วันนี้ คุณใส่ใจเครือข่ายอุปกรณ์เก็บข้อมูล ดีพอแล้วหรือยัง?

ปรับแต่งระบบ SAN ของคุณให้มีประสิทธิภาพสูงสุดสำหรับการดำเนินธุรกิจอย่างต่อเนื่อง

ความเปลี่ยนแปลงเป็นสิ่งที่เกิดขึ้นได้เสมอ สำหรับรูปแบบการใช้เครือข่ายอุปกรณ์เก็บข้อมูล (Storage Network) ภายในองค์กรธุรกิจ เหตุผลก็คือเครือข่ายเหล่านี้มีบทบาทสำคัญมากขึ้นในการช่วยให้องค์กรต่างๆ ดำเนินธุรกิจได้อย่างต่อเนื่องไม่สะดุด แม้ในช่วงเวลาที่ระบบล้มเหลวและไซต์หยุดทำงาน จริงอยู่ที่เมื่อก่อนการสำรองข้อมูลในองค์กรจะใช้เซิร์ฟเวอร์ เทปไดรฟ์ และสวิตช์เพียงไม่กี่หน่วย ซึ่งควบคุมและรักษาความปลอดภัยได้ง่ายๆ จากศูนย์ข้อมูลแห่งเดียว แต่ปัจจุบันทั้งภัยธรรมชาติ และสถานการณ์ฉุกเฉินที่เกิดขึ้นบ่อยครั้ง ได้ทำให้องค์กรส่วนมากต้องคิดถึงการออกแบบเครือข่ายอุปกรณ์เก็บข้อมูลใหม่เสียแล้ว

เพื่อปกป้องตัวเองได้ดีขึ้น องค์กรจำนวนมากต่างหันมาสำรองข้อมูลเก็บไว้ในสถานที่ตั้งแต่สองแห่งขึ้นไป และนำโพรโตคอล TCP/IP มาช่วยในการเข้าถึงข้อมูลจากสถานที่เหล่านั้นอย่างรวดเร็ว ซึ่งการใช้เทคโนโลยีอุปกรณ์เก็บข้อมูลบนพื้นฐานของไอพีอย่าง iSCSI (Internet Small Computer System Interface) หรือ FCIP (Fibre Channel over IP) นั้นทำให้ผู้ใช้สามารถเปลี่ยนเส้นทางไปยังเครือข่ายอุปกรณ์เก็บข้อมูลที่อยู่คนละสถานที่โดยอัตโนมัติ ในกรณีที่ไม่สามารถเข้าถึงข้อมูลจากสถานที่แรกได้ วิธีนี้แม้จะมีประโยชน์ในแง่ของสภาพพร้อมใช้งานของข้อมูล แต่ก็นำมาซึ่งข้อพึงกังวลใหม่ๆ เวลาออกแบบเน็ตเวิร์กสำรอง (Backup Network) ด้วยเหมือนกัน

ประเด็นเหล่านี้จะข้องเกี่ยวกับการรักษาสมรรถนะการขนส่งข้อมูลที่ดีพอ ตลอดทั่วเส้นทางเชื่อมต่อระยะไกล เช่นเดียวกับการรักษาความปลอดภัยข้อมูลเหล่านั้นเวลาเดินทาง และการขยายขนาดเครือข่ายพื้นที่เก็บข้อมูลหรือ SAN พูดสั้นๆ คือบรรดาผู้บริหารฝ่ายไอทีเริ่มที่จะเผชิญปัญหาต่างๆ เหมือนกันหมดเกี่ยวกับเครือข่ายอุปกรณ์เก็บข้อมูล เหมือนอย่างที่เจอกับเครือข่ายข้อมูล และเช่นเดียวกับในเครือข่ายข้อมูล ข้อมูลที่เกี่ยวกับอุปกรณ์เก็บข้อมูลมีแนวโน้มที่จะเพิ่มปริมาณขึ้นบนเครือข่าย WAN ซึ่งทำให้เราต้องครุ่นคิดถึงประเด็นเรื่องความล่าช้าตามระยะทาง และช่องโหว่ความปลอดภัยใหม่ๆ อย่างเลี่ยงมิได้

มืออาชีพด้านไอทีจึงควรพิจารณาคำถามต่อไปนี้ เมื่อถึงคราวจำเป็นต้องสร้างเครือข่าย SAN เชื่อมโยงสถานที่ต่างๆ ซึ่งอาจห่างไกลกันนับร้อยนับพันกิโลเมตร:

- มีวิธีใดบ้างที่จะชดเชยความล่าช้าการส่งข้อมูลอันเกิดจากระยะทาง?
- ข้อมูลที่วิ่งออกจากศูนย์ข้อมูลจะปลอดภัยจากการลอบดักข้อมูล หรือแก้ไขข้อมูลกลางทางได้อย่างไร?
- คุณจะมั่นใจกับกระบวนการพิสูจน์ยืนยัน/ให้อนุญาตผู้ใช้ อุปกรณ์ และเจ้าหน้าที่บริหารด้านไอทีได้อย่างไร?
- มีวิธีใดบ้างที่จะแบ่งพาร์ทิชันการเข้าถึงทรัพยากรบน SAN (คล้ายกันมากกับวิธีที่ VLAN ของอีเธอร์เน็ตแบ่งพาร์ทิชันการเข้าถึงเซิร์ฟเวอร์ต่างๆ โดยพิจารณาตามกลุ่มลอจิคัลยูสเซอร์) เพื่อเพิ่มความสามารถในการขยายขนาด การจำกัดวงความเสียหาย และการดูแลรักษาความปลอดภัย?
- องค์กรต่างๆ เขามีวิธีจัดการสภาพแวดล้อมของ SAN ที่เต็มไปด้วยอุปกรณ์ อินเทอร์เฟซ และมาตรฐานจากต่างผู้ผลิตกันอย่างไรบ้าง?

เร่งความเร็วการส่งข้อมูลของ SAN

การเร่งความเร็วในระบบ SAN นั้นมีแนวคิดคล้ายกับๆ กรณีของระบบเครือข่ายข้อมูล โดยแทนที่จะทำพร็อกซีตัวแอพพลิเคชันโพรโตคอล เราก็หันมาทำพร็อกซีที่ระดับตัวโพรโตคอลควบคุมการทำงานของ SAN เพื่อลดจำนวนรอบเดินทางไปกลับของการ Acknowledge และลดเวลาที่ใช้เคลื่อนย้ายบล็อกข้อมูลจากจุด A ไปยังจุด B ยกตัวอย่างเช่น โพรโตคอล SCSI ใช้อาศัยการเดินทางไปกลับของการ Acknowledge ถึงสองเที่ยวสำหรับทุกๆ การเขียนหนึ่งครั้ง เมื่ออุปกรณ์ลอคัลเรียกข้อมูลจาก SAN ที่อยู่ไกลออกไป อุปกรณ์เหล่านั้นก็จะถูกรับรู้จดจำโดยฝั่งลอคัล เพื่อลดความล่าช้าในการส่งข้อมูลผ่าน WAN นั่นเอง

ปัจจุบัน การเร่งความเร็วในระบบ SAN มีใช้กันอยู่ 2 ประเภท ได้แก่ Write Acceleration และ Tape Acceleration ซึ่งการเลือกใช้ประเภทใดขึ้นอยู่กับชนิดของสื่อเก็บข้อมูลที่ต้องการเข้าถึง ทั้งนี้ มัลติโพรโตคอลสวิตช์สำหรับระบบจัดเก็บข้อมูลตระกูล Cisco MDS 9000 จะสนับสนุนการเร่งความเร็วครบทั้งสองประเภท พร้อมทั้งรองรับการเชื่อมต่อผ่าน Fibre Channel, FCIP, iSCSI และ Fibre Connection (FICON) ของเครื่องเมนเฟรม โดยสวิตช์จะส่งข้อมูลระหว่าง Fibre Channel ไปตามพอร์ตต่างๆ และ Encapsulate ข้อมูล Fibre Channel ให้อยู่ในรูปของไอพี แล้วส่งออกไปทางอินเทอร์เฟซของอีเธอร์เน็ตสู่เครือข่ายไอพีข้างนอก

- **Write Acceleration:** การเร่งความเร็วประเภทนี้ จะใช้สำหรับการส่งข้อมูลแบบ Disk-to-Disk และ Host-to-Disk เพื่อลดจำนวนรอบเดินทางไปกลับของการ Acknowledge (กรณีของ SCSI) จากสองเที่ยวลงเหลือแค่เที่ยวเดียว ซึ่งทำให้สมรรถนะการส่งข้อมูลเพิ่มขึ้นจากเดิมเป็นสองเท่า ในกรณีนี้ การแจ้งบอกสถานะการรับข้อมูลที่ครบสมบูรณ์จะได้รับการส่งออกไปหลังเสร็จสิ้นขั้นตอนการ Handshake รอบที่สอง
- **Tape Acceleration:** การเร่งความเร็วประเภทนี้ เป็นรูปแบบที่พัฒนาขึ้นต่อจาก Write Acceleration ที่กล่าวไปแล้วข้างต้น เพื่อเร่งความเร็วการเคลื่อนย้ายข้อมูลอุปกรณ์เก็บข้อมูลจากมีเดียเซิร์ฟเวอร์ไปยังเทปไดรฟ์ ซึ่งสมรรถนะจะเพิ่มขึ้นได้โดยตัวพร็อกซี ที่ช่วยลดจำนวนรอบการทำ Acknowledge ลงจากเดิม

ศัพท์แสงเกี่ยวกับการรักษาความปลอดภัย และบริหารระบบอุปกรณ์จัดเก็บข้อมูล

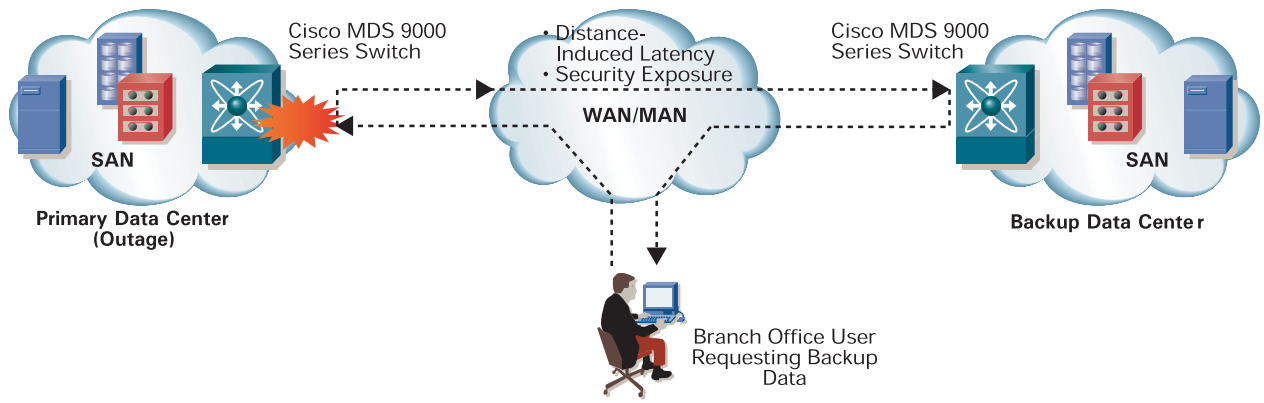
FC-FS-2 Fibre Channel-Framing and Signaling-2: เป็นข้อกำหนดที่บัญญัติโดยคณะกรรมการด้านเทคนิค T11 (T11 Technical Committee) แห่งสมาคมมาตรฐาน INCITS (InterNational Committee for Information Technology Standards) สำหรับการส่งคำสั่ง ข้อมูล และรายละเอียดสถานะต่างๆ ระหว่างอุปกรณ์ SCSI ด้วยกัน

FC-GS-3 Fibre Channel-Generic Services-3: เป็นมาตรฐานการบริหารที่บัญญัติโดยคณะกรรมการด้านเทคนิค T11 แห่ง INCITS สำหรับการส่งข้อมูลเกี่ยวกับสถานะและคอนฟิกูเรชันต่างๆ รวมทั้ง VSAN Information ระหว่างอุปกรณ์ Fibre Channel ด้วยกัน

FC-SP Fibre Channel-Security Protocols: เป็นร่างมาตรฐานที่บัญญัติโดยคณะกรรมการด้านเทคนิค T11 แห่ง INCITS สำหรับรักษาความปลอดภัยข้อมูลอุปกรณ์จัดเก็บข้อมูลของระบบ Fibre Channel ในระหว่างการส่งโดยใช้วิธีเข้ารหัสลับข้อมูล การแลกเปลี่ยนคีย์รหัส และการพิสูจน์ยืนยันตัวตนของอุปกรณ์ ซึ่งได้รับการสนับสนุนจากผู้ผลิต SAN Switch หลายราย รวมถึงผู้ผลิตโฮสต์บัสอะแดปเตอร์ยักษ์ใหญ่ทั้งหมด และมีแผนที่จะได้รับการรับรองเป็นมาตรฐานจริงในเดือนมีนาคม 2549

SMI-S Storage Management Initiative Specification: เป็นมาตรฐานที่พัฒนาขึ้นโดยสมาคม SNIA (Storage Network Industry Association) ซึ่งช่วยให้แอพพลิเคชันบริหารระบบ SAN ของเธิร์ดปาร์ตี้แค่หนึ่งตัวสามารถบริหารกลุ่มอุปกรณ์จัดเก็บข้อมูลของผู้ผลิตมากกว่าหนึ่งรายได้ แทนที่จะต้องใช้แอพพลิเคชันของผู้ผลิตรายนั้นๆ เพียงอย่างเดียว

ความท้าทายในการรักษาความต่อเนื่องทางธุรกิจ



ระยะทางระหว่างสองศูนย์ข้อมูล หรือระหว่างสำนักงานสาขากับวง SAN ที่ห่างไกลมาก ได้ก่อให้เกิดความจำเป็นในการเร่งสมรรถนะของ SAN โดยใช้วิธีพร็อกซี ส่วนกลไกรักษาความปลอดภัยเครือข่ายข้อมูล ยังได้รับการประยุกต์ใช้กับข้อมูล SAN ที่วิ่งไปบน WAN อีกด้วย

ครึ่งหนึ่ง แต่ในระบบเทปมีกลไกการทำเครื่องหมายไฟล์ สำหรับให้คุณตั้งกลไก Acknowledge ให้ทำงานหลังจากที่ส่งข้อมูลไปแล้วตามจำนวนบล็อกที่กำหนดไว้ แทนที่จะทำงานทุกๆ หนึ่งบล็อก เพื่อลดจำนวนรอบของ Acknowledge ให้มากขึ้น โดยสาเหตุที่ต้องใช้ Tape Acceleration ก็เพราะว่าเทปมีความเร็วการเข้าถึงข้อมูลที่ค่อนข้างต่ำมากนั่นเอง

การบีบอัดข้อมูล

เช่นเดียวกับในเครือข่ายข้อมูล เรายังสามารถนำวิธีบีบอัดข้อมูลมาใช้เพิ่มประสิทธิภาพการใช้แบนด์วิดธ์ พร้อมทั้งลดภาวะแออัดของทราฟฟิกในเครือข่ายอุปกรณ์เก็บข้อมูลได้ โดยสวิตช์สำหรับระบบจัดเก็บข้อมูลของซิสโก้นั้นจะสนับสนุนอัลกอริธึมการบีบอัดข้อมูลได้หลายรูปแบบ (แล้วแต่การคอนฟิก) ในอัตราบีบอัดสูงสุดถึง 30:1 ทั้งนี้ อัตราบีบอัดจะมากหรือน้อย ก็ขึ้นอยู่กับความสามารถในการบีบอัดได้ของบล็อกข้อมูล ซึ่งในกรณีทราฟฟิกข้อมูลดาต้าเบส อัตราบีบอัดข้อมูลปกติจะอยู่ที่ 2:1 ถึง 3:1

การรักษาความปลอดภัยข้อมูล

ข้อกังวลในเรื่องความปลอดภัยข้อมูลบนเครือข่าย บัดนี้ได้คืบคลานเข้าสู่โลกของ SAN เรียบร้อยแล้ว ทั้งที่ในอดีต SAN ทั่วไปมีขนาดเล็กบรรจุได้พอดีในหนึ่งศูนย์ข้อมูล แต่อย่างไรก็ตาม เครือข่ายส่งข้อมูลทางไกลในปัจจุบัน ซึ่งถูกส่งผ่านโครงสร้างเครือข่ายข้างนอกของผู้ให้บริการหลายรายๆ นั้นกลับถูกใช้สำหรับเคลื่อนย้ายข้อมูลอุปกรณ์เก็บข้อมูลสำคัญๆ ที่เมื่อก่อนไม่เคยมีโอกาสหลุดรอดออกจากศูนย์ข้อมูลเลย ยกเว้นในรูปสื่อเก็บข้อมูลท้ายรถกระบะเท่านั้น

การปฏิบัติต่อข้อมูลอุปกรณ์เก็บข้อมูลที่เปลี่ยนไปข้างต้นส่งผลให้เกิดความจำเป็นในการประยุกต์ใช้ฟีเจอร์รักษาความปลอดภัยแบบที่พบได้บ่อยๆ ในระบบเครือข่ายไอพีกับโครงข่าย Fibre Channel เช่น การปกป้องข้อมูลระหว่างการขนส่ง หรือการป้องกันผู้ใช้และอุปกรณ์ที่ไม่ได้รับอนุญาตให้เข้าถึงข้อมูล ซึ่งในเครือข่ายที่ประกอบด้วยสวิตช์สำหรับระบบจัดเก็บข้อมูลอย่าง Cisco MDS 9000 (อาจเรียกเครือข่ายประเภทนี้ได้อีกชื่อหนึ่งว่า Storage Fabric) ก็ต้องเพิ่มส่วนของการเข้ารหัสลับข้อมูล และการรักษาความปลอดภัยอินเทอร์เฟซบริหารจัดการ SAN เข้าไปด้วย

- **การเข้ารหัสลับ**: การเข้ารหัสลับข้อมูลจะช่วยป้องกันผู้รุกรานไม่ให้สามารถเรียกดูหรือแก้ไขข้อมูลลับบนเครือข่ายอุปกรณ์เก็บข้อมูลได้ ซึ่งสวิตช์สำหรับระบบจัดเก็บข้อมูลของซิสโก้อาศัยโพรโตคอล IPSec รักษาความลับข้อมูลขณะเดินทาง อย่างกรณี Cisco MDS 9000 จะมาพร้อมกลไกการเข้ารหัส/ถอดรหัสลับ IPSec ด้วยฮาร์ดแวร์ที่สนับสนุนอัลกอริธึม AES (Advanced Encryption Standard), DES (Data Encryption Standard) และ 3DES (Triple Data Encryption Standard) สำหรับทราฟฟิก iSCSI และ FCIP อย่างครบครัน

- **การพิสูจน์ยืนยันตัวตน และให้อนุญาต**: ฟังก์ชันเหล่านี้ กลายเป็นสิ่งที่จำเป็นเสียแล้วสำหรับป้องกันการโจมตีข้อมูลบน SAN รวมถึงการทำอันตรายข้อมูลโดยไม่ตั้งใจ โดยจะอนุญาตเฉพาะผู้ใช้และอุปกรณ์ที่ได้รับการรับรองเท่านั้นที่มีสิทธิ์เชื่อมต่อข้อมูลที่เก็บเอาไว้ ทั้งนี้ การพิสูจน์ยืนยันตัวตนระหว่างสวิตช์กับสวิตช์ และการพิสูจน์ยืนยันของสวิตช์อื่นๆ ที่เชื่อมต่อกับเครือข่ายอุปกรณ์เก็บข้อมูลของซิสโก้ จะอาศัยวิธีแลกเปลี่ยนคีย์เข้ารหัส และใช้คอมโพเน็นต์พิสูจน์ยืนยันอุปกรณ์ตามร่างมาตรฐาน FC-SP (Fibre Channel-Security Protocol) ของคณะกรรมการ INCITS T11 Technical Committee (ดูข้อมูลเพิ่มเติมในกรอบ "ศัพท์แสงเกี่ยวกับการรักษาความปลอดภัย และบริหารระบบอุปกรณ์เก็บข้อมูล") คุณจะสามารถพิสูจน์ยืนยันทั้งตัวผู้ใช้ และอุปกรณ์ได้จากภายในสวิตช์สำหรับระบบจัดเก็บข้อมูล ซึ่งช่วยลดความล่าช้าลง หรือจะพิสูจน์ยืนยันแบบรีโมตผ่านเซิร์ฟเวอร์ AAA (Authentication, Authorization, and Accounting server) ก็ได้

■ **โครงสร้างระบบจัดการที่ปลอดภัย**: ฟังก์ชันบริหารจัดการศูนย์ข้อมูลของเน็ตเวิร์กและอุปกรณ์สตอเรจควรได้รับการป้องกันมิให้ผู้ที่ปราศจากสิทธิ์สามารถเข้าถึง และแก้ไขคอนฟิกูเรชันได้โดยง่าย ซึ่งสวิตช์ Cisco MDS 9000 จะมาพร้อมฟังก์ชันบริหารที่ปลอดภัยมากมาย ได้แก่ SSL (Secure Sockets Layer) และ SSH (Secure Shell) Protocol Version 2 ซึ่งรักษาความปลอดภัยการเข้าถึงระยะไกลโดยใช้วิธีพิสูจน์ยืนยันตัวตนและเข้ารหัสลับ โดยเฉพาะ SSHv2 ยังสามารถทำงานร่วมกับโพรโตคอลพิสูจน์ยืนยันผู้ใช้ฝั่งแบ็กเอนด์อย่าง TACACS+ หรือ RADIUS ที่อาจมีใช้ในองค์กรอยู่แล้วได้ ซึ่งในกรณีนี้ สวิตช์สำหรับระบบจัดเก็บข้อมูลจะประพฤติตนเป็นไคลเอ็นต์ของเซิร์ฟเวอร์ AAA แบ็กเอนด์ที่รันโพรโตคอลต่างๆ ข้างต้น ตบท้ายด้วย SNMPv3 (Simple Network Management Protocol version 3) ที่สนับสนุนการพิสูจน์ยืนยัน และให้อนุญาตเซอร์วิสต่างๆ ในการเข้าถึง SNMP MIB (Management Information Base) ได้เต็มรูปแบบ

จำกัดวงความเสียหายด้วย VSAN

สถาปัตยกรรม VSAN (Virtual SAN) ที่ออกแบบมาอย่างดี จะสามารถช่วยลดจำนวนความต้องการใช้ SAN พร้อมกับทำให้คุณแบ่งแยกโดเมนสำหรับการสำรองข้อมูล กู้คืนข้อมูล และการทำ Mirror ข้อมูลจากระยะไกลออกจากวง SAN ที่เน้นไว้ใช้สำหรับแอพพลิเคชันเป็นหลักได้

เมื่อปีที่แล้ว ทาง INCITS T11 Technical Committee ได้เลือกเทคโนโลยีของซิสโก้ให้เป็นมาตรฐานหลักสำหรับการสร้าง VSAN โดย VSAN ช่วยให้ผู้บริหารเครือข่ายสามารถแยกโครงข่าย SAN ทางกายภาพออกเป็นวง SAN เสมือนจริงหลายวงๆ ที่แยกอิสระจากกันได้ และในทำนองเดียวกับ VLAN ในเครือข่ายข้อมูลแบบอีเธอร์เน็ต วิธีนี้จะมอบความเป็นไปได้ในการสร้างโดเมน SAN ต่างๆ แยกจากกัน โดยไม่จำเป็นต้องลงทุนสร้างโครงข่ายทางกายภาพขึ้นมาใหม่ให้เสียเงินเกินจำเป็น

Cisco MDS 9000 มีคุณสมบัติในการสร้างโทโพโลยี VSAN ในตัวได้มากถึง 256 วง (ซึ่งฮาร์ดแวร์รองรับการเพิ่มจำนวน VSAN ได้สูงสุด 4096 วงบนโครงสร้างเครือข่ายทางกายภาพเดียวกัน) สิ่งนี้ช่วยให้ผู้บริหารระบบใช้การทำโซนนิงธรรมดาจำกัดการเข้าถึงอุปกรณ์ต่างๆ โดยรักษาความปลอดภัยการเข้าถึงที่ตรงขอบเครือข่าย ทั้งนี้ คุณสามารถแบ่งแยกแม้กระทั่งสวิตช์สำหรับระบบจัดเก็บข้อมูลตัวเดียวโดดๆ ออกเป็นเวอร์ชวลเอ็นไวรอนเมนต์หรือเวอร์ชวลโดเมนหลายอันได้ VSAN ยังช่วยจำกัดความเสียหายจากอุปกรณ์เน็ตเวิร์กที่ขัดข้องหรือขาดเสถียรภาพ ไม่ให้ส่งผลกระทบถึงการใช้งานในส่วนอื่นๆที่เหลืออีกด้วย

การบริหารอุปกรณ์จากต่างผู้ผลิต

ตราบที่สภาพแวดล้อมเครือข่ายเติบโตขึ้น องค์กรธุรกิจก็มีแนวโน้มที่จะสร้างโซลูชันระบบจัดเก็บข้อมูลโดยใช้อุปกรณ์จากผู้ผลิตหลายรายมากขึ้น ซึ่งแต่ละรายมาพร้อมโปรแกรมบริหารจัดการ SAN เวอร์ชันของตนเอง จึงจำเป็นที่ผู้บริหารระบบจะต้องหาวิธีบริหารสภาพแวดล้อมเช่นนี้ เพื่อให้ได้ประสิทธิภาพและความคุ้มค่าเงินลงทุนสูงสุด

Cisco Fabric Manager เป็นโปรแกรมที่ทางซิสโก้พัฒนาขึ้น เพื่อช่วยให้ผู้บริหารระบบเรียกดู และบริหารโครงสร้างเครือข่ายเป็นกลุ่มของอุปกรณ์ พร้อมจำลองโทโพโลยีเครือข่ายทั้งหมด และอธิบายในรูปของแผนที่ที่สามารถปรับแต่งข้อมูลได้ ซึ่งอุปกรณ์ใดๆ ก็ตามที่สนับสนุนมาตรฐาน INCITS T11 FC-GS-3 (Fibre Channel-Generic Services-3) สำหรับการบริหารแบบ In-band จะสามารถถูกค้นพบและบรรจุลงแผนที่ของโทโพโลยีได้โดยโปรแกรมนี้ ในส่วนของหน้าต่างโทโพโลยีจะแสดงอุปกรณ์ที่ค้นพบ เพื่อให้คุณปรับแต่งค่าและเข้าไปดูรายละเอียด ขณะที่หน้าต่าง Inventory จะแสดงแผนภูมิต้นไม้ของส่วนประกอบต่างๆ บนเครือข่ายทั้งที่เป็นกายภาพและเสมือนจริง และอีกหน้าต่างที่เหลือจะแสดงเครื่องมือที่ผู้บริหารระบบสามารถใช้ปรับแต่งค่า ติดตามการทำงาน และแก้ปัญหาในอุปกรณ์ได้

นอกจากนี้ Cisco Fabric Manager ยังสนับสนุนมาตรฐานเปิดต่างๆ ที่เปิดโอกาสให้แอพพลิเคชันบริหารจัดการของเธิร์ดปาร์ตี้เข้าถึงข้อมูลเกี่ยวกับสมรรถนะ และคอนฟิกูเรชันภายในตัวสวิตช์ได้ ยกตัวอย่างเช่นมาตรฐาน SMI-S ของสมาคม Storage Networking Industry Association (ดูกรอบ "ศัพท์แสงเกี่ยวกับการรักษาความปลอดภัย และบริหารระบบจัดเก็บข้อมูล") ซึ่งรองรับการบริหารอุปกรณ์โดยใช้โปรแกรมบริหารระบบ SAN จากผู้ผลิตมากกว่าหนึ่งรายได้ เป็นต้น

องค์กรที่พยายามสร้างความต่อเนื่องทางธุรกิจผ่าน SAN ย่อมต้องเผชิญปัญหาเกี่ยวกับสมรรถนะ ความปลอดภัย และการบริหารจัดการแบบที่เคยพบในเครือข่ายข้อมูลมาบ้างไม่มากก็น้อย ด้วยข้อมูลอุปกรณ์จัดเก็บข้อมูลวิ่งไปมาบน WAN ที่เพิ่มปริมาณขึ้นเรื่อยๆ ความล่าช้าอันเนื่องจากระยะทางและช่องโหว่ด้านความปลอดภัยจึงแตกหน่องอกงามขึ้นเรื่อยๆ เช่นกัน เพราะฉะนั้น องค์กรของคุณจึงควรเร่งมองหาเทคนิคเร่งความเร็วการทำงาน รวมถึงโซลูชันรักษาความปลอดภัย และการสนับสนุนอินเทอร์เฟซบริหารจัดการที่อิงตามมาตรฐานอุตสาหกรรมโดยด่วน เพื่อให้ SAN ของคุณทำงานได้คุ้มค่าเงินที่ลงทุนไป และไม่มีปัญหาเกิดขึ้นตามมาในอนาคต ■

อ่านเพิ่มเติม

- แนะนำ Cisco MDS 9000 Family Fabric Management Solutions
  cisco.com/packet/181_6c1
- สมาคม Storage Networking Industry Association
  snia.org/home