

ศูนย์ข้อมูลกับทิศทาง ที่กำลังไปในอนาคต

แนวโน้มล่าสุดที่จะพลิกโฉมหน้าระบบเครือข่ายในศูนย์ข้อมูลไป... ตลอดกาล!

ปัจจุบัน

บริษัทต่างๆ พัฒนาเป้าหมายทางธุรกิจขึ้น เพื่อควบคุมค่าใช้จ่าย และเพิ่มพูนความคล่องตัวในการดำเนินธุรกิจ ซึ่งเทคโนโลยีขั้นสูงที่ใช้ในศูนย์ข้อมูลสามารถเป็นหนทางใหม่ที่น่าสนใจไปสูเป้าหมายตามที่ตั้งใจไว้ได้ ในบทความนี้ จึงขอกล่าวถึงแนวโน้มล่าสุดของเครือข่ายในศูนย์ข้อมูลที่จะส่งผลกระทบต่อชีวิตพวกเรา ตลอดจนการเปลี่ยนแปลงทางสถาปัตยกรรมของระบบเครือข่ายที่จะมีอิทธิพลต่อศูนย์ข้อมูลในอนาคตอย่างไรที่คุณคาดไม่ถึง

แนวโน้มล่าสุด

ความจำเป็นในการควบคุมค่าใช้จ่ายเวลาดำเนินธุรกิจนั้น ได้ส่งผลให้เกิดการควบรวมระบบเป็นหนึ่งเดียว (Consolidation) ของเทคโนโลยีหลายด้านๆ เช่น เซิร์ฟเวอร์ แอปพลิเคชัน ระบบจัดเก็บข้อมูล หรือแม้กระทั่งศูนย์ข้อมูล ขณะที่แนวโน้มในด้านอื่นๆ ถือกำเนิดจากความสำเร็จในการพัฒนาระบบให้มีความไม่สะดุดหยุดนิ่ง (Resiliency) ซึ่งสื่อได้ถึงการรักษาความปลอดภัยแอปพลิเคชันและข้อมูล, ความต่อเนื่องในการทำธุรกิจ และการรวมกลุ่มเซิร์ฟเวอร์ภายใต้สภาพแวดล้อมที่กระจาย

ยกตัวอย่างเช่น การควบรวมกิจการระหว่างสองบริษัท นอกจากช่วยเร่งอัตราเติบโตในธุรกิจที่ไม่เคยย่างเข้าไปแล้ว ยังเท่ากับบังคับให้ต้องควบรวมสองระบบเครือข่ายเข้าด้วยกัน โดยที่รักษาประสิทธิภาพของการเข้าถึงทรัพยากร การทำเราติง และระบบความปลอดภัยอันสูงส่งเอาไว้ ซึ่งเทคโนโลยีการสร้างวงเครือข่ายเสมือนจริง ตลอดจนการแบ่งระบบเครือข่ายเป็นเซ็กเมนต์ย่อยๆ สามารถทำให้การควบรวมกิจการเหล่านั้นง่ายขึ้น ส่วนแนวโน้มบางประการก็เป็นผลสืบเนื่องจากภาวะเติบโตและขยายตัวของบริษัท ซึ่งต้องมีการวางแผนด้านความสามารถในการทำงาน (Capacity) เสียใหม่เพื่อรับมือกับปัจจัยแวดล้อมที่เปลี่ยนไป เช่น ระบบไฟฟ้า ระบบทำความเย็น ระบบสายเคเบิล หรือระบบไหลเวียนอากาศ เป็นต้น



การควบรวมศูนย์ข้อมูล

การควบรวมศูนย์ข้อมูล (Data Center Consolidation) บ่งบอกเป็นนัยถึงเซิร์ฟเวอร์ฟาร์มที่เคยกระจายลดจำนวนลง และถูกย้ายไปในสถานที่ที่มีระบบจัดการดีขึ้น ศูนย์ข้อมูลเหล่านี้จะได้รับการเชื่อมต่อเข้าหากัน อีกทั้งการปฏิบัติงาน การสนับสนุนทางเทคนิค ตลอดจนแนวทางการออกแบบจะถูกทำให้เป็นมาตรฐาน ซึ่งวัตถุประสงค์ของการควบรวมคือ ลดจำนวนสถานที่ปฏิบัติงาน การรวมศูนย์กลางเซิร์ฟเวอร์และแอปพลิเคชัน (ดูภาพที่ 1) และการที่ผู้ดูแลระบบสามารถใช้ทักษะความชำนาญเดิมได้ทันที ศูนย์ข้อมูลรูปแบบใหม่จะมีเซิร์ฟเวอร์และแอปพลิเคชันอัดแน่นมากขึ้น ทำให้ต้องอาศัยความจุพอร์ตที่มากขึ้น การใช้บริการบนระบบเครือข่ายมากขึ้น และสภาพพร้อมให้บริการที่ดีขึ้น เพื่อรองรับปริมาณเรียกใช้งานที่เพิ่มขึ้น

การควบรวมเซิร์ฟเวอร์

การควบรวมเซิร์ฟเวอร์ (Server Consolidation) บ่งบอกถึงการลดจำนวนลงของแพลตฟอร์มเครื่องเซิร์ฟเวอร์และระบบปฏิบัติการ พร้อมการสร้างมาตรฐานในสภาพแวดล้อมของแอปพลิเคชัน (ระดับชั้นเว็บ และมิดเดิลแวร์) โดยการลดจำนวนลงของแพลตฟอร์มเครื่องเซิร์ฟเวอร์นั้น

ช่วยให้การฟื้นคืนสภาพจากภาวะล้มเหลวใช้เวลาน้อยลง บรรเทาปัญหาขาดอะไหล่ในยามฉุกเฉิน และลดความต้องการเจ้าหน้าที่ผู้เชี่ยวชาญรวมถึงความยุ่งยากในบำรุงรักษา ขณะที่การสร้างมาตรฐานของเซิร์ฟเวอร์จะประกอบด้วยเทคโนโลยีของบัส/การ์ดเครือข่าย (เช่น การตัดสินใจเลือกกระหว่าง PCI, PCI-X หรือ PCI-Express และการตัดสินใจว่าจะใช้การ์ดอะไรระหว่าง 10/100, 10/100/1000, หรือ 10 กิกะบิตต่อวินาที) และการปรับปรุงค่า Oversubscription Rate ระหว่างเซิร์ฟเวอร์กับ Access Layer, ระหว่าง Access Layer กับ Aggregation Layer, และสุดท้ายระหว่าง Aggregation Layer กับ Core Layer ซึ่งค่านี้จะเปลี่ยนแปลงไปในทางที่ดีขึ้นมาก หากคุณใช้บัส PCI-Express และการ์ดกิกะบิตต่อวินาที เนื่องจากอัตรา Burst Rate เฉลี่ยที่เพิ่มขึ้นนั่นเอง

การควบรวมเบลด์เซิร์ฟเวอร์

เบลด์เซิร์ฟเวอร์ (Blade Server) เป็นเทคโนโลยีที่ช่วยให้เครื่องรับอุปกรณ์คอมพิวเตอร์ หน่วยความจำ และ I/O แออัดได้มากขึ้น พร้อมกับ กับลดจำนวนสายเคเบิลที่ต้องลากลง (ระบบเครือข่ายและเคียบอร์ด, ระบบวิดีโอ, เม้าส์ - KVM) ซึ่งการควบรวมเบลด์เซิร์ฟเวอร์นี้ เมื่อมองในแง่

ระบบเครือข่ายก็จะประกอบด้วยทางเลือกเทคโนโลยีของ I/O และโครงสร้างระบบเครือข่ายที่ใช้ว่าเป็นแบบ Pass-through หรือ Integrated Network Fabric หากเป็น Pass-through โมดูลเซิร์ฟเวอร์ต่างๆ จะถูกต่อเชื่อมเข้าระบบเครือข่ายโดยตรง ขณะที่แบบ Integrated จะมีสวิตช์สำรองชุดหนึ่งบรรจุในเคสที่โมดูลเซิร์ฟเวอร์เชื่อมต่ออยู่

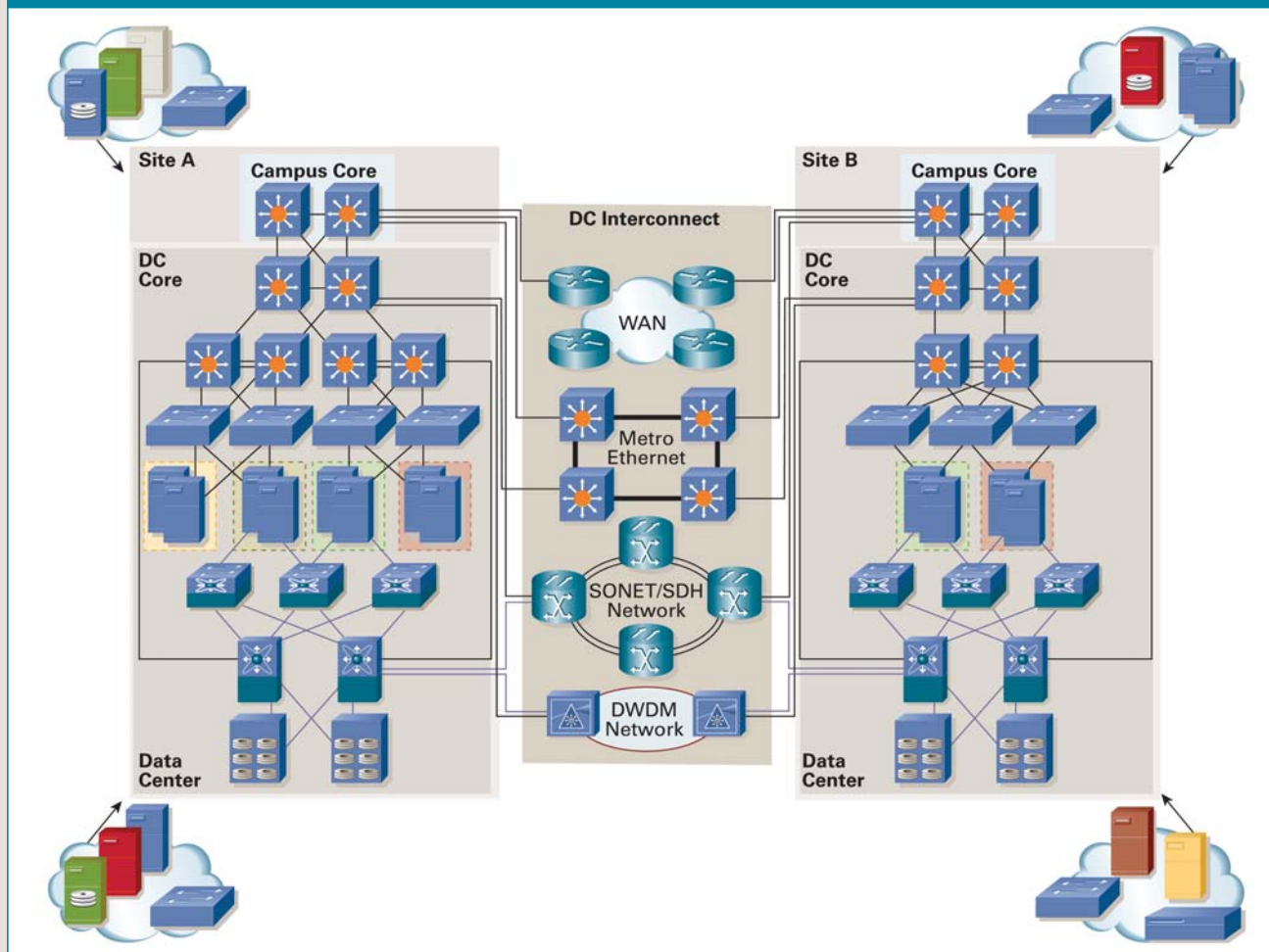
ในสภาพแวดล้อมแบบ Pass-through โมดูลเซิร์ฟเวอร์ต้องการสายเคเบิลเครือข่ายเชื่อมต่อจากข้างนอก แต่ถ้าเป็น Integrated Network Fabric เซิร์ฟเวอร์แต่ละโมดูลจะได้รับการเดินสายไว้ล่วงหน้าไปยังสล็อตซึ่งเป็นที่อยู่ของสวิตช์ภายใน และสวิตช์เหล่านี้ก็จะมีหลายๆ อพลิงก์สำหรับเชื่อมโยงกับโครงสร้างระบบเครือข่ายพื้นฐานของคุณย์ข้อมูลอีกด้วย

การควบรวมระบบจัดเก็บข้อมูล

การควบรวมระบบจัดเก็บข้อมูล (Storage Consolidation) เป็นวิธีที่ช่วยลดความยุ่งยากในการบริหารพื้นที่เก็บข้อมูล โดยกรรมวิธีรวมศูนย์ และปรับปรุงการใช้สอยพื้นที่เก็บข้อมูลให้คุ้มค่ายิ่งขึ้น โดยเปลี่ยนจากเทคโนโลยี Direct Attached Storage Disks (DASD) ไปใช้ระบบจัดเก็บข้อมูล

ภาพที่ 1: การควบรวมทรัพยากรต่างๆ ของศูนย์ข้อมูลส่งพลังเซิร์ฟเวอร์ผ่านที่คอยจัดการกระจายลดจำนวนลง และถูกย้ายไปในสถานที่ที่ระบบจัดเก็บข้อมูล

RESOURCE CONSOLIDATION IN THE DATA CENTER



มัลแวร์ หรืออีกนัยหนึ่งคือ Storage Area Network (SAN) ซึ่งขณะนี้สามารถรองรับพอร์ตไฟเบอร์แซนแนลที่มีความสูงๆ ได้ และการแบ่ง SAN ออกเป็นส่วนย่อย (ผ่าน Virtual SAN) ยังช่วยให้คุณควบคุมระบบจัดเก็บข้อมูลที่กระจัดกระจายเป็นหมู่เกาะเข้าด้วยกันได้มากขึ้น พร้อมลดความแตกต่างในเชิงสถาปัตยกรรมของระบบจัดเก็บข้อมูลได้อย่างมีประสิทธิภาพ

ทั้งนี้ สิ่งที่ต้องทำในเชิงระบบเครือข่ายเวลาควบคุมระบบจัดเก็บข้อมูล ได้แก่ การเพิ่มความหนาแน่นของพอร์ตไฟเบอร์แซนแนลที่ Edge Layer และ Core Layer สำหรับการเชื่อมต่อเซิร์ฟเวอร์ และระบบจัดเก็บข้อมูลอาร์เรย์กับระบบเทปตามลำดับ นอกจากนี้ ควรพิจารณาเพิ่มอุปกรณ์สำรองด้วยเพื่อรองรับปริมาณผู้ใช้งานที่สูงขึ้น

การควบคุมแอปพลิเคชันแบบมัลติเทียร์

การควบคุมแอปพลิเคชันแบบมัลติเทียร์ (Multi-tier Application Integration) จะประกอบด้วยขั้นตอนการย้ายไปสู่แอปพลิเคชันแบบเว็บ โดยที่ฟังก์ชันด้านการนำเสนอ (เว็บ) แอปพลิเคชัน (มิดเดิลแวร์) และฐานข้อมูลจะแยกกันอยู่บนคนละเซิร์ฟเวอร์ นอกจากนี้ การควบคุมแอปพลิเคชันก็ยังรวมถึงการใช้เว็บเซอวิส การสร้างมาตรฐานให้สภาพแวดล้อมมิดเดิลแวร์ และการสนับสนุนด้าน Service Oriented Architecture (SOA) ขณะที่บริการต่างๆ บนระบบเครือข่ายจะเป็นช่องทางที่นำไปสู่การขยายขนาดโครงสร้างระบบเครือข่ายพื้นฐาน การรักษาความปลอดภัย และจัดการข้อมูลที่มีประสิทธิภาพขึ้น รวมไปถึงก่อให้เกิดความสามารถในการแคชคอนเทนต์ที่เป็นแบบไม่เปลี่ยนแปลง และเปลี่ยนแปลงได้ด้วย

การรักษาความปลอดภัยข้อมูลและแอปพลิเคชัน

ความปลอดภัยข้อมูลและแอปพลิเคชันนับเป็นอีกองค์ประกอบหนึ่งที่ต้องได้รับการควบคุมในศูนย์ข้อมูลเช่นเดียวกับองค์ประกอบที่เหลือในระบบเครือข่ายองค์กร การรักษาความปลอดภัยในศูนย์ข้อมูลนี้จะตอบโจทย์ในเรื่องของการปกป้องข้อมูลจากการแก้ไขโดยมิได้รับอนุญาต การปกป้องความลับของข้อมูล และการเข้าถึงข้อมูลที่เก็บไว้ในเซิร์ฟเวอร์ฟาร์มอย่างปลอดภัย ซึ่งสามารถบรรลุผลวัตถุประสงค์ได้ ด้วยการหาวิธีบรรเทาผลกระทบที่เกิดจากการโจมตีเซิร์ฟเวอร์ แอปพลิเคชัน ระบบจัดเก็บข้อมูล และโครงสร้างระบบเครือข่ายหลักที่รองรับ

การรักษาความปลอดภัยเซิร์ฟเวอร์และแอปพลิเคชัน

ประกอบด้วยกระบวนการแบ่งเซ็กเมนต์เซิร์ฟเวอร์ฟาร์มในชั้นของแอปพลิเคชัน การป้องกันตัวจากการโจมตีแบบ Denial-of-Service (DoS) และแบบ Distributed Denial-of-Service (DDoS) และการป้องกันไวรัสไม่ให้เข้า

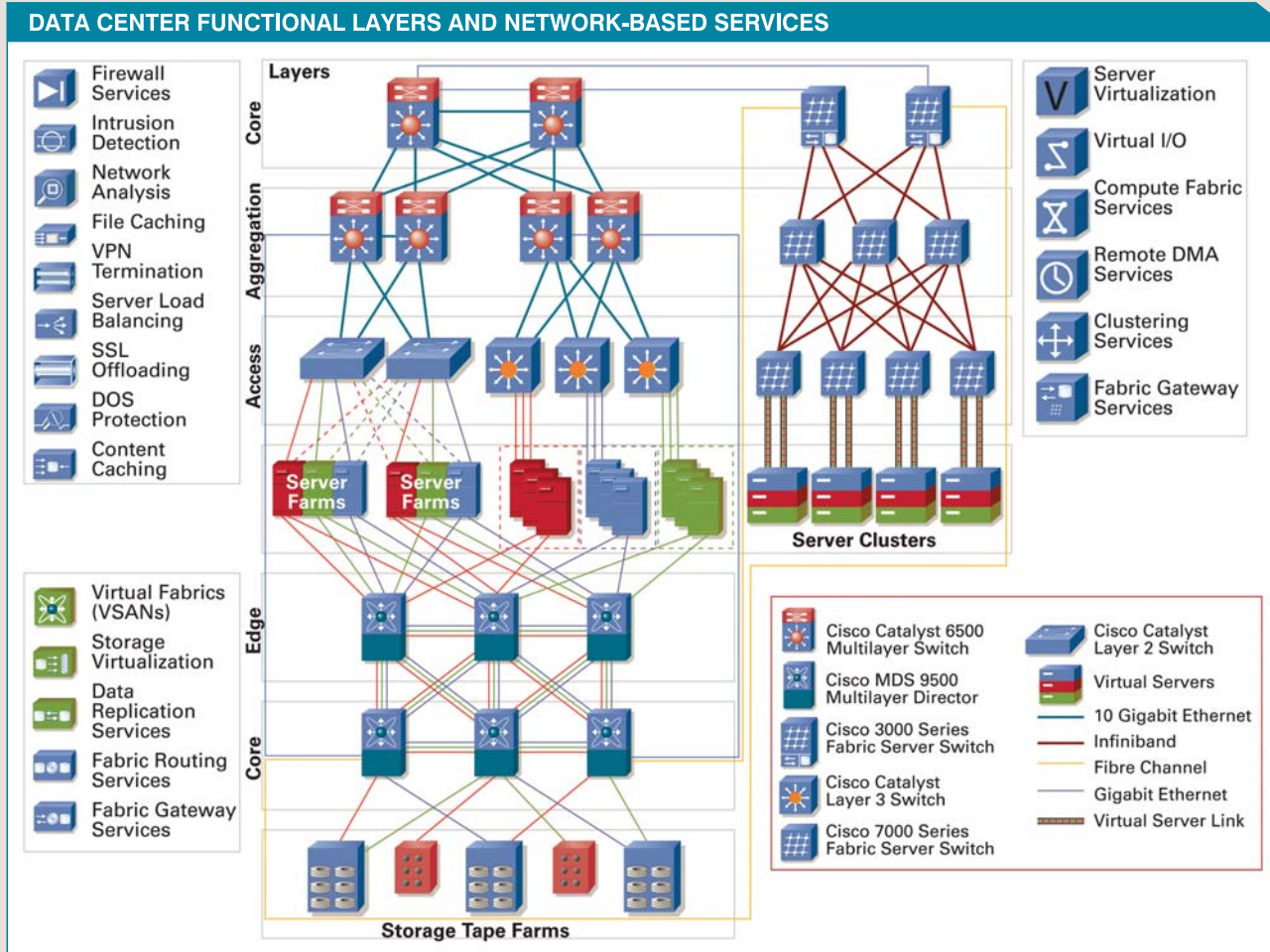
กล้ำกราย ในการบรรลุวัตถุประสงค์ข้างต้นนี้ บริการบนระบบเครือข่ายจะใช้เอเจนต์ที่รันบนเซิร์ฟเวอร์ปกป้องสภาพการทำงานของแอปพลิเคชัน ตลอดจนอุปกรณ์ต่างๆ ที่คอยเฝ้าติดตาม และวิเคราะห์กราฟฟิค เช่น อุปกรณ์ตรวจจับการบุกรุก (IDS) อุปกรณ์ป้องกัน DoS หรือไฟร์วอลล์ เป็นต้น

การรักษาความปลอดภัยโครงสร้างระบบเครือข่ายพื้นฐาน การรักษาความปลอดภัยโครงสร้างระบบเครือข่ายพื้นฐานเกี่ยวข้องโดยตรงกับการปกป้องอุปกรณ์เครือข่าย และลิงก์ต่างๆ ที่คอยขนส่งกราฟฟิคเข้าออกเซิร์ฟเวอร์ฟาร์ม ซึ่งการปกป้องอุปกรณ์เครือข่ายนั้นจะอาศัยกลไกรักษาความปลอดภัยพื้นฐานที่ใช้กันปกติ เช่น กระบวนการพิสูจน์ยืนยันที่เรเตอร์ ระบบจำกัดอัตราไหลข้อมูลที่ป้องกันภาวะข้อมูลท่วมที่คอนโทรลเพลน หรืออุปกรณ์ป้องกันการโจมตี DoS/DDoS ที่คอยกรองกราฟฟิคอันไม่พึงประสงค์ออกไป และสำหรับโครงสร้างระบบเครือข่ายพื้นฐานก็จะได้รับการเสริมแกร่งด้วยคุณสมบัติด้านอื่นๆ ได้แก่ Control Plane Policing ระบบจำกัดอัตราไหลข้อมูลชนิดพิเศษ กระบวนการพิสูจน์ยืนยันที่เรเตอร์ และการป้องกันที่พอร์ต นอกเหนือจากคุณสมบัติอื่นๆ ที่ช่วยปกป้องระบบปลายทางอย่าง Private VLAN

เวอร์ชวลไลเซชัน

เทคโนโลยีเวอร์ชวลไลเซชัน (Virtualization) คำนี้นครอบคลุมถึงความสามารถในการที่ประยุกต์ใช้กับเซิร์ฟเวอร์และแอปพลิเคชัน ประยุกต์ใช้กับบริการบนเครือข่าย เช่น ไฟร์วอลล์ หรือตัวกระจายสมดุลโหลด และประยุกต์ใช้กับอุปกรณ์ย่อยบนโครงสร้างระบบเครือข่ายพื้นฐานอย่างไฟร์วอลล์ หรือสวิตช์ ซึ่งการทำเวอร์ชวลไลซ์ที่เซิร์ฟเวอร์และแอปพลิเคชัน เกี่ยวข้องกับการใช้ Logical Instance ของทรัพยากรเหล่านี้ ในวิถีทางที่ค่อนข้างเป็นอิสระจากแพลตฟอร์มฮาร์ดแวร์ที่ทำงานด้วย โดยแอปพลิเคชันเซอวิส (ตัวระบบปฏิบัติการและซอฟต์แวร์แอปพลิเคชัน) จะได้รับการมองว่าเป็น Logical Instance ในเซิร์ฟเวอร์ที่สามารถย้ายไปทำงานที่เซิร์ฟเวอร์ตัวไหนก็ได้ทุกเมื่อที่ต้องการ คุณสมบัติข้อนี้จำเป็นต้องอาศัยอิมเมจของแอปพลิเคชันเซอวิสที่มีอยู่ก่อนแล้วในเซิร์ฟเวอร์ รวมถึงการแบ่งแยกจากกันระหว่างฟังก์ชันต่างๆ ของ I/O กับแพลตฟอร์มเซิร์ฟเวอร์เพื่อให้การบริหาร Logical Instance ทำได้ง่าย

เทคนิคการทำเวอร์ชวลไลซ์เซิร์ฟเวอร์สามารถแบ่งเป็น 2 ประเภทใหญ่ๆ ประเภทแรก คือ การแบ่งเครื่องเซิร์ฟเวอร์เดี่ยวออกเป็นสองเซิร์ฟเวอร์ทางตรรกะ (อีกนัยคือ 2 เวอร์ชวลเซิร์ฟเวอร์) แต่ละเวอร์ชวลเซิร์ฟเวอร์จะทำงานบนระบบปฏิบัติการและสภาพแวดล้อมคนละตัว และประเภทที่สองคือการจับเซิร์ฟเวอร์หลายๆ เครื่อง รวมกลุ่มกันเป็นเซิร์ฟเวอร์ตัวเดียวทางตรรกะที่ทำงานบนระบบปฏิบัติการเพียงหนึ่งตัว ซึ่งความจุที่พื้ของเวอร์ชวลเซิร์ฟเวอร์จะสามารถเพิ่มขึ้นหรือลดลงได้ง่ายๆ ด้วยการใส่เพิ่ม



ภาพที่ 3: โครงข่ายสวิตชิงในศูนย์ข้อมูลจะประกอบด้วยสื่อข้อมูล (เทคโนโลยีอีเทอร์เนต ไฟเบอร์แบบแนหรืออินพีแบนด์) พร้อมบริการต่างๆ สำหรับรองรับกราฟิกระหว่างไคลเอ็นต์กับเซิร์ฟเวอร์ เซิร์ฟเวอร์กับเซิร์ฟเวอร์ เซิร์ฟเวอร์กับระบบจัดเก็บข้อมูล และระบบจัดเก็บข้อมูลกับระบบจัดเก็บข้อมูล

การแบ่งเซ็กเมนต์

การแบ่งเซ็กเมนต์ (Segmentation) เป็นแนวโน้มเทคโนโลยีที่ช่วยในการแบ่งกลุ่มผู้ใช้ (ตลอดจนการเข้าถึงสภาพแวดล้อมแอปพลิเคชันที่ถูกแบ่งเซ็กเมนต์) ออกจากกันทางตรรกะ ซึ่งมีปัจจัยอยู่ 3 ประการที่ควรพิจารณาเวลาออกแบบสภาพแวดล้อมแบบเซ็กเมนต์ ได้แก่ การควบคุมการเข้าถึงของผู้ใช้ เทคโนโลยีขนส่งกราฟิกที่ปลอดภัย และตัวสภาพแวดล้อมแอปพลิเคชันที่ถูกแบ่งเซ็กเมนต์เอง การควบคุมการเข้าถึงของผู้ใช้ (ทั้งภายใน และภายนอกองค์กร) จะได้รับการบังคับใช้ ณ แอ็กเซสพอยนต์ (Access Point) ต่างๆ เป็นด่านแรก ที่ซึ่งผู้ใช้ได้รับการพิสูจน์ยืนยัน และจัดลงในกลุ่มที่ถูกควบคุมโดยนโยบาย เมื่อถึงฝั่งระบบเครือข่ายการขนส่งที่ทำให้ผู้ใช้ต่างๆ ไปถึงสภาพแวดล้อมแอปพลิเคชันได้ จะเป็นเส้นทางที่ถูกแบ่งแยกกันทางตรรกะ (และหมายถึงสภาพแวดล้อมที่แยกจากกันด้วย) ซึ่งให้ความปลอดภัยแก่กราฟิกของไคลเอ็นต์บนโครงสร้างเครือข่ายพื้นฐาน และเมื่อกราฟิกถูกขับไปที่เซิร์ฟเวอร์ฟาร์ม กฎ Access Control จะถูกบังคับใช้ที่จุดเริ่มเข้าสู่ศูนย์ข้อมูลทันที

เทคโนโลยีการแบ่งเซ็กเมนต์จึงมีประโยชน์ต่อการควบคุมกิจการ ซึ่งทั้งสองบริษัทต้องเชื่อมโยงระบบเครือข่ายเข้าหา

กัน ใช้งานพื้นที่ศูนย์ข้อมูลร่วมกัน และขนถ่ายกราฟิกไปมาระหว่างไคลเอ็นต์กับแอปพลิเคชัน เครือข่ายใดก็ตามที่ให้บริการแบ่งเซ็กเมนต์จำเป็นต้องอาศัยเทคโนโลยีหลายๆ อย่าง เพื่อใช้ตลอดทั่วทั้งระบบเครือข่าย โดยเฉพาะบางบริการจะพึ่งความสามารถในด้านเวอร์ชวลไลเซชันด้วย เช่นที่จุดติดต่อต่างๆ กลไกการควบคุมจะประกอบด้วยการพิสูจน์ยืนยันโดย IEEE 802.1X และระบบ Authentication, Authorization, and Accounting (AAA) เพื่อควบคุมการเข้าถึงของผู้ใช้ การจัดผู้ใช้เข้ากลุ่ม และการบังคับใช้นโยบายกลุ่ม

สำหรับการขนส่งกราฟิกของไคลเอ็นต์ก็มีการใช้เทคโนโลยีหลายอย่างเหมือนกัน เช่น โพรโตคอล Generic Routing Encapsulation (GRE), Layer 2 Tunneling Protocol Version (L2TPv3), Multiprotocol Label Switching (MPLS VPN) หรือแม้กระทั่ง VPN Routing/Forwarding Lite (VRF Lite) เพื่อให้การขนส่งที่ปลอดภัยโดยใช้เส้นทางเวอร์ชวลหลายๆ เส้น และที่ศูนย์ข้อมูล การจับคู่เส้นทางขนส่งกับสภาพแวดล้อมแอปพลิเคชันก็จะใช้เวอร์ชวลเราเตอร์ เวอร์ชวลไฟร์วอลล์ และบริการเวอร์ชวลอื่นๆ ประกอบกัน เป็นต้น

สถาปัตยกรรมศูนย์ข้อมูลแบบใหม่

แนวโน้มทั้งหมดที่กล่าวมาข้างต้นได้ก่อให้เกิดความท้าทายในหลายด้านๆ ซึ่งล้วนแล้วต้องอาศัยการพัฒนาสถาปัตยกรรมศูนย์ข้อมูลที่แข็งแกร่ง เพื่อให้การรับเทคโนโลยีใหม่มาใช้เป็นไปอย่างราบรื่น และปัจจัยสำคัญต่อการพัฒนาสถาปัตยกรรมศูนย์ข้อมูลที่ว่านี้ ได้แก่ การเลือกใช้เทคโนโลยีโครงสร้างระบบเครือข่ายพื้นฐานที่เหมาะสมการเลือกบริการที่จะรับบนศูนย์ข้อมูล และการกำหนดวัตถุประสงค์ของสภาพแวดล้อมแบบกระจาย (Distributed) ต่างๆ

โครงสร้างระบบเครือข่ายในศูนย์ข้อมูล

ในศูนย์ข้อมูลประกอบด้วยโครงข่ายสวิตชิงต่างๆ ที่สนับสนุนการทำงานของเซิร์ฟเวอร์ฟาร์มอยู่ (ดูภาพที่ 3) ซึ่งโครงข่ายสวิตชิงถือเป็นฟังก์ชันหลักที่ช่วยให้อุปกรณ์ในศูนย์ข้อมูลแลกเปลี่ยนข้อมูลกันได้อย่างมีประสิทธิภาพมากขึ้น และทราฟฟิกในศูนย์ข้อมูลก็สามารถแบ่งออกเป็นประเภทย่อยๆ ได้แก่ โคลเอ็นต์กับเซิร์ฟเวอร์ เซิร์ฟเวอร์กับเซิร์ฟเวอร์ เซิร์ฟเวอร์กับระบบจัดเก็บข้อมูล และระบบจัดเก็บข้อมูลกับระบบจัดเก็บข้อมูล

เริ่มต้นด้วยทราฟฟิกระหว่างโคลเอ็นต์กับเซิร์ฟเวอร์ จะเกิดขึ้นตอนที่ผู้ใช้ติดต่อกับแอปพลิเคชัน ในขณะที่ทราฟฟิกระหว่างเซิร์ฟเวอร์กับเซิร์ฟเวอร์ก็เป็นผลพวงทางอ้อมจากการติดต่อระหว่างโคลเอ็นต์กับเซิร์ฟเวอร์อีกทอดหนึ่ง (ยกตัวอย่างเช่น แอปพลิเคชันเซิร์ฟเวอร์แลกเปลี่ยนข้อมูลสถานะซึ่งกันและกัน แอปพลิเคชันเซิร์ฟเวอร์แลกเปลี่ยนข้อมูลกับเซิร์ฟเวอร์ฐานข้อมูล หรือเซิร์ฟเวอร์ฐานข้อมูลตัวหนึ่งสืบค้นข้อมูลจากเซิร์ฟเวอร์ฐานข้อมูลอีกตัวหนึ่ง) หรือเกิดจากการที่เซิร์ฟเวอร์ต้องแลกเปลี่ยนข้อมูลของงานใหญ่ชิ้นหนึ่ง ที่ถูกซอยย่อยเป็นงานเล็กๆ หลายๆ ชิ้น ต่อมาทราฟฟิกระหว่างเซิร์ฟเวอร์กับระบบจัดเก็บข้อมูล เกิดขึ้นจากการที่โฮสต์เข้าถึงดิสก์เป้าหมายภายในระบบจัดเก็บข้อมูลอาร์เรย์ หรือเข้าถึงระบบเทป และสำหรับทราฟฟิกระหว่างระบบจัดเก็บข้อมูลกับระบบจัดเก็บข้อมูลนั้น โดยทั่วไปจะเกิดตอนทำซ้ำข้อมูลระหว่างระบบจัดเก็บข้อมูลอาร์เรย์นั่นเอง

สำหรับเทคโนโลยีในการเชื่อมต่อเครือข่ายจะมีทั้งอีเทอร์เน็ต ไฟเบอร์แกนเนล และทางเลือกคลื่นลูกใหม่ก็คือ อินฟินิแบนด์ โดยอีเทอร์เน็ตยังเป็นที่ยอมรับ และได้รับการพัฒนาต่อเนื่องเพราะให้ประสิทธิภาพที่สูงในราคาต่ำ อีกทั้งผ่านการพิสูจน์แล้วว่าใช้งานได้ดี สำหรับแอปพลิเคชันที่ติดต่อกันระหว่างโคลเอ็นต์กับเซิร์ฟเวอร์ ส่วนไฟเบอร์แกนเนลนั้นจะเป็นเทคโนโลยีที่ใช้ใน SAN ต่อไป เนื่องจากมีคุณสมบัติที่จำเป็นสำหรับการติดต่อกันระหว่างเซิร์ฟเวอร์กับระบบจัดเก็บข้อมูล และระบบจัดเก็บข้อมูลกับระบบจัดเก็บข้อมูล

ในส่วนของอินฟินิแบนด์เป็นเทคโนโลยีที่เกิดขึ้นได้ เนื่องจากให้ทรูพัตที่สูงมาก ความล่าช้าต่ำ ราคาไม่แพง และให้ความสามารถที่จำเป็นในสภาพแวดล้อมเซิร์ฟเวอร์ คลัสเตอร์ นอกจากนี้ โครงสร้างระบบเครือข่ายแต่ละประเภทก็จะใช้เทคโนโลยีที่แตกต่างกัน และให้บริการต่างๆ ที่รองรับทราฟฟิกหลากหลายชนิดด้วย

บริการในศูนย์ข้อมูล

บริการต่างๆ บนโครงสร้างอีเทอร์เน็ตพื้นฐานโดยหลักจะใช้กับทราฟฟิกส่งผ่านระหว่างโคลเอ็นต์กับเซิร์ฟเวอร์ และระหว่างเซิร์ฟเวอร์กับเซิร์ฟเวอร์ ในบางกรณีของแอปพลิเคชันประเภททำธุรกรรม บริการเหล่านี้ครอบคลุมถึงการรักษาความปลอดภัย การอพยพย้ายเซิร์ฟเวอร์ และการจัดการระบบเครือข่าย โดยที่การรักษาความปลอดภัยนั้นประกอบด้วยไฟร์วอลล์ การตรวจจับผู้บุกรุก ระบบรักษาความปลอดภัยไอพี (IPSec) Secure Sockets Layer (SSL) VPN และการบรรเทาความเสียหายจาก DoS และ DDoS ตลอดจนบริการบนเครือข่ายขั้นพื้นฐานอย่าง Broadcast Suppression, ARP inspection และ PVLANS

สำหรับบริการอพยพย้ายเซิร์ฟเวอร์ประกอบด้วย การกระจายสมดุลโหลดเซิร์ฟเวอร์ และ SSL Offload รวมถึงบริการรูปแบบใหม่อีกสองอย่าง ได้แก่ ไฟล์แคชชิง (File Caching) และการจัดการแอสเซจ (Message Manipulation) ไฟล์แคชชิงจะใช้ในกระบวนการรวบรวมเซิร์ฟเวอร์ โดยรวบรวมไฟล์ภายในศูนย์ข้อมูลไว้ที่ศูนย์กลาง พร้อมรักษาระดับประสิทธิภาพการเข้าถึงไฟล์ให้เท่าๆ กับตอนก่อนการรวบรวม ส่วนการจัดการแอสเซจใช้กับการแลกเปลี่ยนข้อมูลระหว่างแอปพลิเคชันที่มีลักษณะแตกต่าง โดยมุ่งให้เกิดการควบคุมแอปพลิเคชันในองค์กรที่เรียบง่ายขึ้น

สุดท้ายในบริการจัดการระบบเครือข่ายในศูนย์ข้อมูลนอกจากการจัดการอุปกรณ์เครือข่ายขั้นพื้นฐานแล้ว แนวโน้มล่าสุดที่ควรจับตามองอย่างยิ่ง ก็คือการนำเสนอเวอร์ชันเซอริวิสต์ต่างๆ ได้แก่ เซิร์ฟเวอร์ แอปพลิเคชัน และระบบเครือข่าย โดยเฉพาะบริการบางตัวยังนำคุณสมบัติด้านการเฝ้าดู (Monitoring) มาใช้สร้างข้อมูลเชิงเปรียบเทียบ เพื่อวิเคราะห์ความปลอดภัย ตลอดจนวางแผนขยายระบบเครือข่าย และอพยพย้ายเซิร์ฟเวอร์ เพื่อให้การใช้งานภายในศูนย์ข้อมูลเกิดประสิทธิภาพสูงเท่าที่ใจต้องการ ■

อ่านเพิ่มเติม

- แฉทางที่คึกคักในการออกแบบศูนย์ข้อมูล cisco.com/go/datacenter
- หนังสือให้ความรู้เรื่องศูนย์ข้อมูลจากสำนักพิมพ์ Cisco Press *Data Center Fundamentals*, by Mauricio Arregoces and Maurizio Portolani (Cisco Press - ISBN: 1587050234)