ความปลอดภัยตามขนาดที่เหมาะสม: การกำกับดูแลใน AWS

การวิเคราะห์คุณสมบัติต่างๆ ของ AWS ที่จะช่วยลดความท้าทายภายในองค์กร

ตุลาคม 2015

(โปรดดูเวอร์ชันล่าสุดของเอกสารฉบับนี้ที่ https://aws.amazon.com/compliance/aws-whitepapers/)

สารบัญ

บทคัดย่อ

คุณสามารถทำงานเกือบทุกอย่างบน AWS ที่คุณเรียกใช้บนระบบในองค์กรได้ รวมทั้งเว็บไซต์ แอปพลิเคชัน ฐานข้อมูล แอปบนอุปกรณ์เคลื่อนที่ การส่งเสริมการขายผ่านอีเมล การวิเคราะห์ข้อมูลแบบกระจาย การจัดเก็บสื่อ และเครือข่ายส่วนตัว บริการต่างๆ ของ AWS ออกแบบมาเพื่อทำงานร่วมกันเพื่อที่คุณสามารถสร้างโซลูชันที่สมบูรณ์แบบได้ ประโยชน์ที่มักจะถูกมองข้ามในการย้ายเวิร์กโหลดไปยัง AWS คือการได้รับความปลอดภัยในระดับสูงขึ้นตามขนาดที่เหมาะสมด้วยการใช้คุณสมบัติที่ช่วยสนับสนุนการกำกับดูแลที่มีอยู่มากมาย การกำกับดูแลในระบบคลาวด์มีต้นทุนในการเริ่มต้นต่ำกว่า สามารถทำงานได้ง่ายกว่า และมีความคล่องตัวมากขึ้นด้วยการใช้ระบบอัตโนมัติที่มีการเฝ้าติดตาม การควบคุมความปลอดภัย และทำงานจากส่วนกลางมากขึ้น ซึ่งเป็นเหตุผลเดียวกับที่การให้บริการโครงสร้างพื้นฐานในระบบคลาวด์มีข้อดีมากกว่าการให้บริการแบบภายในองค์กร เอกสารฉบับนี้อธิบายว่าคุณสามารถใช้ AWS เพื่อกำกับดูแลทรัพยากรด้านเทคโนโลยีสารสนเทศในระดับสูงให้มีประสิทธิภาพได้อย่างไร เมื่อใช้ร่วมกับ รายงานความเสี่ยงและการปฏิบัติตามข้อกำหนดของ AWS และ รายงานเกี่ยวกับรายการตรวจสอบการตรวจประเมินความปลอดภัย เอกสารฉบับนี้จะช่วยให้คุณเข้าใจคุณสมบัติด้านความปลอดภัยและการกำกับดูแลซึ่งมีอยู่ในบริการ AWS เพื่อรวมเอาประโยชน์ของการรักษาความปลอดภัยเข้ากับแนวทางปฏิบัติที่ดีสำหรับการสร้างสภาพแวดล้อมแบบครบวงจรด้วย AWS

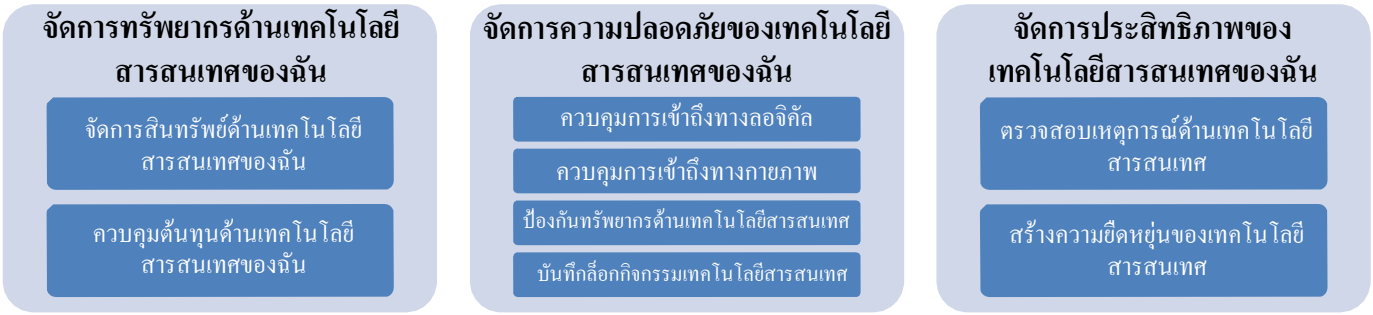
ข้อมูลเบื้องต้น

หน่วยงานด้านอุตสาหกรรมและกฎระเบียบได้ได้รวบรวมและจัดทำกฎหมายทั้งเก่าและใหม่มากมายเข้าไว้ด้วยกัน เพื่อบังคับใช้มาตรการด้านกำกับดูแลองค์กรและการรักษาความปลอดภัยต่างๆ ด้วยเหตุนี้ บริษัทวิจัยต่างๆ จึงได้ประเมินว่ามีหลายบริษัทใช้จ่ายเงินทุนด้านเทคโนโลยีสารสนเทศเพื่อจัดการกับโครงสร้างพื้นฐานมากถึงร้อยละ 75 และใช้เงินทุนด้านเทคโนโลยีสารสนเทศสำหรับงานเทคโนโลยีสารสนเทศที่เกี่ยวข้องโดยตรงกับธุรกิจของบริษัทเพียงร้อยละ 25 แนวทางสำคัญประการหนึ่งในการปรับปรุงตัววัดผลนี้คือ การจัดการกับข้อกำหนดการกำกับดูแลด้านเทคโนโลยีสารสนเทศของส่วนงานสนับสนุนให้มีประสิทธิภาพมากขึ้น วิธีที่ง่ายและมีประสิทธิภาพสำหรับเรื่องนี้ก็คือ การใช้ประโยชน์จากคุณสมบัติด้านการกำกับดูแลแบบสำเร็จรูปของ AWS

ถึงแม้ AWS จะมีคุณสมบัติที่สนับสนุนการกำกับดูแลด้านเทคโนโลยีสารสนเทศมากมาย แต่เรื่องยากอยู่ที่การตัดสินใจว่าจะเริ่มต้นอย่างไรและมีอะไรบ้างที่ต้องดำเนินการ เอกสารฉบับนี้พูดถึงหลักการกำกับดูแลด้านเทคโนโลยีสารสนเทศที่ใช้กันทั่วไปโดยการแสดงกรณีการใช้งาน (หรือความท้าทายภายในองค์กร) คุณสมบัติในการสนับสนุนของ AWS และการนำเสนอคุณค่าของการใช้คุณสมบัติเหล่านั้นที่สัมพันธ์กับการกำกับดูแล เอกสารฉบับนี้ออกแบบมาเพื่อช่วยให้คุณบรรลุวัตถุประสงค์ต่างๆ ของหลักการกำกับดูแลด้านเทคโนโลยีสารสนเทศแต่ละส่วน[1]

เอกสารฉบับนี้ยึดถือตามแนวทางของหลักการสำคัญๆ ของเฟรมเวิร์กการกำกับดูแลด้านเทคโนโลยีสารสนเทศที่ใช้กันอย่างแพร่หลาย (เช่น CoBIT, ITIL, COSO, CMMI ฯลฯ) อย่างไรก็ตาม หลักการกำกับดูแลด้านเทคโนโลยีสารสนเทศในเอกสารนี้เป็นเพียงข้อมูลทั่วไปที่ช่วยให้ลูกค้าใช้ประเมินคุณสมบัติด้านการกำกับดูแลของการใช้ AWS เทียบกับสิ่งที่สามารถดำเนินการโดยใช้ทรัพยากรและเครื่องมือต่างๆ ภายในองค์กรของคุณเท่านั้น หลักการกำกับดูแลด้านเทคโนโลยีสารสนเทศต่อไปนี้มีการอธิบายด้วยแนวทาง “กรณีการใช้งาน”:

ฉันต้องการทำให้ดีขึ้น...



[1] แม้ว่าเอกสารฉบับนี้จะมีรายการคุณสมบัติที่สนับสนุนการกำกับดูแลอยู่จำนวนมาก แต่เนื่องจากมีการพัฒนาคุณสมบัติใหม่ๆ อยู่ตลอดเวลา เอกสารนี้จึงไม่ได้ระบุถึงคุณสมบัติที่มีอยู่ทั้งหมด โปรดบทช่วยสอน เครื่องมือสำหรับนักพัฒนา และเอกสารประกอบเพิ่มเติมที่ http://aws.amazon.com/resources/

จัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ

จัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศ

การระบุและการจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศเป็นขั้นตอนแรกของการกำกับดูแลด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ สินทรัพย์ด้านเทคโนโลยีสารสนเทศมีได้ตั้งแต่เราเตอร์ สวิตช์ เซิร์ฟเวอร์ โฮสต์ และไฟร์วอลล์ระดับสูงไปจนถึงแอปพลิเคชัน บริการ ระบบปฏิบัติการ และสินทรัพย์ซอฟต์แวร์อื่นๆ ที่ใช้งานอยู่ในเครือข่าย รายการสินทรัพย์ฮาร์ดแวร์และซอฟต์แวร์ล่าสุดเป็นข้อมูลสำคัญสำหรับการตัดสินใจเกี่ยวกับการอัปเกรดและการจัดซื้อ การติดตามสถานะการรับประกัน หรือสำหรับการแก้ไขปัญหาและการรักษาความปลอดภัย การมีรายการสินทรัพย์ที่ถูกต้องกลายเป็นสิ่งที่จำเป็นสำหรับธุรกิจเพื่อให้สามารถมองเห็นข้อมูลได้ตามความต้องการและจัดทำรายงานที่มีความครอบคลุม นอกจากนี้ รายการข้อมูลสินทรัพย์ที่ครอบคลุมยังมีความสำคัญเป็นพิเศษสำหรับข้อกำหนดการปฏิบัติตามบางอย่างด้วย ตัวอย่างเช่น FISMA, SOX, PCI DSS และ HIPAA ต่างกำหนดให้รายการข้อมูลสินทรัพย์ที่ถูกต้องเป็นส่วนหนึ่งในข้อกำหนดของตน อย่างไรก็ตาม การรวมเอาทรัพยากรส่วนต่างๆ ภายในองค์กรเข้าด้วยกันก็อาจแค่ทำให้การดูแลรักษารายการข้อมูลนี้ยุ่งยาก หรืออย่างแย่ที่สุดเลยคือไม่สามารถดำเนินการได้ องค์กรต่างๆ มักใช้โซลูชันของบริษัทอื่นเพื่อสนับสนุนระบบอัตโนมัติในการทำรายการข้อมูลสินทรัพย์ และถึงอย่างนั้นก็ยังไม่สามารถดูรายการของสินทรัพย์ทุกประเภทได้อย่างละเอียดในคอนโซลเดียวเสมอไป

การใช้ AWS ทำให้มีคุณสมบัติต่างๆ ในการดูรายการข้อมูลที่ถูกต้องของทรัพยากรด้านเทคโนโลยีสารสนเทศของ AWS ได้อย่างรวดเร็วและง่ายดาย โปรดดูคุณสมบัติเหล่านั้น คำแนะนำเกี่ยวกับ ‘วิธีการ’ ที่เกี่ยวข้อง และลิงก์ต่างๆ เพื่อเรียนรู้เพิ่มเติมเกี่ยวกับคุณสมบัติที่ด้านล่าง:

คุณสมบัติที่สนับสนุนการกำกับดูแลของ AWS	การได้รับความปลอดภัยตามขนาดที่เหมาะสม
เพจ Account Activity	แสดงรายการสรุปของทรัพยากรด้านเทคโนโลยีสารสนเทศโดยการให้รายละเอียดการใช้งานแต่ละบริการตามภูมิภาค เรียนรู้เพิ่มเติม
คลังชุดเก็บข้อมูลประจำตัวของ Amazon Glacier	เสนอรายการข้อมูลของ Glacier โดยการแสดงทรัพยากรด้านเทคโนโลยีสารสนเทศทั้งหมดใน Glacier เรียนรู้เพิ่มเติม
AWS CloudHSM	เสนอการควบคุมคีย์การเข้ารหัสแบบเสมือนและแบบกายภาพโดยการจัดหา HSM เฉพาะลูกค้าเพื่อใช้ในการจัดเก็บข้อมูลคีย์ เรียนรู้เพิ่มเติม
AWS Data Pipeline Task Runner	ดำเนินการประมวลผลงานแบบอัตโนมัติโดยการโพลล์ AWS Data Pipeline สำหรับงานต่างๆ แล้วจึงจัดการและรายงานสถานะของงานเหล่านั้น เรียนรู้เพิ่มเติม
AWS Management Console	เสนอรายการของสินทรัพย์และข้อมูลแบบในเวลาจริงโดยการแสดงทรัพยากรด้านเทคโนโลยีสารสนเทศทั้งหมดที่ทำงานอยู่ใน AWS ตามบริการ เรียนรู้เพิ่มเติม
AWS Storage Gateway APIs	เสนอความสามารถในการจัดทำโปรแกรมรายการสินทรัพย์และข้อมูลโดยการเขียนโปรแกรมอินเทอร์เฟส เครื่องมือ และสคริปต์เพื่อจัดการทรัพยากร เรียนรู้เพิ่มเติม

ควบคุมต้นทุนด้านเทคโนโลยีสารสนเทศ

คุณสามารถควบคุมต้นทุนด้านเทคโนโลยีสารสนเทศได้ดีขึ้นด้วยการใช้วิธีการที่คุ้มค่าที่สุดในการเป็นเจ้าของทรัพยากรโดยการทำความเข้าใจต้นทุนต่างๆ ของบริการด้านเทคโนโลยีสารสนเทศ อย่างไรก็ตาม การจัดการและการติดตามต้นทุนและ ROI ที่เกี่ยวข้องกับทรัพยากรด้านเทคโนโลยีสารสนเทศที่ใช้ภายในองค์กรอาจเป็นเรื่องยากและไม่แม่นยำนัก เนื่องจากเป็นการคำนวณที่ซับซ้อนมาก การวางแผนเกี่ยวกับความสามารถ การคาดการณ์สำหรับการใช้งาน ต้นทุนในการจัดซื้อ ค่าเสื่อมราคา ต้นทุนที่เป็นเงินทุน และต้นทุนสำหรับสิ่งอำนวยความสะดวกเป็นแค่บางส่วนที่ทำให้การคำนวณต้นทุนโดยรวมในการเป็นเจ้าของเป็นเรื่องยาก

เมื่อใช้ AWS คุณจะมีคุณสมบัติหลายอย่างที่ช่วยให้เข้าใจและควบคุมต้นทุนของทรัพยากรด้านเทคโนโลยีสารสนเทศได้ง่ายๆ และถูกต้องแม่นยำ เมื่อใช้ AWS คุณสามารถลดต้นทุนลงได้ถึงร้อยละ 80 เมื่อเทียบกับการใช้งานระบบภายในองค์กรที่ทัดเทียมกัน[2] โปรดดูคุณสมบัติเหล่านั้น คำแนะนำเกี่ยวกับ 'วิธีการ' ที่เกี่ยวข้อง และลิงก์ต่างๆ เพื่อเรียนรู้เพิ่มเติมเกี่ยวกับคุณสมบัติที่ด้านล่าง:

คุณสมบัติที่สนับสนุนการกำกับดูแลของ AWS	การได้รับความปลอดภัยตามขนาดที่เหมาะสม
เพจ Account Activity	แสดงต้นทุนของการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศในทุกช่วงเวลาโดยการแสดงทรัพยากรที่ใช้ตามบริการ เรียนรู้เพิ่มเติม
การเปิดใช้งานอินสแตนซ์การตรวจสอบความถูกต้องตามจริงของ Amazon EC2	ช่วยป้องกันความผิดพลาดในการเปิดใช้งานทรัพยากรและการเกิดต้นทุนเพิ่มเติม โดยป้องกันไม่ให้มีการหมดเวลาหรือความผิดพลาดในการเชื่อมต่อจากการเปิดใช้งานอินสแตนซ์เพิ่มเติม เรียนรู้เพิ่มเติม
การติดแท็กทรัพยากรของ Amazon EC2	แสดงความสัมพันธ์ระหว่างต้นทุนของทรัพยากรและหน่วยธุรกิจโดยใช้ป้ายกำกับแบบกำหนดเองที่สามารถค้นหาได้ในการประมวลผลทรัพยากร เรียนรู้เพิ่มเติม
AWS Account Billing	มีคุณสมบัติการเรียกเก็บเงินที่ใช้งานง่าย ซึ่งจะช่วยตรวจสอบและชำระเงินตามใบเรียกเก็บโดยการให้รายละเอียดของทรัพยากรที่ใช้และต้นทุนที่เกี่ยวข้องที่มีการคำนวณตามจริง เรียนรู้เพิ่มเติม
AWS Management Console	เสนอมุมมองแบบครบวงจรในตำแหน่งเดียวของปัจจัยด้านต้นทุนโดยการแสดงทรัพยากรด้านเทคโนโลยีสารสนเทศทั้งหมดที่ทำงานอยู่ใน AWS ตามบริการ รวมถึงค่าใช้ค่าจ่ายจริงและอัตราการเรียกใช้ เรียนรู้เพิ่มเติม
การกำหนดราคาบริการ AWS ที่เกี่ยวข้อง	เสนอการรับรู้ที่ชัดเจนเกี่ยวกับต้นทุนของทรัพยากรด้านเทคโนโลยีสารสนเทศของ AWS โดยการกำหนดราคาสำหรับผลิตภัณฑ์ AWS แต่ละอย่างและลักษณะของการกำหนดราคาเฉพาะเจาะจง เรียนรู้เพิ่มเติม
AWS Trusted Advisor	ช่วยปรับปรุงต้นทุนของทรัพยากรด้านเทคโนโลยีสารสนเทศโดยการค้นหาทรัพยากรที่ไม่ได้ใช้และที่ไม่ได้ทำงานอยู่ เรียนรู้เพิ่มเติม
การแจ้งเตือนการเรียกเก็บเงิน	แสดงการแจ้งเตือนล่วงหน้าเกี่ยวกับการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศโดยส่งการแจ้งข้อมูลของกิจกรรมที่มีการใช้จ่าย เรียนรู้เพิ่มเติม
การเรียกเก็บเงินรวม	เสนอการควบคุมต้นทุนแบบรวมศูนย์และการแสดงผลต้นทุนข้ามบัญชีโดยการรวมหลายบัญชี AWS เข้าไว้ในใบเรียกเก็บเงินเดียว เรียนรู้เพิ่มเติม

[2] โปรดดู รายงานต้นทุนรวมในการเป็นเจ้าของ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการประหยัดต้นทุนรวมด้วยการใช้ AWS

การกำหนดราคาค่าบริการที่ใช้ตามจริง	แสดงการคำนวณทรัพยากรและบริการต่างๆ ที่คุณสามารถใช้สร้างแอปพลิเคชันภายในไม่กี่นาทีตาม การกำหนดราคาค่าบริการที่ใช้ตามจริง ไม่มีต้นทุนในการจัดซื้อล่วงหน้า หรือต้นทุนในการดูแล รักษาแบบต่อเนื่อง โดยการปรับขนาดการใช้งานไปยังหลายๆ เซิร์ฟเวอร์โดยอัตโนมัติเมื่อมีความ ต้องการแอปพลิเคชันเพิ่มขึ้น เรียนรู้เพิ่มเติม

จัดการความปลอดภัยของเทคโนโลยีสารสนเทศ

ควบคุมการเข้าถึงทรัพยากรด้านเทคโนโลยีสารสนเทศทางกายภาพ

การจัดการการเข้าถึงทางกายภาพเป็นส่วนประกอบสำคัญของโปรแกรมการกำกับดูแลด้านเทคโนโลยีสารสนเทศ นอกเหนือจากการล็อค สัญญาณเตือนภัย การควบคุมการเข้าถึง และวิดีโอวงจรปิดที่เป็นส่วนประกอบแบบดั้งเดิมของการรักษาความปลอดภัยทางกายภาพแล้ว การควบคุมทางอิเล็กทรอนิกส์สำหรับการเข้าถึงทางกายภาพยังมีความสำคัญอย่างมากในการรักษาความปลอดภัยทางกายภาพให้มีประสิทธิภาพ อุตสาหกรรมการรักษาความปลอดภัยทางกายภาพแบบดั้งเดิมกำลังเปลี่ยนแปลงอย่างรวดเร็วและขอบเขตของความเชี่ยวชาญเฉพาะทำให้การรักษาความปลอดภัยทางกายภาพมีความซับซ้อนเพิ่มขึ้นมาก เนื่องจากวิธีการควบคุมและข้อควรพิจารณาสำหรับการรักษาความปลอดภัยทางกายภาพภายในองค์กรมีความซับซ้อนมากขึ้น ทำให้ผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศที่มีความเชี่ยวชาญ และมีคุณสมบัติเฉพาะด้านเป็นที่ต้องการตัวเพื่อมาจัดการกับการควบคุมทางกายภาพเกี่ยวกับข้อมูลประจำตัวในการเข้าถึงสำหรับบัตร/เครื่องอ่านบัตร อุปกรณ์ควบคุม และเซิร์ฟเวอร์ระบบสำหรับการโฮสต์ข้อมูลเกี่ยวกับการรักษาความปลอดภัยทางกายภาพให้มีประสิทธิภาพ

เมื่อใช้ AWS คุณสามารถเอาต์ซอร์สการควบคุมที่เกี่ยวข้องกับการรักษาความปลอดภัยทางกายภาพโครงสร้างพื้นฐานของ AWS ให้กับผู้เชี่ยวชาญของ AWS ที่มีทักษะและได้รับทรัพยากรที่จำเป็นในการรักษาความปลอดภัยสภาพแวดล้อมทางกายภาพได้อย่างง่ายดายและมีประสิทธิภาพ AWS มีผู้ตรวจสอบอิสระหลายรายทำหน้าที่ตรวจสอบความปลอดภัยทางกายภาพของศูนย์ข้อมูลตลอดทั้งปี เพื่อรับรองถึงการออกแบบและการทดสอบอย่างละเอียดเกี่ยวกับประสิทธิภาพของการควบคุมด้านความปลอดภัยทางกายภาพของเรา เรียนรู้เพิ่มเติมเกี่ยวกับโปรแกรมตรวจสอบของ AWS และการควบคุมความปลอดภัยทางกายภาพที่เกี่ยวข้องที่ด้านล่าง:

คุณสมบัติที่สนับสนุนการกำกับดูแลของ AWS	การได้รับความปลอดภัยตามขนาดที่เหมาะสม
การควบคุมการเข้าถึงทางกายภาพของ AWS SOC 1	เสนอการควบคุมที่มีความโปร่งใสเพื่อป้องกันการเข้าถึงศูนย์ข้อมูลโดยไม่ได้รับอนุญาต การควบคุมมีการออกแบบ ทดสอบ และตรวจสอบอย่างถูกต้องโดยบริษัทตรวจสอบอิสระ เรียนรู้เพิ่มเติม
การควบคุมการเข้าถึงทางกายภาพของ AWS SOC 2-Security	เสนอการควบคุมที่มีความโปร่งใสเพื่อป้องกันการเข้าถึงศูนย์ข้อมูลโดยไม่ได้รับอนุญาต การควบคุมมีการออกแบบ ทดสอบ และตรวจสอบอย่างถูกต้องโดยบริษัทตรวจสอบอิสระ เรียนรู้เพิ่มเติม
การควบคุมการเข้าถึงทางกายภาพของ AWS PCI DSS	เสนอการควบคุมที่มีความโปร่งใสเพื่อป้องกันการเข้าถึงศูนย์ข้อมูลโดยไม่ได้รับอนุญาต ซึ่งสัมพันธ์กับมาตรฐานการรักษาความปลอดภัยสำหรับอุตสาหกรรมการชำระเงินผ่านบัตรเครดิต การควบคุมมีการออกแบบ ทดสอบ และตรวจสอบอย่างถูกต้องโดยบริษัทตรวจสอบอิสระ เรียนรู้เพิ่มเติม
การควบคุมการเข้าถึงทางกายภาพของ AWS ISO 27001	เสนอการควบคุมและกระบวนการที่มีความโปร่งใสเพื่อป้องกันการเข้าถึงศูนย์ข้อมูลโดยไม่ได้รับอนุญาต ซึ่งสัมพันธ์กับมาตรฐานแนวทางการปฏิบัติของการรักษาความปลอดภัยของ ISO 27002 การควบคุมมีการออกแบบ ทดสอบ และตรวจสอบอย่างถูกต้องโดยบริษัทตรวจสอบอิสระ เรียนรู้เพิ่มเติม

การควบคุมการเข้าถึงทางกายภาพของ AWS FedRAMP	เสนอการควบคุมและกระบวนการที่มีความโปร่งใสเพื่อป้องกันการเข้าถึงศูนย์ข้อมูลโดยไม่ได้รับอนุญาต ซึ่งสัมพันธ์กับมาตรฐานที่เป็นแนวทางปฏิบัติของ NIST 800-53 การควบคุมมีการออกแบบ ทดสอบ และตรวจสอบอย่างถูกต้องโดยบริษัทตรวจสอบอิสระที่ได้รับการรับรองจากรัฐบาล เรียนรู้เพิ่มเติม

ควบคุมการเข้าถึงทรัพยากรด้านเทคโนโลยีสารสนเทศแบบลอจิคัล

วัตถุประสงค์หลักประการหนึ่งของการกำกับดูแลด้านเทคโนโลยีสารสนเทศคือ การจัดการกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลแบบลอจิคัลอย่างมีประสิทธิภาพ อย่างไรก็ตาม องค์กรจำนวนมากพยายามที่จะปรับขนาดโซลูชันภายในองค์กรของตนให้สามารถรองรับข้อควรพิจารณาและความซับซ้อนของการเข้าถึงแบบลอจิคัลที่มีการเติบโตและเปลี่ยนแปลงอยู่ตลอดเวลา รวมถึงความสามารถในการสร้างกฎของสิทธิ์ระดับน้อยที่สุด จัดการกับสิทธิ์ในการเข้าถึงทรัพยากร รับมือกับการเปลี่ยนแปลงบทบาทและความต้องการข้อมูล และการเติบโตของข้อมูลที่สำคัญ ความท้าทายหลักๆ ที่ไม่เคยหายไปสำหรับการจัดการกับการเข้าถึงแบบลอจิคัลในสภาพแวดล้อมภายในองค์กรคือ การให้สิทธิ์การเข้าถึงกับผู้ใช้ตาม:

- บทบาท (เช่น ผู้ใช้อินเทอร์เน็ต ผู้รับเหมา บุคคลภายนอก หุ้นส่วน ฯลฯ)
- การจัดหมวดหมู่ข้อมูล (เช่น ข้อมูลที่เป็นความลับ ใช้ภายในเท่านั้น ส่วนตัว สาธารณะ ฯลฯ)
- ชนิดข้อมูล (เช่น ข้อมูลประจำตัว ข้อมูลส่วนบุคคล ข้อมูลการติดต่อ ข้อมูลที่เกี่ยวข้องกับงาน ใบรับรองดิจิทัล รหัสผ่านแบบกระบวนการรับรู้ ฯลฯ)

AWS มีคุณสมบัติด้านการควบคุมมากมายที่ให้คุณสามารถใช้จัดการกับการเข้าถึงแบบลอจิคัลได้อย่างมีประสิทธิภาพตามตารางการทำงานของระบบที่ยึดตามสิทธิ์ระดับน้อยที่สุด โปรดดูคุณสมบัติเหล่านั้น คำแนะนำเกี่ยวกับ 'วิธีการ' ที่เกี่ยวข้อง และลิงก์ต่างๆ เพื่อเรียนรู้เพิ่มเติมเกี่ยวกับคุณสมบัติที่ด้านล่าง:

คุณสมบัติที่สนับสนุนการกำกับดูแลของ AWS	การได้รับความปลอดภัยตามขนาดที่เหมาะสม
รายการควบคุมการเข้าถึง Amazon S3 (ACL)	เสนอสิทธิ์และเงื่อนไขแบบส่วนกลางโดยการเพิ่มเงื่อนไขเฉพาะเพื่อควบคุมวิธีการเข้าใช้งาน AWS ของผู้ใช้ เช่น เวลาของวัน ที่อยู่ IP ต้นทาง ไม่ว่าจะใช้ SSL หรือได้รับการรับรองด้วยอุปกรณ์ Multi-Factor Authentication เรียนรู้เพิ่มเติม ที่นี่ และ ที่นี่
นโยบายบัคเก็ต Amazon S3	เสนอความสามารถในการสร้างกฎที่มีเงื่อนไขสำหรับการจัดการกับการเข้าถึงบัคเก็ตและออบเจ็กต์โดยการให้คุณสามารถจำกัดการเข้าถึงตามบัญชี รวมถึงแอตทริบิวต์ตามคำขอ เช่น ตัวอ้างอิง HTTP และที่อยู่ IP เรียนรู้เพิ่มเติม
การรับรองความถูกต้องของสตริงการสืบค้น Amazon S3	มีความสามารถในการให้ HTTP หรือเบราว์เซอร์สามารถเข้าถึงทรัพยากรที่ตามปกติแล้วต้องได้รับการรับรองความถูกต้องโดยการใช้ลายเซ็นในสตริงการสืบค้นเพื่อรักษาความปลอดภัยคำขอ เรียนรู้เพิ่มเติม
AWS CloudTrail	มีการบันทึกล็อกการทำงานของ API หรือคอนโซล (เช่น บันทึกล็อกหากผู้อื่นเปลี่ยนแปลงนโยบายบัคเก็ต การหยุดทำงานและอินสแตนซ์ ฯลฯ) ทำให้สามารถตรวจสอบขั้นสูงได้ เรียนรู้เพิ่มเติม
AWS IAM Multi-Factor Authentication (MFA)	เสนอการบังคับใช้ MFA กับทรัพยากรทั้งหมดโดยการกำหนดให้มีโทเค็นในการลงชื่อเข้าใช้และเข้าถึงทรัพยากร เรียนรู้เพิ่มเติม

นโยบายรหัสผ่านของ AWS IAM	เสนอความสามารถในการจัดการกับคุณภาพและการควบคุมรหัสผ่านของผู้ใช้โดยอนุญาตให้คุณกำหนดนโยบายรหัสผ่านสำหรับรหัสผ่านของผู้ใช้ IAM โดยการระบุว่ารหัสผ่านต้องมีความยาวที่แน่นอนและต้องมีการเลือกอักขระ ฯลฯ เรียนรู้เพิ่มเติม
สิทธิ์ของ AWS IAM	มีความสามารถในการจัดการสิทธิ์ได้ง่ายๆ โดยการให้คุณระบุผู้ที่มีสิทธิ์เข้าถึงทรัพยากรของ AWS และสิ่งที่พวกเขาสามารถดำเนินการกับทรัพยากรเหล่านี้ เรียนรู้เพิ่มเติม
นโยบาย AWS IAM	ให้คุณสามารถจัดการกับการเข้าถึงด้วยสิทธิ์ระดับน้อยที่สุดแบบละเอียดโดยการอนุญาตให้สร้างหลายผู้ใช้ภายในบัญชี AWS และกำหนดข้อมูลประจำตัวในการรักษาความปลอดภัยให้กับผู้ใช้และจัดการสิทธิ์ของผู้ใช้ เรียนรู้เพิ่มเติม
บทบาทของ AWS IAM	เสนอความสามารถในการกำหนดสิทธิ์การเข้าถึงชั่วคราวให้กับผู้ใช้หรือบริการที่ตามปกติแล้วไม่มีสิทธิ์เข้าถึงทรัพยากร AWS โดยการกำหนดชุดของสิทธิ์เพื่อเข้าถึงทรัพยากรที่ผู้ใช้หรือบริการต้องการ เรียนรู้เพิ่มเติม
AWS Trusted Advisor	เสนอการประเมินการจัดการความปลอดภัยอัตโนมัติโดยการค้นหาและการเลื่อนระดับปัญหาเกี่ยวกับสิทธิ์และความปลอดภัยที่เป็นไปได้ เรียนรู้เพิ่มเติม

ดูแลทรัพยากรด้านเทคโนโลยีสารสนเทศให้ปลอดภัย

การดูแลทรัพยากรด้านเทคโนโลยีสารสนเทศให้ปลอดภัยเป็นพื้นฐานสำคัญของโปรแกรมการกำกับดูแลด้านเทคโนโลยีสารสนเทศ อย่างไรก็ตาม สำหรับสภาพแวดล้อมภายในองค์กร มีขั้นตอนการรักษาความปลอดภัยที่ต้องดำเนินการเมื่อมีการออนไลน์เซิร์ฟเวอร์ใหม่ ตัวอย่างเช่น ไฟร์วอลล์และนโยบายการควบคุมการเข้าถึงจะต้องได้รับการอัปเดต อิมเมจของเซิร์ฟเวอร์ที่สร้างใหม่ต้องได้รับการตรวจสอบว่าเป็นไปตามนโยบายการรักษาความปลอดภัย และแพ็คเกตของซอฟต์แวร์ทั้งหมดต้องเป็นเวอร์ชันล่าสุด เว้นแต่การรักษาความปลอดภัยเหล่านี้จะดำเนินการโดยอัตโนมัติและให้บริการด้วยวิธีการที่สามารถตอบสนองต่อความต้องการที่ต้องมีการปรับเปลี่ยนสูงของธุรกิจ องค์กรที่ทำงานโดยใช้การกำกับดูแลแบบดั้งเดิมเพียงอย่างเดียวทำให้ผู้ใช้ต้องแก้ไขปัญหาการควบคุมความปลอดภัย ไม่เช่นนั้นจะทำให้เกิดความล่าช้าที่สร้างต้นทุนสูงให้กับธุรกิจ

AWS มีคุณสมบัติการรักษาความปลอดภัยมากมายที่ช่วยให้คุณดูแลทรัพยากรด้านเทคโนโลยีสารสนเทศให้ปลอดภัยได้อย่างง่ายดายและมีประสิทธิภาพ โปรดดูคุณสมบัติเหล่านั้น คำแนะนำเกี่ยวกับ 'วิธีการ' ที่เกี่ยวข้อง และลิงก์ต่างๆ เพื่อเรียนรู้เพิ่มเติมเกี่ยวกับคุณสมบัติที่ด้านล่าง:

คุณสมบัติที่สนับสนุนการกำกับดูแลของ AWS	การได้รับความปลอดภัยตามขนาดที่เหมาะสม
Amazon Linux AMIs	มีความสามารถในการปรับใช้อิมเมจ "รุ่นสมบูรณ์" (เสริมความปลอดภัย) โดยการจัดทำอิมเมจแบบส่วนตัวที่จะใช้กับอินสแตนซ์ทั้งหมด เรียนรู้เพิ่มเติม
อินสแตนซ์เฉพาะของ Amazon EC2	เสนอเครือข่ายแบบเสมือนแบบส่วนตัวที่แยกออกมา และทำให้แน่ใจว่าอินสแตนซ์การประมวลผลของ Amazon EC2 จะถูกแยกออกมาที่ระดับฮาร์ดแวร์ และมีการเปิดใช้งานอินสแตนซ์เหล่านี้ใน VPC เรียนรู้เพิ่มเติม
วิซาร์ดการเปิดใช้งาน Amazon EC2 Instance	ช่วยให้กระบวนการเปิดใช้งานสอดคล้องกันโดยการกำหนดข้อจำกัดเกี่ยวกับอิมเมจของเครื่องที่สามารถใช้งานได้เมื่อเปิดใช้งานอินสแตนซ์ เรียนรู้เพิ่มเติม

กลุ่มความปลอดภัยของ Amazon EC2	เสนอการควบคุมการรับส่งข้อมูลขาเข้าและขาออกแบบมีรายละเอียดแยกย่อย โดยการทำงานเหมือนกับไฟรวอลล์ที่ควบคุมการรับส่งข้อมูลสำหรับอินสแตนซ์เดียวหรือมากกว่า เรียนรู้เพิ่มเติม
ที่เก็บถาวรของ Amazon Glacier	เสนอบริการจัดเก็บข้อมูลระยะยาวราคาประหยัดสำหรับการเก็บรักษาข้อมูลแบบถาวรและการสำรองข้อมูลที่ปลอดภัยและมั่นคงโดยใช้การเข้ารหัส AES 256 บิตเป็นค่าเริ่มต้น เรียนรู้เพิ่มเติม
Amazon S3 Client-Side Encryption	เสนอความสามารถในการเข้ารหัสข้อมูลก่อนที่จะส่งไปยัง Amazon S3 โดยการสร้างไลบรารีของตนเองที่เข้ารหัสข้อมูลออบเจ็กต์บนฝั่งไคลเอ็นต์ก่อนที่จะอัปโหลดไปยัง Amazon S3 AWS SDK for Java ยังสามารถเข้ารหัสข้อมูลโดยอัตโนมัติก่อนที่จะอัปโหลดไปยัง Amazon S3 ได้ด้วย เรียนรู้เพิ่มเติม
Amazon S3 Server-Side Encryption	เสนอการเข้ารหัสออบเจ็กต์ที่จัดเก็บและคีย์ที่จัดการโดย AWS ด้วยการใช้การเข้ารหัส AES 256 บิตสำหรับข้อมูล Amazon S3 เรียนรู้เพิ่มเติม
Amazon VPC	เสนอเครือข่ายเสมือนซึ่งแทบจะเหมือนกับเครือข่ายแบบเดิมที่ใช้งานภายในองค์กร แต่มีข้อดีในการใช้โครงสร้างพื้นฐานที่สามารถปรับขยายได้ของ AWS คุณจึงสามารถสร้างเซกชันที่แยกกันทางลอจิคัลของ AWS ที่จะเปิดใช้งานทรัพยากรของ AWS ในเครือข่ายเสมือนที่คุณกำหนดได้ เรียนรู้เพิ่มเติม
การแยกส่วนทางลอจิคัลของ Amazon VPC	มีการแยกส่วนแบบเสมือนของทรัพยากรโดยสามารถแยกส่วนอิมเมจของเครื่องออกจากทรัพยากรบนเครือข่ายอื่นๆ ได้ เรียนรู้เพิ่มเติม
ACL เครือข่ายของ Amazon VPC	เสนอการแยกส่วน 'แบบไฟร์วอลล์' สำหรับซับเน็ตที่เชื่อมโยงกันโดยการควบคุมการใช้งานเครือข่ายขาเข้าและขาออกที่ระดับซับเน็ต เรียนรู้เพิ่มเติม
ที่อยู่ IP ส่วนตัวของ Amazon VPC	ช่วยป้องกันที่อยู่ IP ส่วนตัวจากความสุ่มเสี่ยงบนอินเทอร์เน็ตโดยการกำหนดเส้นทางการรับส่งข้อมูลผ่านทางอินสแตนซ์ Network Address Translation (NAT) ในซับเน็ตสาธารณะ เรียนรู้เพิ่มเติม
กลุ่มความปลอดภัยของ Amazon VPC	มีการแยกส่วน 'แบบไฟร์วอลล์' สำหรับAmazon EC2 Instance ที่เชื่อมโยงกันโดยการควบคุมการใช้งานเครือข่ายขาเข้าและขาออกที่ระดับอินสแตนซ์ เรียนรู้เพิ่มเติม
เทมเพลต AWS CloudFormation	เสนอความสามารถในการใช้อิมเมจของเครื่องเฉพาะร่วมกับทรัพยากรอื่นๆ อย่างสอดคล้องกันและมีการกำหนดค่าโดยการเตรียมใช้งานโครงสร้างพื้นฐานด้วยสคริปต์ต่างๆ เรียนรู้เพิ่มเติม
AWS Direct Connect	ขจัดความจำเป็นในการเชื่อมต่ออินเทอร์เน็ตสาธารณะกับ AWS โดยการกำหนดการเชื่อมต่อเครือข่ายเฉพาะจากสถานที่ตั้งไปยังศูนย์ข้อมูลของ AWS เรียนรู้เพิ่มเติม
การเชื่อมต่อ VPN สำหรับฮาร์ดแวร์/ซอฟต์แวร์ภายในองค์กร	เสนอการควบคุมความปลอดภัยของเครือข่ายแบบมีรายละเอียดแยกย่อยโดยการอนุญาตให้มีการเชื่อมต่อที่ปลอดภัยจากเครือข่ายที่มีอยู่กับ AWS เรียนรู้เพิ่มเติม
เกตเวย์ส่วนตัวแบบเสมือน	เสนอการควบคุมความปลอดภัยของเครือข่ายแบบมีรายละเอียดแยกย่อยโดยการสร้างการเชื่อมต่อ VPN สำหรับฮาร์ดแวร์กับ VPC เรียนรู้เพิ่มเติม

จัดการกับการบันทึกล็อกทรัพยากรด้านเทคโนโลยีสารสนเทศ

เครื่องมือสนับสนุนหลักในการรักษาความปลอดภัยเทคโนโลยีสารสนเทศคือ การบันทึกล็อกทรัพยากรด้านเทคโนโลยีสารสนเทศ การบันทึกล็อกมีความสำคัญอย่างยิ่งต่อการกำกับดูแลด้านเทคโนโลยีสารสนเทศสำหรับกรณีการใช้งานลักษณะต่างๆ รวมถึงแต่ไม่จำกัดเฉพาะ: การตรวจสอบ/การติดตามพฤติกรรมที่น่าสงสัย การสนับสนุนการวิเคราะห์เพื่อการพิสูจน์หลักฐาน การตอบสนองต่อข้อกำหนดการปฏิบัติตาม การสนับสนุนการดูแลรักษาและการดำเนินงานด้านเทคโนโลยีสารสนเทศ/ระบบเครือข่าย การจัดการ/การลดต้นทุนในการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ การตรวจสอบระดับการบริการ และการสนับสนุนกระบวนการภายในของธุรกิจ องค์กรต่างๆ พึ่งพาการจัดการล็อกที่มีประสิทธิภาพมากขึ้นเรื่อยๆ เพื่อสนับสนุนการทำงานด้านการควบคุมดูแลหลักๆ รวมถึงการจัดการต้นทุน ระดับการบริการ และการตรวจสอบแอปพลิเคชันสำหรับธุรกิจ และกิจกรรมที่ให้ความสำคัญกับการปฏิบัติตามและการรักษาความปลอดภัยเทคโนโลยีสารสนเทศอื่นๆ SANS Log Management Survey แสดงให้เห็นอย่างสอดคล้องกันว่าองค์กรต่างๆ ต้องการใช้ประโยชน์จากล็อกของตนเองเพิ่มขึ้นอย่างต่อเนื่อง แต่ก็ต้องเจอปัญหาเกี่ยวกับความสามารถในการใช้กรณีการใช้งานกับทรัพยากรภายในองค์กรที่จะรวบรวมและวิเคราะห์ล็อกเหล่านั้น เมื่อมีการรวบรวมและวิเคราะห์ล็อกหลากหลายประเภทมากขึ้นจากแหล่งข้อมูลด้านเทคโนโลยีสารสนเทศที่แตกต่างกัน องค์กรต้องรับภาระต้นทุนในการดำเนินการที่เกี่ยวข้องกับการปรับข้อมูลล็อกให้เป็นรูปแบบต่างๆ ที่มีการใช้งานกันอย่างกว้างขวาง พร้อมกับมีฟังก์ชันการค้นหา การรวบรวม และการรายงาน การจัดการล็อกเป็นความสามารถสำคัญในการตรวจสอบความปลอดภัย การปฏิบัติตามข้อกำหนด และการตัดสินใจที่มีประสิทธิภาพสำหรับกิจกรรมนับหมื่นนับแสนรายการในแต่ละวัน

เมื่อใช้ AWS ทำให้มีคุณสมบัติการบันทึกล็อกมากมายที่ช่วยให้คุณบันทึกล็อกและติดตามการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ โปรดดูคุณสมบัติเหล่านั้น คำแนะนำเกี่ยวกับ 'วิธีการ' ที่เกี่ยวข้อง และลิงก์ต่างๆ เพื่อเรียนรู้เพิ่มเติมเกี่ยวกับคุณสมบัติที่ด้านล่าง:

คุณสมบัติที่สนับสนุนการกำกับดูแลของ AWS	การได้รับความปลอดภัยตามขนาดที่เหมาะสม
ล็อกการเข้าถึงของ Amazon CloudFront	จัดทำไฟล์ล็อกที่มีข้อมูลเกี่ยวกับการเข้าถึงออบเจ็กต์ต่างๆ ของผู้ใช้ ล็อกสามารถกระจายไปยังบัคเก็ต Amazon S3 เฉพาะได้โดยตรง เรียนรู้ เพิ่มเติม
ล็อกของฐานข้อมูล Amazon RDS	เสนอวิธีในการตรวจสอบจำนวนของไฟล์ล็อกที่สร้างโดยอินสแตนซ์ฐานข้อมูล Amazon RDS ใช้เพื่อวิเคราะห์ แก้ไขปัญหา และแก้ไขปัญหาการกำหนดค่าฐานข้อมูลหรือประสิทธิภาพการทำงาน เรียนรู้เพิ่มเติม
Amazon S3 Object Expiration	เสนอการหมดอายุของล็อกแบบอัตโนมัติโดยการจัดกำหนดเวลาเอาออบเจ็กต์ออกหลังจากช่วงเวลาที่กำหนด เรียนรู้เพิ่มเติม
ล็อกการเข้าถึงเซิร์ฟเวอร์ Amazon S3	จัดทำล็อกของคำขอเข้าถึงที่มีรายละเอียดเกี่ยวกับคำขอ เช่น ประเภทคำขอ ทรัพยากรที่ต้องการร้องขอ และเวลาและวันที่ที่มีการดำเนินการกับคำขอ เรียนรู้เพิ่มเติม
AWS CloudTrail	จัดทำล็อกของการดำเนินการด้านความปลอดภัยที่เสร็จสิ้นแล้วผ่านทาง AWS Management Console หรือ API เรียนรู้เพิ่มเติม

จัดการกับประสิทธิภาพของเทคโนโลยีสารสนเทศ

ตรวจสอบและตอบสนองต่อเหตุการณ์

การจัดการประสิทธิภาพของเทคโนโลยีสารสนเทศและการตรวจสอบกลายเป็นส่วนสำคัญเชิงกลยุทธ์ของโปรแกรมการกำกับดูแลด้านเทคโนโลยีสารสนเทศ การตรวจสอบด้านเทคโนโลยีสารสนเทศเป็นองค์ประกอบสำคัญของการกำกับดูแลที่จะช่วยคุณป้องกัน ตรวจสอบ และแก้ไขปัญหาด้านเทคโนโลยีสารสนเทศที่อาจส่งผลกระทบกับประสิทธิภาพและ/หรือความปลอดภัย ความท้าทายสำคัญของการกำกับดูแลสภาพแวดล้อมภายในองค์กรสำหรับการจัดการประสิทธิภาพของเทคโนโลยีสารสนเทศคือ คุณต้องเผชิญกับการตรวจสอบหลายระบบเพื่อจัดการกับทุกระดับชั้นของทรัพยากรด้านเทคโนโลยีสารสนเทศและการผสมกันของเครื่องมือการจัดการที่มีกรรมสิทธิ์และกระบวนการของเทคโนโลยีสารสนเทศ ซึ่งทำให้เกิดความซับซ้อนของระบบ ถ้าโชคดีระบบอาจแค่ตอบสนองช้า แต่ในกรณีเลวร้ายที่สุดคือมีผลกระทบกับประสิทธิภาพในการตรวจสอบและการจัดการกับการทำงานด้านเทคโนโลยีสารสนเทศ ยิ่งไปกว่านั้น รูปแบบการคุกคามความปลอดภัยที่มีความซับซ้อนและทันสมัยมากขึ้น ทำให้ความสามารถในการตรวจสอบเหตุการณ์และการตอบสนองต้องพัฒนาอย่างต่อเนื่องและรวดเร็วทันกับการจัดการภัยคุกคามต่างๆ ซึ่งทำให้การจัดการกับประสิทธิภาพภายในองค์กรกำลังเผชิญกับความท้าทายที่เพิ่มขึ้นอย่างต่อเนื่องเกี่ยวกับการจัดหาโครงสร้างพื้นฐาน ความสามารถในการปรับขยาย ความสามารถในการจำลองเงื่อนไขการทดสอบในหลายพื้นที่ทางภูมิศาสตร์ ฯลฯ

เมื่อใช้ AWS ทำให้มีคุณสมบัติการตรวจสอบหลายอย่างที่จะช่วยตรวจสอบและจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศได้ง่ายและมีประสิทธิภาพ โปรดดูคุณสมบัติเหล่านั้น คำแนะนำเกี่ยวกับ 'วิธีการ' ที่เกี่ยวข้อง และลิงก์ต่างๆ เพื่อเรียนรู้เพิ่มเติมเกี่ยวกับคุณสมบัติที่ด้านล่าง:

คุณสมบัติที่สนับสนุนการกำกับดูแลของ AWS	การได้รับความปลอดภัยตามขนาดที่เหมาะสม
Amazon CloudWatch	เสนอข้อมูลทางสถิติที่คุณสามารถดู วิเคราะห์ กำหนดการแจ้งเตือนเกี่ยวกับลักษณะการทำงานของอินแสตนซ์ ตัววัดผลเหล่านี้ ได้แก่ การใช้ CPU, ปริมาณการใช้งานเครือข่าย, I/O และเวลาแฝง เรียนรู้เพิ่มเติม
การแจ้งเตือนของ Amazon CloudWatch	เสนอการแจ้งเตือนอย่างสม่ำเสมอสำหรับเหตุการณ์สำคัญโดยการกำหนดตัววัดผลแบบกำหนดเอง การแจ้งเตือน และการแจ้งข้อมูลเหตุการณ์ เรียนรู้เพิ่มเติม
สถานะ Amazon EC2 Instance	เสนอการตรวจสอบสถานะของอินสแตนซ์ที่สรุปผลของการทดสอบแบบอัตโนมัติและให้ข้อมูลเกี่ยวกับกิจกรรมบางอย่างที่ได้รับการจัดกำหนดการสำหรับอินสแตนซ์ ใช้การตรวจสอบแบบอัตโนมัติเพื่อตรวจดูว่าปัญหาเฉพาะนั้นๆ มีผลกระทบกับอินสแตนซ์หรือไม่ เรียนรู้เพิ่มเติม
ทีมการจัดการกับการเกิดเหตุของ Amazon	เสนอการตรวจหาการเกิดเหตุอย่างต่อเนื่อง การตรวจสอบและการจัดการที่มีพนักงานปฏิบัติงานตลอด 24 ชั่วโมงทุกวันเพื่อสนับสนุนการตรวจหา การวิเคราะห์ และการแก้ไขเหตุการณ์ด้านความปลอดภัยบางอย่าง เรียนรู้เพิ่มเติม
การยอมรับทางเลือกของ Amazon S3 TCP	เสนอความสามารถในการปรับปรุงเวลาในการกู้คืนหลังมีการสูญหายของแพคเก็ตจำนวนมาก เรียนรู้เพิ่มเติม
Amazon Simple Notification Service	เสนอการแจ้งเตือนอย่างสม่ำเสมอสำหรับเหตุการณ์สำคัญโดยการจัดการกับการส่งข้อความไปยังปลายทางที่บอกรับการใช้งานหรือไคลเอ็นต์ เรียนรู้เพิ่มเติม
AWS Elastic Beanstalk	เสนอความสามารถในการตรวจสอบรายละเอียดการใช้งานแอปพลิเคชันสำหรับการจัดเตรียมความจุ โหลดบาลานซ์ การปรับขยายอัตโนมัติ และการตรวจสอบสถานะของแอปพลิเคชัน เรียนรู้เพิ่มเติม

Elastic Load Balancing	เสนอความสามารถในการกระจายปริมาณการใช้งานแอปพลิเคชันขาเข้าไปยังหลาย Amazon EC2 Instance โดยอัตโนมัติด้วยการตรวจหา อินสแตนซ์ที่ใช้งานและการกำหนดเส้นทางรับส่งข้อมูลใหม่ไปยังอินสแตนซ์ที่ไม่ได้ใช้ เรียนรู้เพิ่มเติม

สร้างความยืดหยุ่น

การวางแผนสำหรับการป้องกันข้อมูลและการกู้คืนจากความเสียหายควรเป็นส่วนประกอบที่สำคัญที่สุดของการกำกับดูแลด้านเทคโนโลยีสารสนเทศสำหรับทุกองค์กร ถึงจะบอกว่าประโยชน์ของ DR ไม่เป็นที่น่าสงสัย แต่ทุกองค์กรก็กังวลเกี่ยวกับความสามารถในการสำรองข้อมูลและกลับมาทำงานหลังจากการเกิดเหตุการณ์หรือความเสียหาย การใช้การกำกับดูแลเกี่ยวกับความยืดหยุ่นของทรัพยากรด้านเทคโนโลยีสารสนเทศอาจมีราคาสูงและซับซ้อน รวมทั้งยังยุ่งยากและเสียเวลามาก องค์กรต่างๆ จึงต้องเจอกับเหตุการณ์ต่างๆ ซึ่งทำให้เกิดการหยุดทำงานที่ไม่คาดคิดและเป็นอุปสรรคในการดำเนินงานมากขึ้นเรื่อยๆ เหตุการณ์เหล่านี้สามารถเกิดจากปัญหาทางเทคนิค (เช่น ไวรัส การเสียหายของข้อมูล ความผิดพลาดของบุคคล ฯลฯ) หรือภัยทางธรรมชาติ (เช่น ไฟไหม้ น้ำท่วม ไฟฟ้าขัดข้อง ไฟฟ้าดับที่เกี่ยวข้องกับสภาพอากาศ ฯลฯ) ซึ่งทำให้องค์กรต้องรับภาระด้านต้นทุนที่เพิ่มขึ้นและมีความซับซ้อนในการวางแผน การทดสอบ และการดำเนินการสำหรับไซต์ที่มีการป้องกันความผิดพลาดภายในองค์กรเนื่องจากการเติบโตของข้อมูลอย่างต่อเนื่อง

การรับมือกับความท้าทายเหล่านี้ การจำลองเสมือนเซิร์ฟเวอร์ของระบบประมวลผลแบบคลาวด์ทำให้โปรแกรมความยืดหยุ่นที่มีคุณภาพมีความเหมาะสมและคุ้มค่า เมื่อใช้ AWS ทำให้มีคุณสมบัติหลายอย่างที่ให้คุณสามารถสร้างความยืดหยุ่นสำหรับทรัพยากรด้านเทคโนโลยีสารสนเทศได้ง่ายและมีประสิทธิภาพ โปรดดูคุณสมบัติเหล่านั้น คำแนะนำเกี่ยวกับ 'วิธีการ' ที่เกี่ยวข้อง และลิงก์ต่างๆ เพื่อเรียนรู้เพิ่มเติมเกี่ยวกับคุณสมบัติที่ด้านล่าง:

คุณสมบัติที่สนับสนุนการกำกับดูแลของ AWS	การได้รับความปลอดภัยตามขนาดที่เหมาะสม
สแนปช็อตของ Amazon EBS	มีความพร้อมใช้งานสูง ความน่าเชื่อถือสูง ไดรฟ์จัดเก็บข้อมูลที่คาดการณ์ได้ด้วยการควบคุมการสำรองข้อมูลที่มีการเพิ่มจุดเวลาของเซิร์ฟเวอร์ เรียนรู้เพิ่มเติม
การใช้งานแบบหลาย AZ ของ Amazon RDS	มีความสามารถในการป้องกันข้อมูลในกรณีที่เกิดปัญหาด้วยการควบคุมพร้อมใช้งานแบบอัตโนมัติ สถาปัตยกรรมที่มีความยืดหยุ่นแบบเดียวกัน เรียนรู้เพิ่มเติม
AWS Import/Export	เสนอความสามารถในการย้ายข้อมูลจำนวนมากในสถานที่โดยการสร้างการนำเข้าและส่งออกงานอย่างรวดเร็วด้วยเครือข่ายภายในความเร็วสูงของ Amazon เรียนรู้เพิ่มเติม
AWS Storage Gateway	เสนอการผนวกรวมที่ราบรื่นและปลอดภัยระหว่างสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศแบบภายในองค์กรและโครงสร้างพื้นฐานในการจัดเก็บข้อมูลของ AWS โดยการจัดกำหนดเวลาสแนปช็อตที่เกตเวย์จัดเก็บใน Amazon S3 ในรูปแบบสแนปช็อต Amazon EBS เรียนรู้เพิ่มเติม
AWS Trusted Advisor	เสนอการจัดการประสิทธิภาพแบบอัตโนมัติและการควบคุมความพร้อมใช้งานด้วยการระบุทางเลือกในการเพิ่มความพร้อมใช้งานและระบบการสำรองของแอปพลิเคชัน AWS เรียนรู้เพิ่มเติม
โซลูชันของบริษัทอื่นที่ครอบคลุม	เสนอการจัดเก็บข้อมูลที่ปลอดภัยและการควบคุมความพร้อมใช้งานแบบอัตโนมัติด้วยการให้คุณเชื่อมต่อกับตลาดของแอปพลิเคชันเครื่องมือได้ง่ายๆ เรียนรู้เพิ่มเติม
บริการฐานข้อมูล AWS No-SQL/SQL ที่ได้รับการจัดการ	เสนอการจัดเก็บข้อมูลที่ปลอดภัยและคงทนพร้อมกับมีการจำลองข้อมูลโดยอัตโนมัติไปยัง Availability Zone หลายแห่งในภูมิภาคเพื่อให้ความพร้อมใช้งานสูงและความคงทนของข้อมูลไปด้วยในตัว เรียนรู้เพิ่มเติม: • ฐานข้อมูล Amazon Dynamo • Amazon RDS

การใช้งานแบบหลายภูมิภาค	เสนอความหลากหลายทางภูมิศาสตร์ของสถานที่ตั้งคอมพิวเตอร์ การเชื่อมโยงระบบไฟฟ้า สายด่วนแก้ไขปัญหา ฯลฯ เพื่อให้มีสถานที่ตั้งหลากหลาย เรียนรู้เพิ่มเติม
การตรวจสอบสภาพการทำงาน Route 53 และ DNS Failover	ตรวจสอบความพร้อมใช้งานของข้อมูลสำรองที่จัดเก็บด้วยการให้คุณกำหนดค่า DNS Failover เป็นแบบ active-active, active-passive และการกำหนดค่าแบบผสมเพื่อปรับปรุงความพร้อมใช้งานของแอปพลิเคชันได้ เรียนรู้เพิ่มเติม

ดัชนีของคุณสมบัติที่สนับสนุนการกำกับดูแลบริการ

ข้อมูลข้างต้นมีการนำเสนอตามหลักการกำกับดูแล เพื่อการอ้างอิงของคุณ สรุปข้อมูลเกี่ยวกับคุณสมบัติการกำกับดูแลโดยบริการส่วนใหญ่ของ AWS มีการอธิบายไว้ในตารางด้านล่าง:

บริการ AWS	**คุณสมบัติการกำกับดูแล**
Amazon EC2	การเปิดใช้อินสแตนซ์การตรวจสอบความถูกตามจริงของ Amazon EC2 การติดแท็กทรัพยากรของ Amazon EC2 Amazon Linux AMIs Amazon EC2 Dedicated Instances วิซาร์ดการเปิดใช้งาน Amazon EC2 Instance กลุ่มความปลอดภัยของ Amazon EC2
Elastic Load Balancing	การกระจายปริมาณการใช้งานของ Elastic Load Balancing
Amazon VPC	Amazon VPC การแยกทางลอจิคัลของ Amazon VPC ACL เครือข่าย Amazon VPC ที่อยู่ IP ส่วนตัวของ Amazon VPC กลุ่มความปลอดภัยของ Amazon VPC การเชื่อมต่อ VPN สำหรับฮาร์ดแวร์/ซอฟต์แวร์ภายในองค์กร
Amazon Route 53	ชุดเรกคอร์ดทรัพยากรที่มีเวลาแฝงของ Amazon Route 53 การตรวจสอบสภาพการทำงานของ Route 53 และ DNS Failover
AWS Direct Connect	AWS Direct Connect
Amazon S3	รายการควบคุมการเข้าถึง Amazon S3 (ACL) นโยบายบัคเก็ต Amazon S3 Amazon S3 Query String Authentication Amazon S3 Client-Side Encryption Amazon S3 Server-Side Encryption Amazon S3 Object Expiration

	ล็อกการเข้าถึงเซิร์ฟเวอร์ Amazon S3 การยอมรับทางเลือกของ Amazon S3 TCP การปรับขยายกรอบเวลาของ Amazon S3 TCP
Amazon Glacier	คลังชุดเก็บข้อมูลประจำตัวของ Amazon Glacier ที่เก็บถาวรของ Amazon Glacier
Amazon EBS	สแนปช็อตของ Amazon EBS
AWS Import/Export	AWS Import/Export bulk datano…
AWS Storage Gateway	การผนวกรวม AWS Storage Gateway AWS Storage Gateway APIs
Amazon CloudFront	Amazon CloudFront ล็อกการเข้าถึงของ Amazon CloudFront
Amazon RDS	ล็อกของฐานข้อมูล Amazon RDS การใช้งานแบบหลาย AZ ของ Amazon RDS บริการฐานข้อมูล AWS No-SQL/SQL ที่ได้รับการจัดการ
ฐานข้อมูล Amazon Dynamo	บริการฐานข้อมูล AWS No-SQL/SQL ที่ได้รับการจัดการ
AWS Management Console	เพจ Account Activity AWS Account Billing การกำหนดราคาบริการ AWS การเรียกเก็บเงิน AWS Trusted Advisor Billing Alarms การเรียกเก็บเงินรวม การกำหนดราคาค่าบริการที่ใช้ตามจริง AWS CloudTrail Amazon Incident Management Team Amazon Simple Notification Service การใช้งานแบบหลายภูมิภาค
AWS Identity and Access Management (IAM)	AWS IAM Multi-Factor Authentication (MFA) นโยบายรหัสผ่าน AWS IAM สิทธิ์ของ AWS IAM นโยบายของ AWS IAM บทบาทของ AWS IAM
Amazon CloudWatch	AWS CloudWatch Dashboard การแจ้งเตือนของ Amazon CloudWatch
AWS Elastic Beanstalk	การตรวจสอบ AWS Elastic Beanstalk

AWS CloudFormation	เทมเพลต AWS CloudFormation
AWS Data Pipeline	AWS Data Pipeline Task Runner
AWS CloudHSM	การจัดเก็บข้อมูลคีย์ CloudHSM
AWS Marketplace	โซลูชันของบริษัทอื่นที่ครอบคลุม
ศูนย์ข้อมูล	การควบคุมการเข้าถึงทางกายภาพของ AWS SOC 1 การควบคุมการเข้าถึงทางกายภาพของ AWS SOC 2-Security การควบคุมการเข้าถึงทางกายภาพของ AWS PCI DSS การควบคุมการเข้าถึงทางกายภาพของ AWS ISO 27001 การควบคุมการเข้าถึงทางกายภาพของ AWS FedRAMP

บทสรุป

ความสำคัญหลักของการกำกับดูแลด้านเทคโนโลยีสารสนเทศ คือ การจัดการทรัพยากร ความปลอดภัย และประสิทธิภาพเพื่อมอบคุณค่าเชิงกลยุทธ์ที่สอดคล้องกับเป้าหมายของธุรกิจ เมื่อพิจารณาจากการเติบโตของอัตราและความซับซ้อนที่เพิ่มขึ้นของเทคโนโลยี มีความท้าทายเพิ่มขึ้นเรื่อยๆ สำหรับสภาพแวดล้อมแบบภายในองค์กรที่จะปรับขยายเพื่อให้มีการควบคุมแบบละเอียด และคุณสมบัติที่จำเป็นในการมอบการกำกับดูแลด้านเทคโนโลยีสารสนเทศที่มีคุณภาพและคุ้มค่า การกำกับดูแลในระบบคลาวด์มีค่าใช้จ่ายในการเริ่มใช้งานต่ำกว่า สามารถทำงานได้ง่ายกว่า และมีความคล่องตัวมากขึ้นด้วยการใช้ระบบอัตโนมัติที่มีการเฝ้าติดตาม การควบคุมความปลอดภัย และทำงานจากส่วนกลางมากขึ้น ซึ่งเป็นเหตุผลเดียวกับที่การให้บริการโครงสร้างพื้นฐานในระบบคลาวด์มีข้อดีมากกว่าการให้บริการแบบภายในองค์กร

ข้อมูลอ้างอิงและแหล่งข้อมูลเพิ่มเติม

ฉันสามารถทำอะไรได้บ้างด้วย AWS http://aws.amazon.com/solutions/aws-solutions/

ฉันจะเริ่มต้นใช้งาน AWS ได้อย่างไร http://docs.aws.amazon.com/gettingstarted/latest/awsgsg-intro/gsg-aws-intro.html