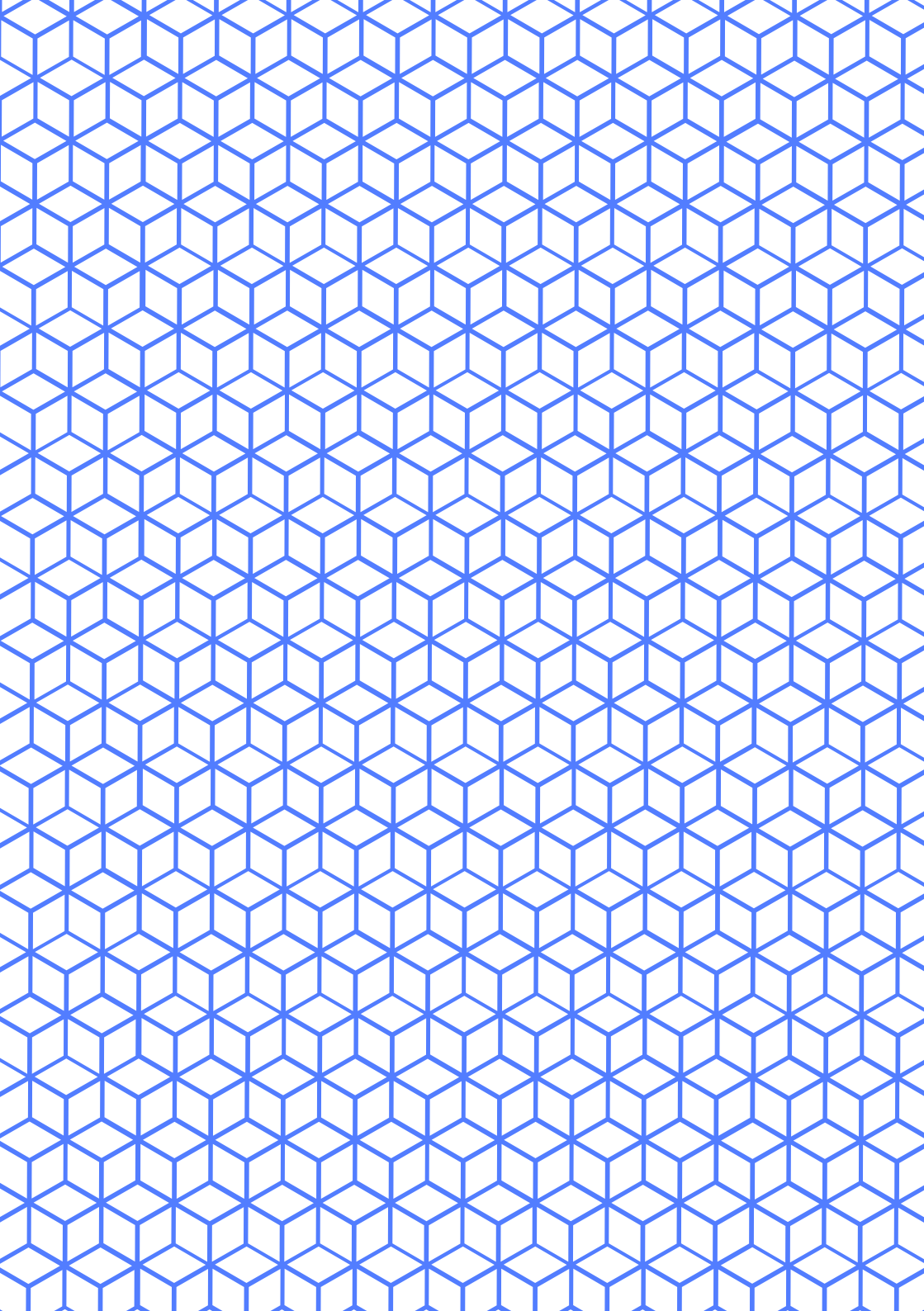
amazon web services

AWS SÄKERHET OCH EFTERLEVNAD

SNABB-REFERENS-GUIDE

2017



ÖVERSIKT

ÖVERSIKT

När ni migrerar era reglerade belastningar till molnet får ni tillgång till våra många styrningsfunktioner, som ni kan använda för att uppnå högre säkerhet i stor skala. Molnbaserad styrning är billigare att börja använda, ger enklare drift och ökad smidighet genom att det ger bättre tillsyn, säkerhetskontroll och central automatisering. Migreringen till molnet innebär att ni kan utnyttja AWS för att minska antalet säkerhetskontroller ni behöver underhålla.

En på lämpligt vis skyddad miljö är resultatet av en miljö som efterlever alla regler. Vi erbjuder robusta infrastrukturskontroller som har verifierats genom ett stort antal intyg och certifieringar. Varje certifiering innebär att en kontrollant har verifierat att specifika säkerhetskontroller finns att tillgå och fungerar som avsett. Du kan läsa mer om alla de intyg och certifieringar som vi har fått på sidan som behandlar AWS garantiprogram.

Vi erbjuder dessutom en stor mängd tjänster och verktyg som ni kan använda för att efterleva alla regler i molnet, däribland Amazon Inspector, AWS Artifact, AWS Service Catalog, AWS CloudTrail, AWS Config och AWS Config Rules.

PROGRAM

PROGRAM

Våra miljöer granskas kontinuerligt, och vår infrastruktur och våra tjänster är godkända för drift enligt flera efterlevnadsstandarder och branschcertifieringar i alla områden och vertikaler. Ni kan utnyttja dessa certifieringar för att verifiera våra säkerhetskontrollers implementering och effektivitet.

Bild 1: Garantiprogram

Obs! Vi lägger ständigt till fler program. En helt aktuell lista med AWS nuvarande garantiprogram finns på webbplatsen.

Certifieringar/intyg ges av externa och oberoende kontrollanter. Våra certifieringar, granskningsrapporter och efterlevnadsintyg grundar sig i resultaten av kontrollantens arbete.

Lagarna/föreskrifterna/integriteten och ***harmoniseringen/ramverket*** är specifika för er bransch eller funktion. Vi stöder er genom att tillhandahålla funktioner (t.ex. säkerhetsfunktioner) och nödvändig information (däribland efterlevnadsregler,

mappningsdokument och vitböcker). Formell ”direkt” certifiering av dessa lagar, föreskrifter och program är antingen 1) inte möjligt för molnleverantörer att erhålla eller 2) representerar en mindre delmängd av de krav som vi enligt våra nuvarande formella certifierings-/intygsprogram redan uppfyller.

Detta är några av våra mest populära program:

PCI DSS – Payment Card Industry (PCI) Data Security Standards (DSS) är stränga säkerhetsstandarder för att förhindra bedrägerier och skydda kortinnehavares data för säljare som behandlar kreditkortsbetalningar.

ISO 27001 – ISO 27001 är en global säkerhetsstandard som används vida kring och som skisserar kraven för system för hantering av informationssäkerhet. Den tillhandahåller en systematisk metod för att hantera företags- och kundinformation som bygger på återkommande riskbedömningar.

SOC – AWS Service Organization Control-rapporter (SOC) är rapporter från oberoende, externa parter som visar hur AWS lyckas nå fram till viktiga efterlevnadskontroller och mål. Syftet med dessa rapporter är att hjälpa er och era granskare att förstå AWS-kontrollerna som har inrättats för att stödja driften och efterlevnaden. Det finns fyra typer av AWS SOC-rapporter: AWS SOC 1 Report, AWS SOC 2: Security & Availability Report, AWS SOC 2: Confidentiality Report, samt AWS SOC 3: Security & Availability Report.

FedRAMP – Ett av den amerikanska statens program för att upprätthålla standarder i fråga om säkerhetsbedömning, auktorisering och kontinuerlig övervakning. FedRAMP följer säkerhetskontrollstandarden NIST 800-53.

PROGRAM

DoD Cloud Security Model (CSM) – Standarder för cloud computing som utfärdas av amerikanska DISA (Defense Information Systems Agency) och dokumenteras i amerikanska försvarsdepartementets (DoD) Security Requirements Guide (SRG). De tillhandahåller en auktoriseringsprocess för dem som äger DoD-belastningar och har unika arkitektoniska krav beroende på inverkningsnivå.

HIPAA – Health Insurance Portability and Accountability Act (HIPAA) innehåller stränga säkerhets- och efterlevnadsstandarder för organisationer som behandlar eller lagrar skyddad hälsoinformation (Protected Health Information, PHI).

Det finns kompletta beskrivningar av varje program som vi anpassar oss efter på webbsidan om AWS garantiprogram.

AWS Artifact

AWS Artifact-portalen innehåller våra säkerhets- och efterlevnads-dokument. De kallas även granskningsartefakter. Ni kan använda artefakterna för att visa att er AWS-infrastruktur och era AWS-tjänster är säkra och följer alla föreskrifter för era granskare eller tillsynsmyndigheter.

Några exempel på granskningsartefakter är SOC-rapporter (Service Organization Control), PCI-rapporter (Payment Card Industry) och certifieringar från ackrediteringsorgan över hela världen och efterlevnadsvertikaler som verifierar AWS-säkerhetskontrollernas implementering och driftseffektivitet.

Det går att komma åt AWS Artifact-portalen direkt från AWS Management Console.

BRANSCHER

BRANSCHER

Kunder inom följande branscher använder AWS för att uppfylla sina behov av att efterleva föreskrifter:

- Jordbruk och gruvnäring
- Analys och big data
- Datorer och elektronik
- E-handel
- Utbildning
- Energi och allmänna nyttigheter
- Finansiella tjänster
- Mat och dryck
- Spel
- Myndigheter
- Hälsovård och biologi
- Försäkring
- Tillverkning
- Medier och underhållning
- Ideella organisationer
- Fastigheter och byggnation
- Detaljhandel, partihandel och distribution
- Programvara och internet
- Telekommunikation
- Transport och logistik
- Resor och hotellverksamhet

HUR VI FÖRDELAR ANSVARET

HUR VI FÖRDELAR ANSVARET

När ni flyttar er IT-infrastruktur till AWS börjar ni använda modellen med delat ansvar som visas i bild 2. Eftersom vi driver, hanterar och kontrollerar IT-komponenterna från värdoperativsystemet och virtualiseringsskiktet ned till den fysiska säkerheten i anläggningarna där tjänsterna används, lättar en del av den operativa bördan som faller på er.

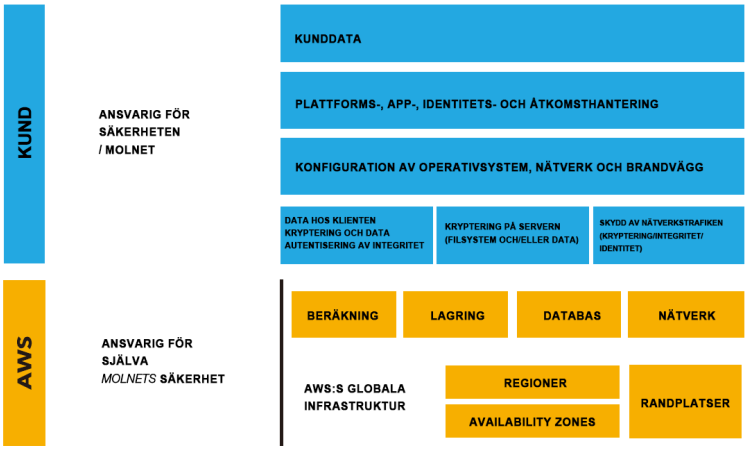


Bild 2: Modellen med delat ansvar

Modellen med delat ansvar gäller även IT-kontroller. Precis som ni delar ansvaret för driften av IT-miljön med oss, är ni även delaktiga i hanteringen, driften och verifieringen av IT-kontroller. Vi minskar er arbetsbörda med driftkontroller genom att hantera de kontroller som är kopplade till den fysiska infrastrukturen som används i AWS-miljön.
Ni kan använda dokumentationen om AWS kontroller och efterlevnad för att utföra egna utvärderingar och verifieringar av kontrollerna enligt de krav som den aktuella efterlevnadsstandarden ställer.

AWS – SJÄLVA MOLNETS EFTERLEVNAD

Vi har ansvar för att hjälpa er att upprätthålla en säker och efterlevnadsklar miljö. I allmänhet

verifierar vi att våra tjänster och anläggningar i hela världen upprätthåller en överallt förekommande kontrollmiljö som fungerar effektivt. Vår kontrollmiljö omfattar policyer, rutiner och kontrollaktiviteter som utnyttjar diverse aspekter av Amazons övergripande kontrollmiljö.

Den kollektiva kontrollmiljön omfattar de medarbetare, de rutiner och den teknik som krävs för att upprätta och upprätthålla en miljö som stöder vårt kontrollramverks driftseffektivitet. Vi har byggt in passande molnspecifika kontroller som identifieras av ledande branschorgan inom cloud computing i vårt kontrollramverk. Vi håller noga uppsikt över dessa branschgrupper för att identifiera den ledande praxisen som vi kan införa och för att bli bättre på att hjälpa er med att hantera deras kontrollmiljö.

demonstrerar vi vår efterlevnadshållning för att hjälpa er att verifiera efterlevnaden av branschens och myndigheternas krav. Vi arbetar med externa certifieringsorgan och oberoende granskare för att ge er mycket information om de policyer, rutiner och kontroller som vi har upprättat och använder.

övervakar vi att vi löpande följer globala standarder och bästa praxis genom att använda tusentals säkerhetskontrollkrav.

KUND – EFTERLEVNAD I MOLNET

Ungefär som i ett traditionellt datacenter har ni ansvar för hanteringen av gästoperativsystemet (däribland uppdateringar och säkerhetskorrigeringar) och andra tillhörande datorprogram, samt för konfigurationen av den av AWS tillhandahållna säkerhetsgruppsbrandväggen. Ni bör noga fundera över vilka tjänster ni väljer, eftersom ert ansvar varierar beroende på de tjänster ni använder, integrationen av dessa tjänster i er IT-miljö, samt tillämpliga lagar och föreskrifter.

Om ni ska kunna hantera era AWS-resurser säkert måste ni veta vilka ni använder (tillgångsinventering), konfigurera gästoperativsystemet och applikationerna på era resurser säkert (säkra konfigurationsinställningar, korrigeringar och skydd mot skadliga program), samt ha kontroll över ändringar av resurserna (förändringshantering).

Ni kan använda den information vi tillhandahåller om vårt risk- och efterlevnadsprogram och ta med den i ert styrningsramverk.

ERT INNEHÅLL

ERT INNEHÅLL

Vi ger er per design ansvaret för och kontroll över ert innehåll. Med enkla men kraftfulla verktyg kan ni ta reda på var ert innehåll lagras, skydda innehållet medan det överförs eller lagras, samt hantera era användares åtkomst till AWS tjänster och resurser.

> **Obs!** Vi försöker inte komma åt eller använda ert innehåll för något annat syfte än att ge er och era slutanvändare tillgång till de valda AWS-tjänsterna. Vi använder aldrig ert innehåll för egna syften, däribland marknadsföring eller annonsering.

Åtkomst – Med våra avancerade funktioner för åtkomst, kryptering och loggning (t.ex. AWS CloudTrail) kan ni hantera åtkomsten till ert innehåll och AWS tjänster och resurser. Vi försöker inte komma åt eller använda ert innehåll för något annat syfte än vad lagen kräver och för att upprätthålla AWS tjänster och ge er och era slutanvändare tillgång till dem.

Lagring – Ni väljer den region eller de regioner där ni vill lagra ert innehåll. Vi flyttar eller replikerar inte ert innehåll utanför de av kunden valda regionerna, förutom om lagen kräver att vi gör det och för att upprätthålla AWS tjänster och ge er och era slutanvändare tillgång till dem. Om ni t.ex. är en europeisk kund kan ni välja att distribuera era AWS-tjänster uteslutande i EU-regionen (Tyskland).

ERT INNEHÅLL

Säkerhet – Ni kan välja hur ert innehåll skyddas. Vi erbjuder stark kryptering av ert innehåll när det överförs och befinner sig i vila, och vi ger er möjlighet att hantera era egna krypteringsnycklar.

Utlämning av ert innehåll – Vi lämnar inte ut ert innehåll såvida vi inte måste göra det för att följa lagen eller en giltig och bindande order från en myndighet eller förvaltningsmyndighet. Ifall vi måste lämna ut ert innehåll, meddelar vi först er så att ni kan försöka skydda er mot den som begärt ut uppgifterna.

> **Viktigt!** Om vi är förbjudna att meddela er, eller om det finns en tydlig indikation på brottsligt beteende i samband med användningen av Amazons produkter eller tjänster, meddelar vi inte er innan vi lämnar ut ert innehåll.

Säkerhetsgarantier – För att hjälpa er att inrätta, sköta och utnyttja vår säkerhetskontrollmiljö har vi tagit fram ett säkerhetsgarantiprogram där vi använder global bästa praxis i fråga om integritet och dataskydd. Dessa säkerhetsåtgärder och kontrollprocesser verifieras på ett oberoende vis genom ett flertal externa, oberoende bedömningar.

> **Obs!** För att verifiera att vi hanterar molnets säkerhet med tekniska och fysiska kontroller för att förhindra obehörig åtkomst till eller röjande av kundens innehåll, har en oberoende granskare certifierat att vi följer branschstandarder.

VAR INNEHÅLLET LAGRAS

AWS:s datacenter är byggda i kluster i olika länder runtom i världen. Vi kallar våra datacenterkluster i ett visst land en ”region”. Ni har tillgång till ett flertal AWS-regioner runtom i världen och kan välja att använda en region, alla regioner eller en valfri kombination av regioner.

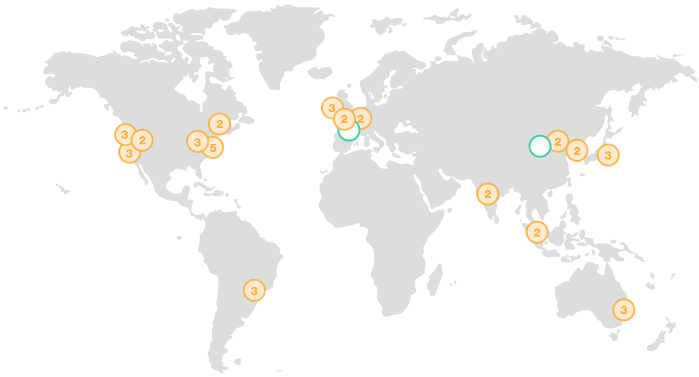


Bild 3. Regioner

Ni har fullständig kontroll och bestämmer över regionen där era data lagras fysiskt, vilket gör det lätt att uppfylla regionala efterlevnads- och datalagringskrav. Ni kan välja den AWS-region eller de AWS-regioner där ni vill lagra ert innehåll, vilket är till nytta om ni har specifika geografiska krav. Om ni t.ex. är en europeisk kund kan ni välja att distribuera era AWS-tjänster uteslutande i EU-regionen (Tyskland). Om ni väljer detta lagras ert innehåll i Tyskland, såvida ni inte väljer en annan AWS-region.

KONTINUERLIG DRIFT

Vår infrastruktur har hög tillgänglighet, och vi tillhandahåller de funktioner ni behöver för att kunna ha en motståndskraftig IT-infrastruktur. Våra system är designade för att tåla system- och maskinvaruhaverier med minimal inverkan på kunderna.

Motståndskraft handlar om att minska risken för att tillgångar inte går att nå.

Återställning handlar om att minska effekterna när tillgångar inte går att nå.

Säkerhetskopiering är en strategi för att hantera förluster av data, vare sig det handlar om en olycka eller något avsiktligt.

Katastrofåterställning är en process för att förbereda sig för och komma tillbaka efter en katastrof. Alla händelser som har negativ inverkan på den kontinuerliga driften eller ekonomin skulle kunna betecknas som en katastrof. AWS-molnet stöder många populära arkitekturer för katastrofåterställning, alltifrån ”kontrollampsmiljöer” som är klara att skalanpassas på ett ögonblick till ”standbymiljöer” som möjliggör snabb överlämning vid fel.

Läs mer om katastrofåterställning i AWS på adressen **https://aws.amazon.com/disaster-recovery/**.

Våra datacenter är byggda i kluster i olika globala regioner. Alla datacenter är online och används av kunderna; inget datacenter är ”kallt”. Om något av dem kraschar flyttar automatiska processer kunddatatrafik bort från det område som påverkas.

Vi tillhandahåller möjligheten att placera instanser och att lagra data i flera geografiska regioner liksom i flera tillgänglighetszoner inom varje region. Genom att distribuera applikationer i flera tillgänglighetszoner kan ni hantera de flesta felorsaker, däribland naturkatastrofer och systemkrascher.

KONTINUERLIG DRIFT

Ni kan bygga upp mycket motståndskraftiga system i molnet genom att använda flera instanser i flera tillgänglighetszoner och genom att använda datareplikering för att uppnå extremt högt ställda mål för återställningstid och återställningspunkter.

Ni har ansvar för att hantera och testa säkerhetskopieringen och återställningen av ert informationssystem som bygger på AWS infrastruktur. Ni kan använda AWS infrastruktur för att kunna återställa era kritiska IT-system snabbare efter en katastrof utan att betala infrastrukturskostnaden för en andra, fysisk plats. AWS-molnet stöder många populära arkitekturer för katastrofåterställning, från ”kontrollampsmiljöer” som är klara att skalanpassas på ett ögonblick till ”standbymiljöer” som möjliggör snabb överlämning vid fel.

SÄKERHET

SÄKERHET

Molnsäkerheten i AWS är vår högsta prioritet. AWS Security Center informerar om säkerhet och efterlevnad i fråga om AWS.

Vi sköter den globala molninfrastrukturen som ni använder för att etablera ett antal grundläggande datorresurser, t.ex. beräkningar och lagring. Vår globala infrastruktur omfattar de anläggningar, de nätverk, den maskinvara och de driftprogram (t.ex. värdoperativsystem, virtualiseringsprogramvara osv.) som stöder etableringen och användningen av dessa resurser. Vår globala infrastruktur är designad och hanteras enligt bästa säkerhetspraxis samt ett antal standarder för säkerhetsefterlevnad. Som kund hos AWS kan ni lita på att ni bygger webbarkitekturer på de säkraste datorinfrastrukturerna i världen.

RESURSER

RESURSER

Alla webbsidor och vitböcker som omnämns i detta dokument finns på AWS resurscentral för snabb åtkomst till säkerhets- och efterlevnadsreferensmaterial på adressen **https://aws.amazon.com/compliance/reference/**.

PARTNER OCH MARKNADEN

AWS Partner Network (APN) är AWS globala partnerprogram. Det hjälper APN-partner att bygga upp framgångsrika, AWS-baserade företag eller lösningar genom att ge affärsstöd, tekniskt stöd, marknadsstöd och stöd för marknadsintroduktion. Mer information finns på **https://aws.amazon.com/partners/**.

AWS Marketplace är en säljkanal som gör det enkelt för AWS-säljare att erbjuda programvarulösningar som körs i AWS-molnet. Mer information finns på **https://aws.amazon.com/marketplace/**.

UTBILDNING

Oavsett om ni är helt gröna, bättrar på befintliga IT-kunskaper eller bara vässar era kunskaper om molnet, kan AWS-utbildning hjälpa er och teamet att bli mer kunniga så att ni kan bli mer effektiva i molnet. Mer information finns på **https://aws.amazon.com/training/**.


amazon
web services