**รายงานสรุปผลการพัฒนาระบบความปลอดภัยทางไซเบอร์**

**Privileged Access Management (PAM)**

**1.ข้อมูลทีม**

1. นายศุภชัย นะที (ป๋อง) โรงพยาบาลเทพรัตนเวชชานุกูล เฉลิมพระเกียรติ ๖๐ พรรษา, เขต 1

2. นายนพดล วงค์คำ (เก่ง) สสจ.ลำพูน, เขต 1

3. นายกันต์ชยภัทร ให้พร (ทัพ) โรงพยาบาลสมเด็จพระยุพราชเด่นชัย, เขต 1

4. นายวิทยา ยอดเงิน (โล่) โรงพยาบาลสิงห์บุรี, เขต 4

5. นายจตุรงค์ คำป้อ (เบิ้ม) โรงพยาบาลขุนยวม, เขต 1

6. นายวิริยะ เขตวิทย์ (น้อย) โรงพยาบาลลำปาง, เขต 1

7. นายสกุลชัย ฉิมรักแก้ว (ปั๊ก) โรงพยาบาลขอนแก่น, เขต 7

8. นายชัยวิชิต จันตะมะ (ชัย) โรงพยาบาลเมืองปาน, เขต 1

9. นายเฉลิมพล มโนน้อม (เอ็ม) โรงพยาบาลดอกคำใต้, เขต 1

10. นางวรางคณา เอื้อหยิ่งศักดิ์ (เอ๋) โรงพยาบาลพะเยา, เขต 1

11. นายสินธุ์ คำวะรัตน์ (สิน) โรงพยาบาลแม่ใจ, เขต 1

12. นายบรรจง กิตติสว่างวงค์ (ดอย) โรงพยาบาลน่าน, เขต 1

**2. การวิเคราะห์ปัญหาและความต้องการ**

**2.1 ปัญหาที่พบในปัจจุบัน**

การให้สิทธิ์บริษัทหรือหน่วยงานภายนอกเข้าถึงระบบของโรงพยาบาลจากระยะไกล (Remote Access) อาจก่อให้เกิดปัญหาหลายประการ ดังนี้:

1. ความเสี่ยงด้านความปลอดภัยของข้อมูล

การรั่วไหลของข้อมูลผู้ป่วย: การเข้าถึงระบบจากภายนอกอาจเพิ่มความเสี่ยงในการรั่วไหลของข้อมูลสุขภาพส่วนบุคคล (PHI) ซึ่งเป็นข้อมูลที่ต้องการการป้องกันอย่างเข้มงวด

การโจมตีทางไซเบอร์: การเปิดช่องทางการเข้าถึงจากภายนอกอาจเป็นเป้าหมายของการโจมตี เช่น มัลแวร์หรือแรนซัมแวร์ ที่อาจส่งผลกระทบต่อการดำเนินงานของโรงพยาบาล

2. การปฏิบัติตามกฎระเบียบและมาตรฐาน

การละเมิดกฎระเบียบ: การให้สิทธิ์เข้าถึงระบบแก่บุคคลภายนอกอาจขัดต่อกฎระเบียบหรือมาตรฐานที่เกี่ยวข้องกับความปลอดภัยของข้อมูลสุขภาพ เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

3. การจัดการสิทธิ์การเข้าถึง

การควบคุมสิทธิ์ที่ไม่เหมาะสม: หากไม่มีการกำหนดสิทธิ์การเข้าถึงอย่างชัดเจน อาจทำให้บุคคลภายนอกเข้าถึงข้อมูลหรือระบบที่ไม่เกี่ยวข้องกับหน้าที่ของตน

4. ความเสี่ยงด้านความน่าเชื่อถือของระบบ

ความเสถียรของระบบ: การเข้าถึงจากภายนอกอาจส่งผลต่อประสิทธิภาพและความเสถียรของระบบ หากไม่มีการจัดการทรัพยากรอย่างเหมาะสม

5. การฝึกอบรมและความตระหนักรู้

ความไม่เข้าใจในนโยบายความปลอดภัย: บุคคลภายนอกอาจไม่เข้าใจหรือไม่ปฏิบัติตามนโยบายความปลอดภัยของโรงพยาบาลอย่างเคร่งครัด

6. การบำรุงรักษาและอัปเดตระบบ

ความล่าช้าในการอัปเดต: การให้สิทธิ์เข้าถึงจากภายนอกอาจทำให้การอัปเดตระบบหรือการบำรุงรักษาเป็นไปอย่างล่าช้า หรือไม่สอดคล้องกับนโยบายของโรงพยาบาล

เพื่อแก้ไขปัญหาเหล่านี้ โรงพยาบาลควรกำหนดนโยบายและมาตรการความปลอดภัยที่ชัดเจน เช่น การใช้ระบบยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication) การเข้ารหัสข้อมูล และการฝึกอบรมบุคลากรทั้งภายในและภายนอกเกี่ยวกับความปลอดภัยของข้อมูล

* 1. **ความต้องการของระบบ**

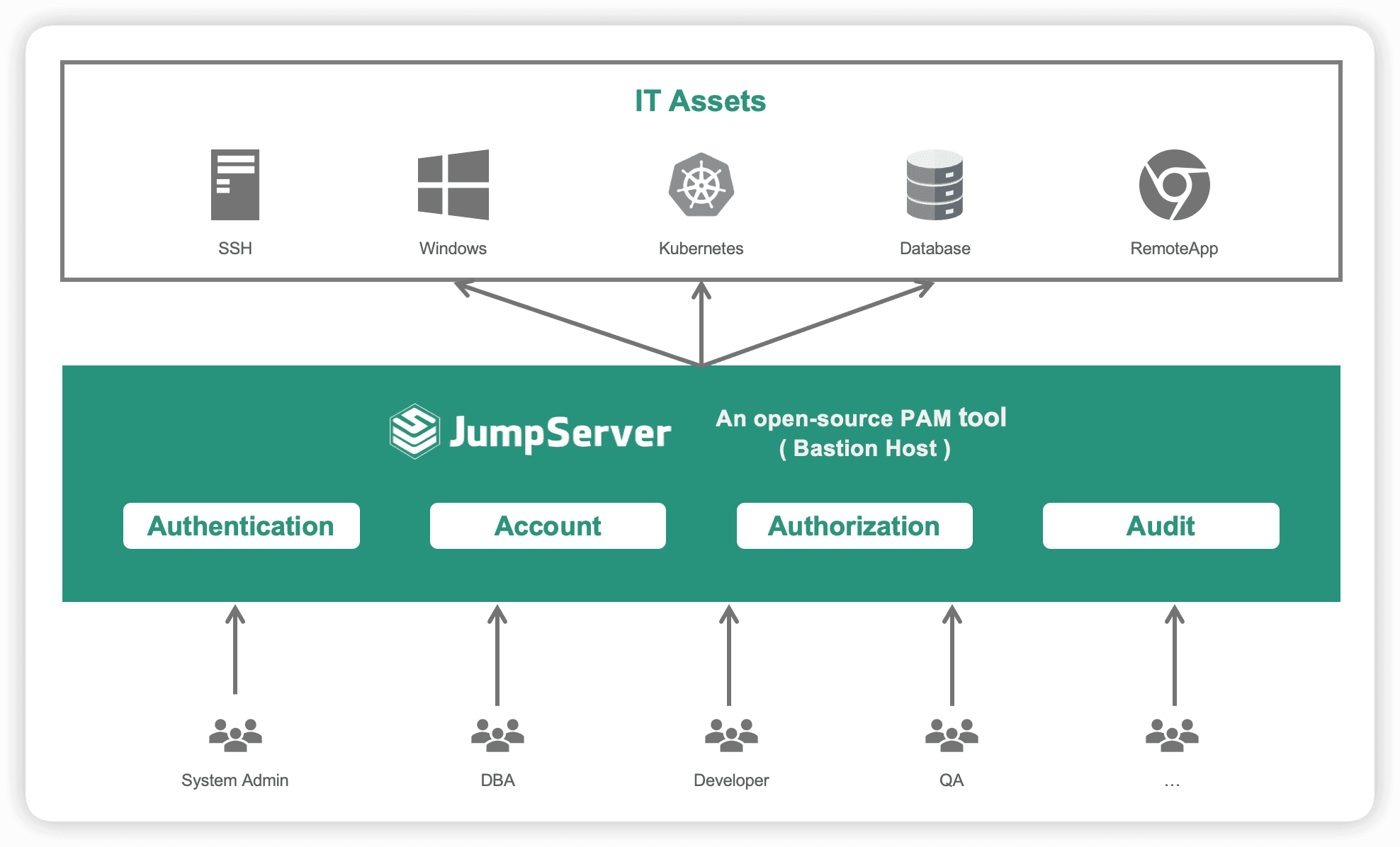
**Open Source Jump Server**

**Requirement**

- CPU 4Core

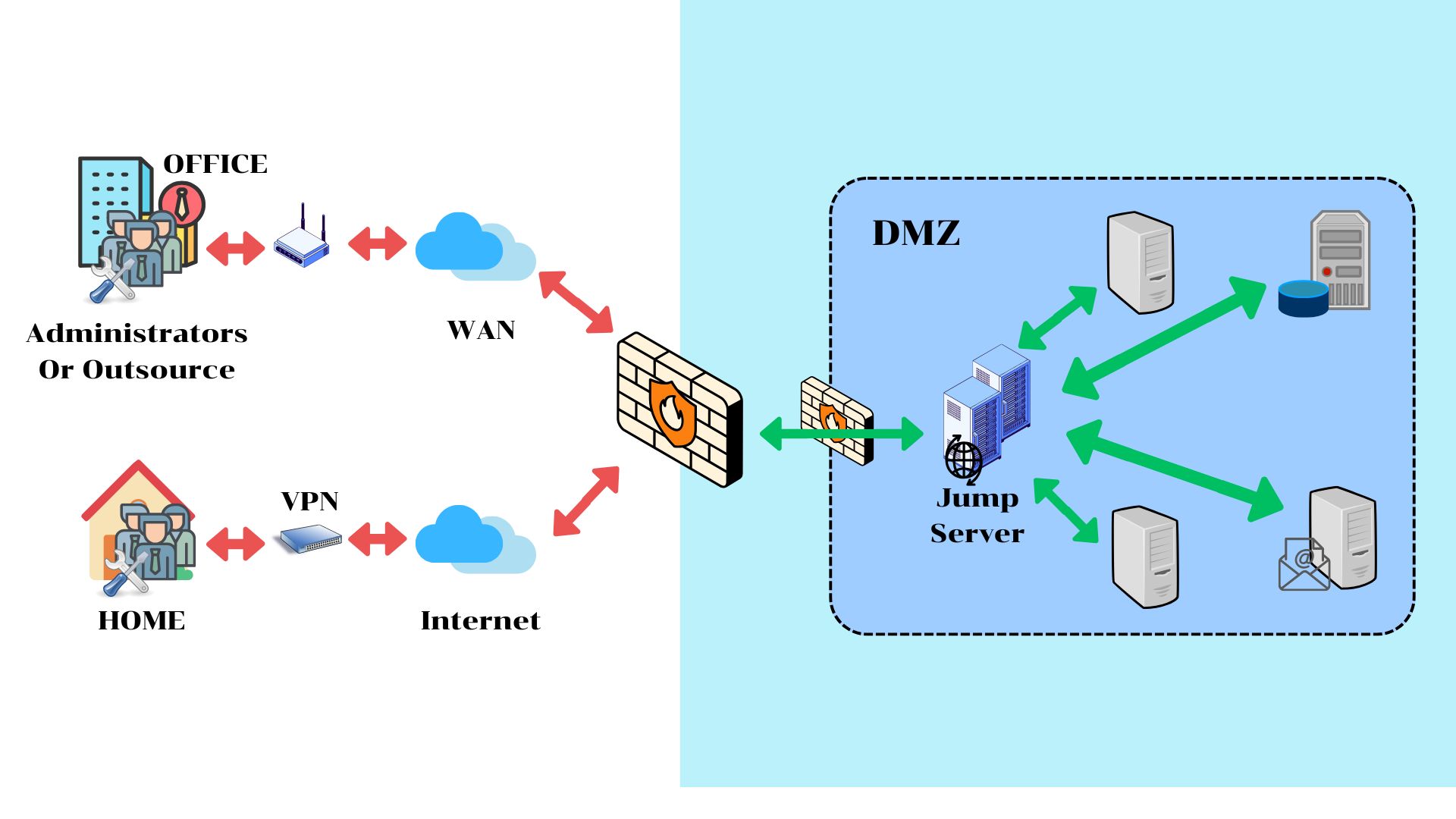
- RAM 8GB

- Storage 90GB SSD



**3. การออกแบบระบบ**

**3.1 สถาปัตยกรรมระบบ**

****

**3.2 การออกแบบความปลอดภัย**

การออกแบบระบบควบคุมการเข้าถึงระยะไกล (Remote Access Control) สำหรับโรงพยาบาลจำเป็นต้องคำนึงถึงความปลอดภัยของข้อมูลผู้ป่วยและความมั่นคงของระบบสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตและการโจมตีทางไซเบอร์ ดังนั้น การออกแบบควรประกอบด้วยองค์ประกอบดังต่อไปนี้:

1. การยืนยันตัวตนและการกำหนดสิทธิ์การเข้าถึง

การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication - MFA): ใช้การยืนยันตัวตนมากกว่าหนึ่งวิธี เช่น รหัสผ่านร่วมกับการยืนยันผ่านอุปกรณ์มือถือ เพื่อเพิ่มความปลอดภัยในการเข้าถึงระบบ

การกำหนดสิทธิ์ตามบทบาท (Role-Based Access Control - RBAC): กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบตามบทบาทหน้าที่ของผู้ใช้งาน เพื่อให้แน่ใจว่าผู้ใช้สามารถเข้าถึงเฉพาะข้อมูลที่จำเป็นต่อการปฏิบัติงานเท่านั้น

2. การเข้ารหัสข้อมูล

การเข้ารหัสข้อมูลระหว่างการส่งผ่าน (Data-in-Transit Encryption): ใช้โปรโตคอลการเข้ารหัส เช่น TLS/SSL เพื่อป้องกันการดักฟังข้อมูลระหว่างการส่งผ่าน

การเข้ารหัสข้อมูลที่จัดเก็บ (Data-at-Rest Encryption): เข้ารหัสข้อมูลที่จัดเก็บในเซิร์ฟเวอร์หรืออุปกรณ์จัดเก็บข้อมูล เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

3. การตรวจสอบและบันทึกกิจกรรม

การบันทึกกิจกรรมการเข้าถึง (Access Logs): บันทึกข้อมูลการเข้าถึงระบบ เช่น เวลา ผู้ใช้ และกิจกรรมที่ดำเนินการ เพื่อใช้ในการตรวจสอบและวิเคราะห์เหตุการณ์ที่อาจเกิดขึ้น

การตรวจสอบความปลอดภัยอย่างต่อเนื่อง (Continuous Security Monitoring): ใช้เครื่องมือและระบบที่สามารถตรวจสอบกิจกรรมที่ผิดปกติหรือพยายามโจมตีระบบแบบเรียลไทม์

4. การป้องกันและตอบสนองต่อภัยคุกคาม

การใช้ไฟร์วอลล์และระบบป้องกันการบุกรุก (Firewall and Intrusion Prevention Systems): ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและการโจมตีจากภายนอก

การวางแผนตอบสนองต่อเหตุการณ์ (Incident Response Plan): จัดทำแผนการตอบสนองเมื่อเกิดเหตุการณ์ความปลอดภัย เช่น การรั่วไหลของข้อมูล หรือการโจมตีทางไซเบอร์ เพื่อให้สามารถจัดการและกู้คืนระบบได้อย่างรวดเร็ว

5. การฝึกอบรมและสร้างความตระหนักรู้

การฝึกอบรมบุคลากร (Staff Training): จัดการฝึกอบรมเกี่ยวกับนโยบายความปลอดภัยและวิธีการปฏิบัติเพื่อป้องกันภัยคุกคามทางไซเบอร์

การสร้างความตระหนักรู้ (Awareness Programs): ส่งเสริมความตระหนักรู้เกี่ยวกับความเสี่ยงและวิธีการป้องกันภัยคุกคามทางไซเบอร์ในองค์กร

6. การปฏิบัติตามมาตรฐานและกฎระเบียบ

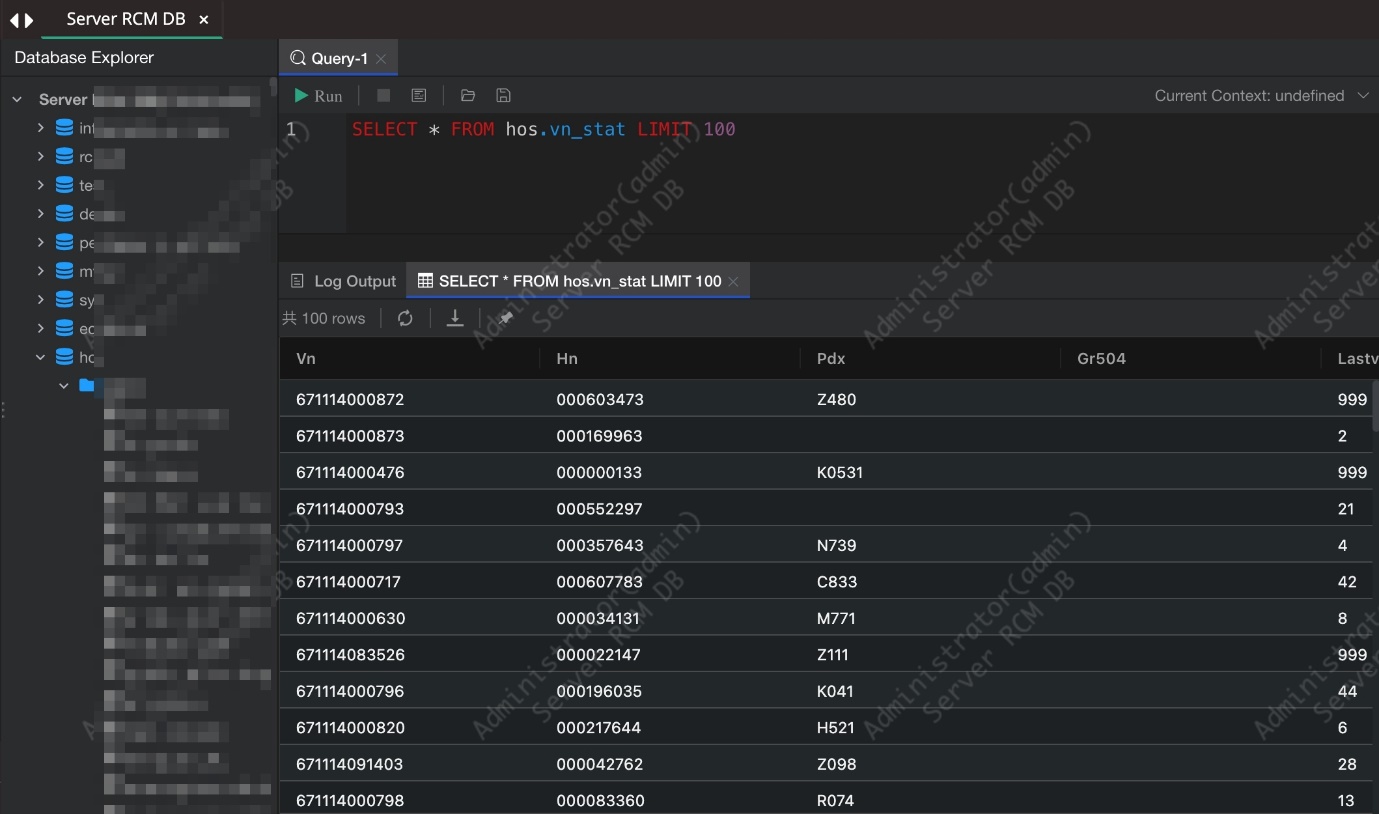
การปฏิบัติตามมาตรฐานความปลอดภัย (Compliance with Security Standards): ปฏิบัติตามมาตรฐานและแนวทางที่เกี่ยวข้อง เช่น แนวทางการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโรงพยาบาลของรัฐ

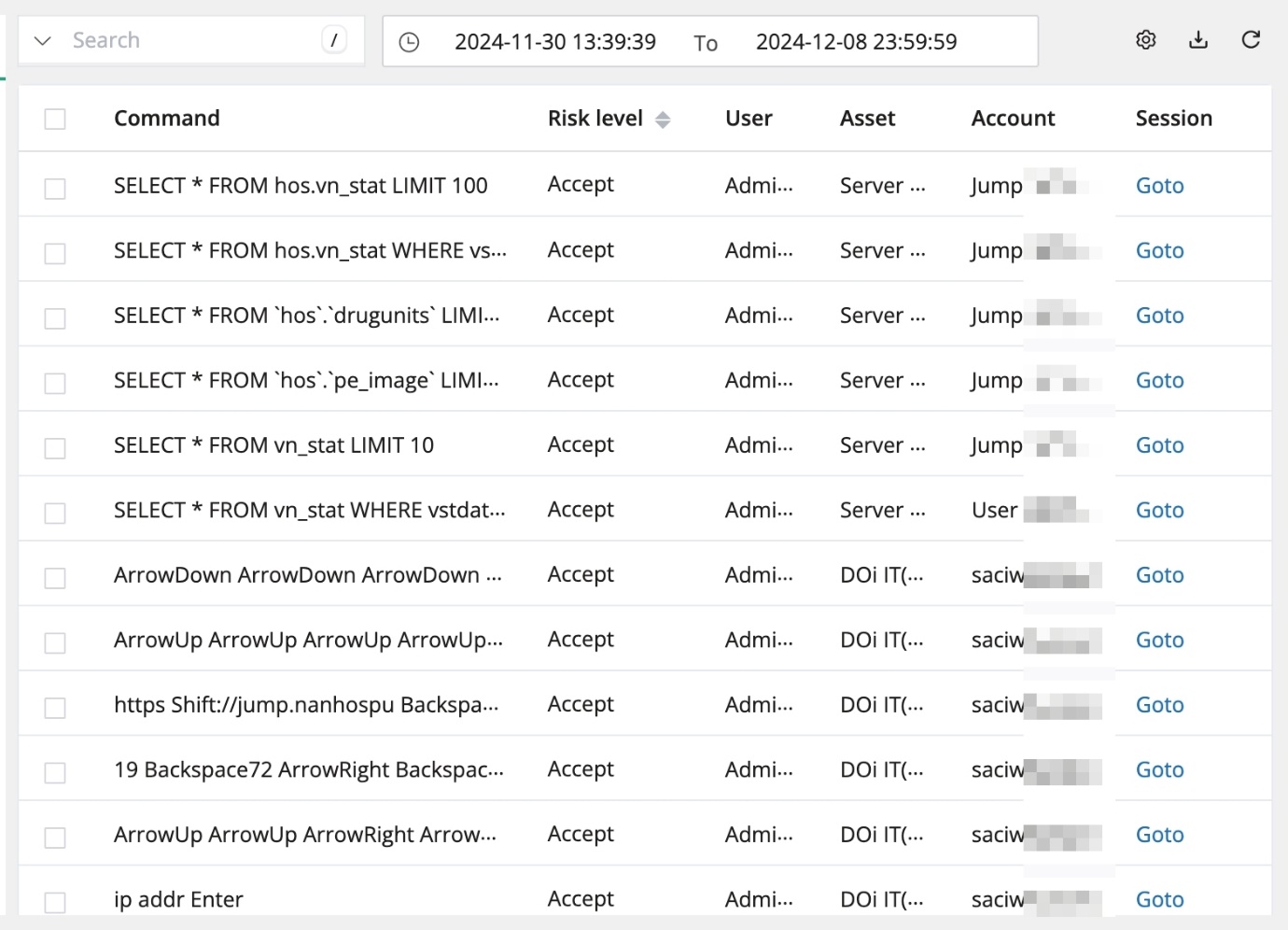
การประเมินและปรับปรุงระบบอย่างสม่ำเสมอ (Regular Assessment and Improvement): ดำเนินการประเมินความปลอดภัยของระบบเป็นระยะ และปรับปรุงตามความจำเป็นเพื่อรับมือกับภัยคุกคามใหม่ ๆ

การออกแบบระบบควบคุมการเข้าถึงระยะไกลที่มีความปลอดภัยสำหรับโรงพยาบาลควรคำนึงถึงองค์ประกอบเหล่านี้ เพื่อป้องกันความเสี่ยงและรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ

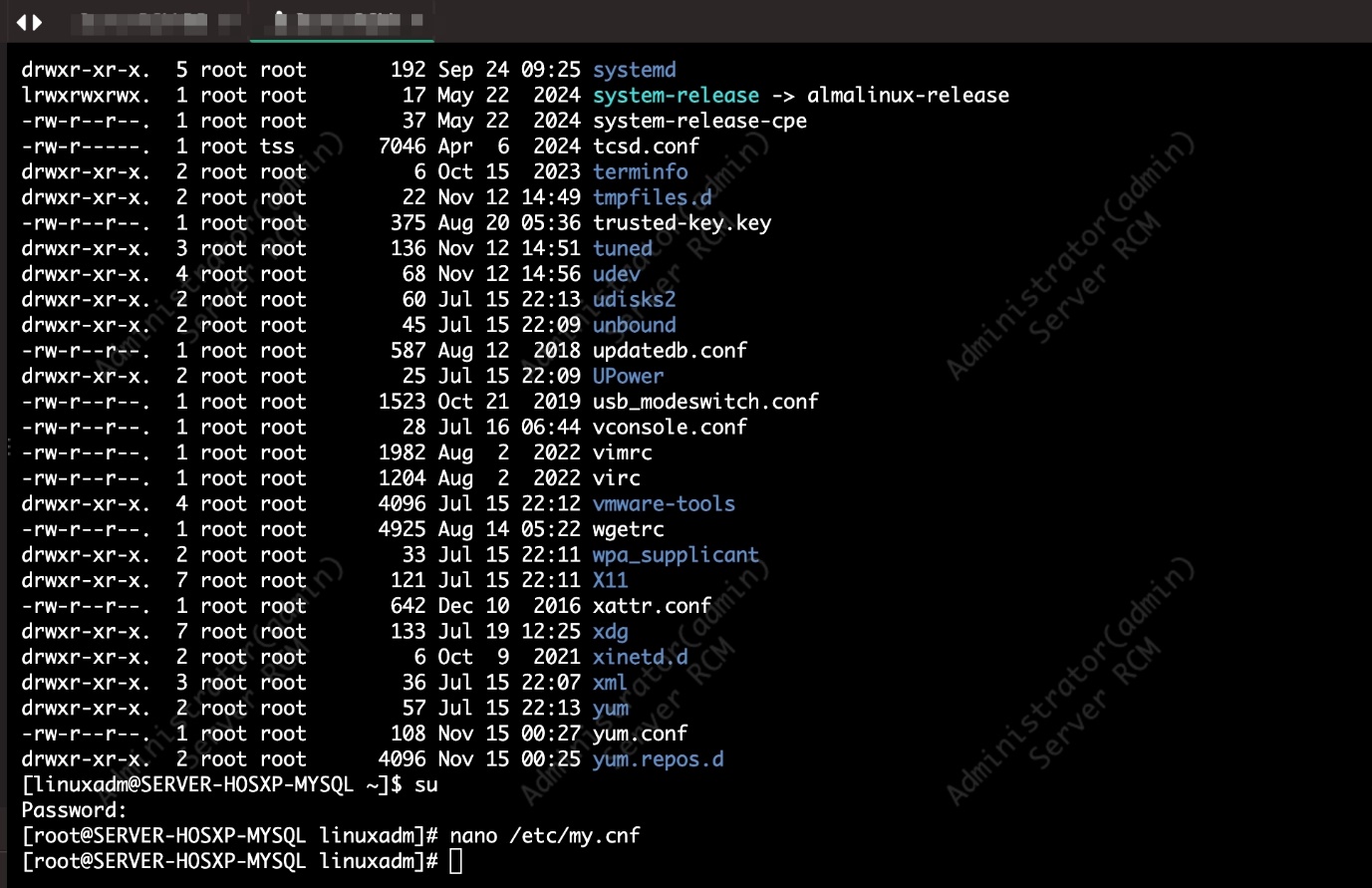
**3.3 แผนการทดสอบ**

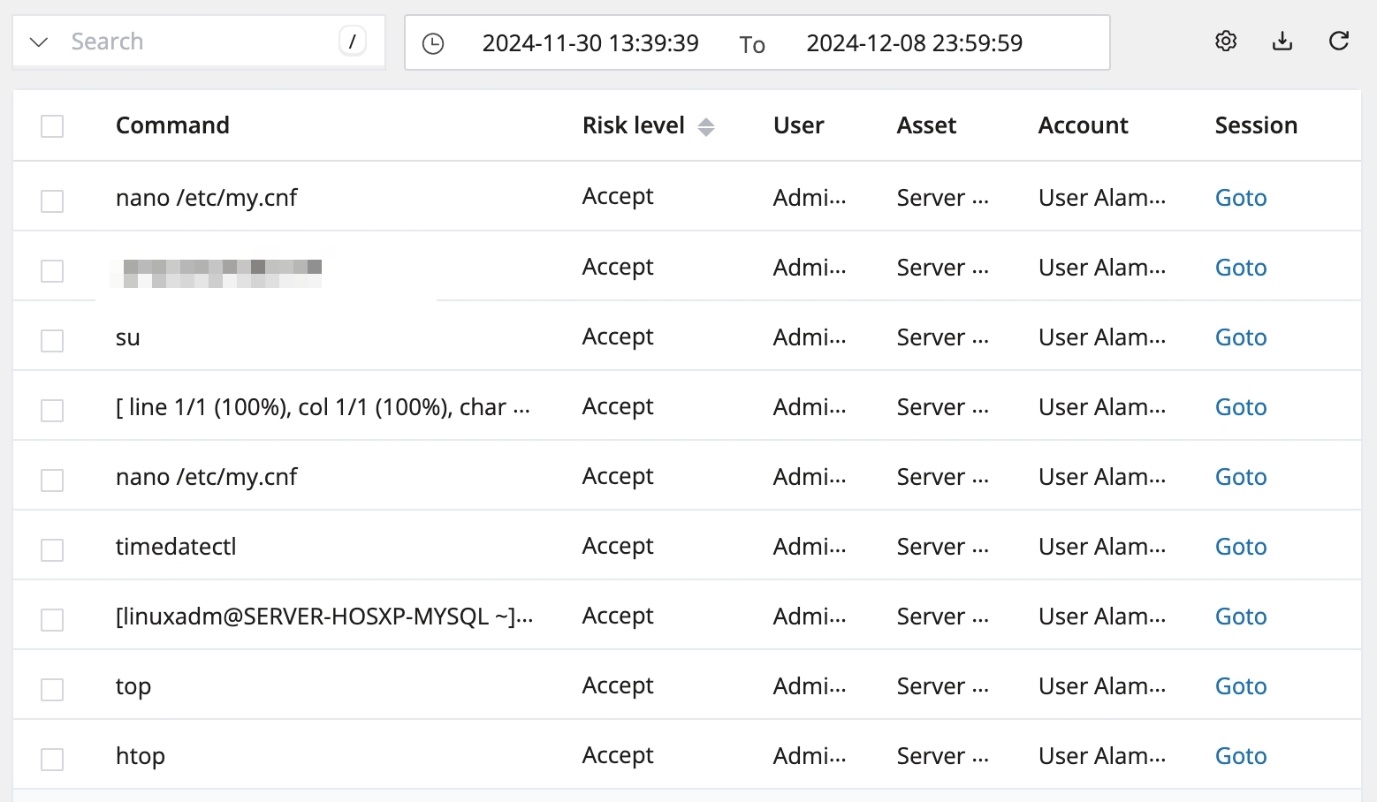
**- Test Cases & Results**

**1. การ Access MySQL**



**2.การ Access SSH**

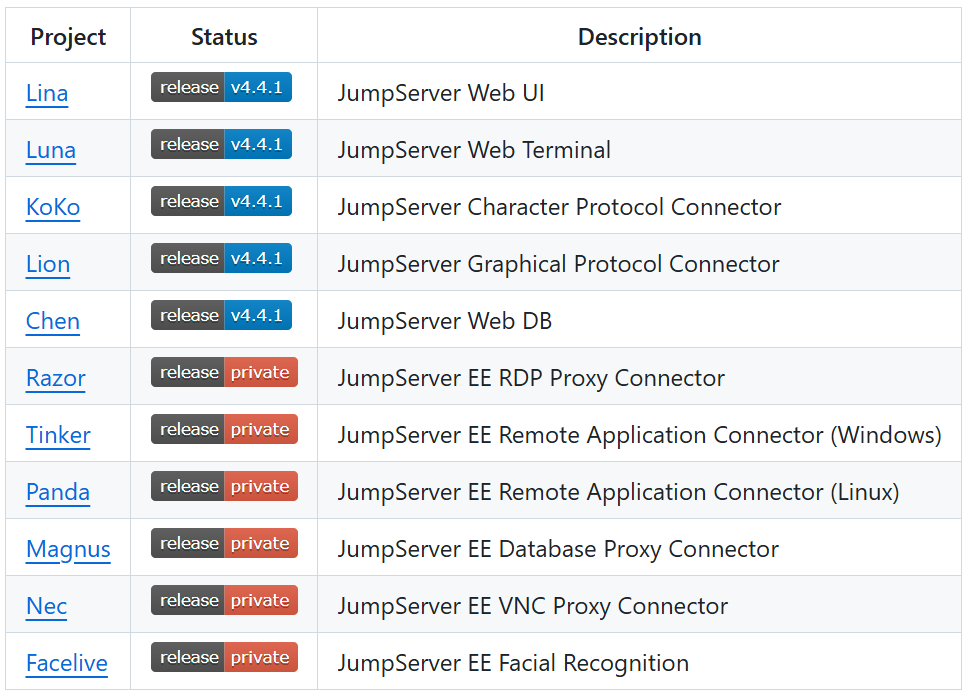


****

**4. การพัฒนาและติดตั้ง**

**4.1 เครื่องมือและเทคโนโลยี**

**- Tools & Technologies Used**

****

**Des:** [**Introduction - JumpServer**](https://www.jumpserver.com/docs)

**:[JumpServer · GitHub](https://github.com/jumpserver)**

**4.2 ขั้นตอนการติดตั้ง**

**- Configurations**

**Installation & Quickstart**

การติดตั้ง JumpServer เวอร์ชัน 4.0 บนระบบปฏิบัติการ Linux สามารถทำได้ตามขั้นตอนดังต่อไปนี้:

1. เตรียมความพร้อมของระบบ

- ระบบปฏิบัติการ: แนะนำให้ใช้ CentOS 7 หรือ Ubuntu 20.04

- ทรัพยากรระบบ: ควรมี CPU 4 คอร์ และ RAM อย่างน้อย 8GB

- การเชื่อมต่ออินเทอร์เน็ต: ระบบควรสามารถเข้าถึงอินเทอร์เน็ตได้เพื่อดาวน์โหลดแพ็กเกจที่จำเป็น

2. ติดตั้งและตั้งค่าคอนฟิกฐานข้อมูล

JumpServer ต้องการฐานข้อมูลเพื่อจัดเก็บข้อมูลต่าง ๆ โดยสามารถใช้ MySQL หรือ PostgreSQL ได้

- ติดตั้ง MySQL:

sudo yum install -y mysql-server

sudo systemctl start mysqld

sudo systemctl enable mysqld

- สร้างฐานข้อมูลและผู้ใช้สำหรับ JumpServer:

CREATE DATABASE jumpserver DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4\_general\_ci;

CREATE USER 'jumpserver'@'%' IDENTIFIED BY 'your\_password';

GRANT ALL PRIVILEGES ON jumpserver.\* TO 'jumpserver'@'%';

FLUSH PRIVILEGES;

3. ติดตั้ง JumpServer

- ดาวน์โหลด JumpServer เวอร์ชันล่าสุด:

cd /opt

wget https://github.com/jumpserver/jumpserver/releases/download/v4.0.0/jumpserver-installer-v4.0.0.tar.gz

tar -xf jumpserver-installer-v4.0.0.tar.gz

cd jumpserver-installer-v4.0.0

- ติดตั้ง JumpServer:

./install.sh all

คำสั่งนี้จะติดตั้งส่วนประกอบทั้งหมดที่จำเป็นสำหรับการทำงานของ JumpServer

4. ตั้งค่าคอนฟิก JumpServer

- แก้ไขไฟล์คอนฟิก:

vi ~/.jumpserver/config.txt

ปรับปรุงค่าต่าง ๆ เช่น การเชื่อมต่อฐานข้อมูล และพอร์ตที่ใช้

- เริ่มต้นบริการ JumpServer:

./jmsctl start

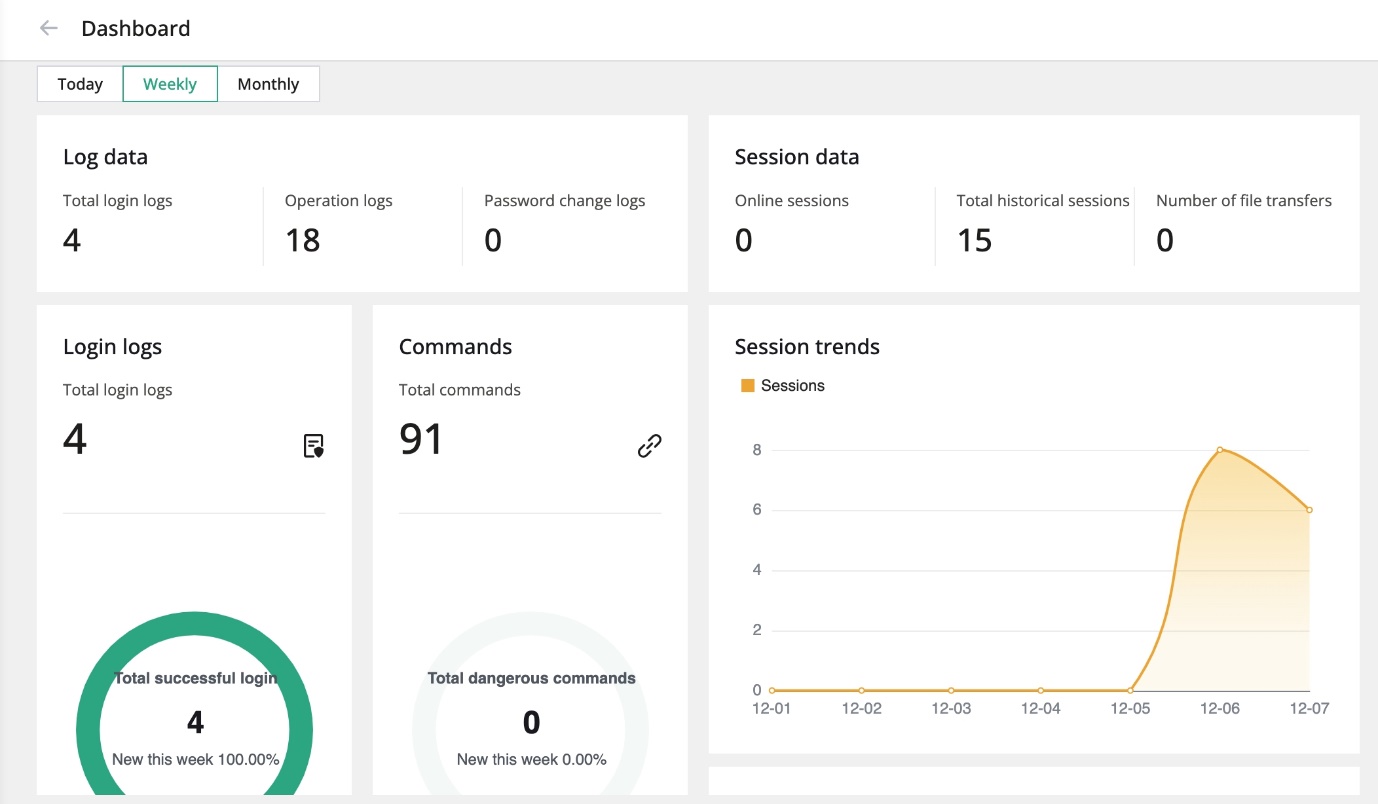
5. เข้าถึง JumpServer ผ่านเว็บอินเทอร์เฟซ

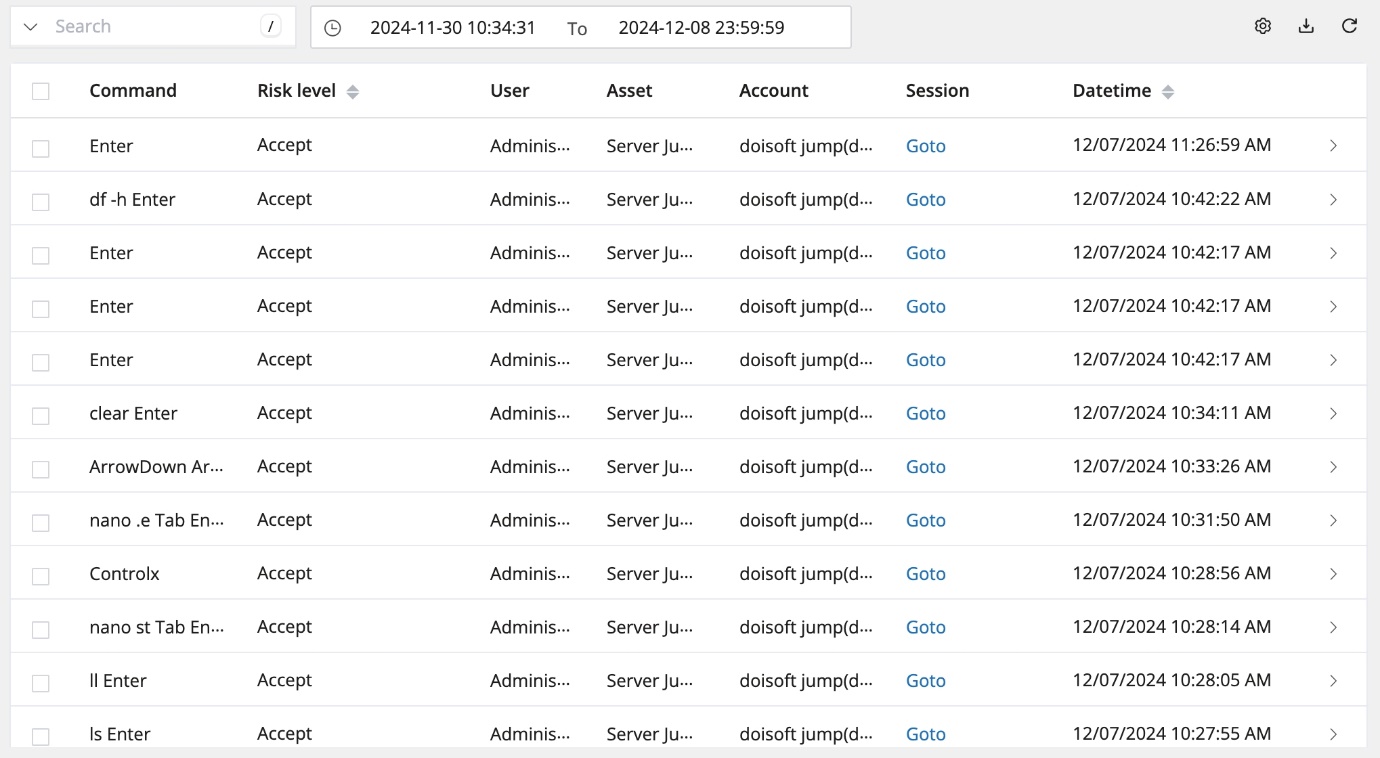
หลังจากติดตั้งและเริ่มต้นบริการแล้ว คุณสามารถเข้าถึง JumpServer ผ่านเว็บเบราว์เซอร์โดยไปที่ http://<server\_ip>:8080

หมายเหตุ: ขั้นตอนการติดตั้งอาจแตกต่างกันไปตามระบบปฏิบัติการและสภาพแวดล้อมของคุณ สำหรับรายละเอียดเพิ่มเติมและการตั้งค่าขั้นสูง แนะนำให้ศึกษาเอกสารทางการของ JumpServer

***Following*** [**https://www.jumpserver.com/docs/installation**](https://www.jumpserver.com/docs/installation)

**5. ผลการทดสอบ**

****

****

การทดสอบระบบ Privileged Access Management (PAM) เพื่อประเมินว่าระบบทำงานได้อย่างมีประสิทธิภาพและตรงตามความต้องการ สามารถดำเนินการผ่านกระบวนการที่ครอบคลุมด้าน ฟังก์ชันการทำงาน, ความปลอดภัย, และ การรองรับเหตุการณ์ที่ผิดปกติ

ขั้นตอนการทดสอบ PAM

1. การทดสอบฟังก์ชันการทำงาน (Functional Testing)

ตรวจสอบว่าระบบ PAM ทำงานตามที่กำหนด:

- การจัดเก็บและจัดการรหัสผ่าน

- ทดสอบว่ารหัสผ่านสามารถจัดเก็บได้อย่างปลอดภัย (เช่น การเข้ารหัส)

- ตรวจสอบการเปลี่ยนรหัสผ่านอัตโนมัติ (Password Rotation)

- การเข้าถึงแบบมีสิทธิ์จำกัด

- ตรวจสอบว่าเฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงบัญชี privileged ได้

- การรองรับการยืนยันตัวตนหลายปัจจัย (MFA)

- ทดสอบการบังคับใช้งาน MFA สำหรับบัญชี privileged

- การจำกัดการเข้าถึงตามเวลา (Time-bound Access)

- ตรวจสอบว่า PAM สามารถอนุญาตการเข้าถึงเฉพาะช่วงเวลาที่กำหนดได้

2. การทดสอบความปลอดภัย (Security Testing)

ทดสอบว่า PAM ป้องกันภัยคุกคามได้อย่างเหมาะสม:

- Brute Force Attack

- ใช้เครื่องมือจำลองการเดารหัสผ่าน เพื่อทดสอบว่าระบบล็อกบัญชีหรือแจ้งเตือนเมื่อมีความพยายามผิดปกติ

- Privilege Escalation

- จำลองการโจมตีเพื่อยกระดับสิทธิ์ของผู้ใช้ และตรวจสอบว่าระบบสามารถป้องกันได้

- การบันทึกและตรวจสอบกิจกรรม

- ทดสอบว่าระบบสามารถบันทึกกิจกรรมการเข้าถึงทั้งหมด และบันทึกมีความสมบูรณ์หรือไม่

- Data Encryption

- ตรวจสอบการเข้ารหัสของข้อมูลที่จัดเก็บ เช่น รหัสผ่านและคีย์

3. การทดสอบประสิทธิภาพ (Performance Testing)

- ทดสอบความเร็วในการประมวลผลคำขอ (เช่น การปล่อยรหัสผ่านหรือการอนุญาตการเข้าถึง)

- ทดสอบระบบภายใต้ภาระงานหนัก (Stress Testing) เพื่อดูว่าระบบยังทำงานได้ดีหรือไม่

4. การทดสอบการตอบสนองต่อเหตุการณ์ (Incident Response Testing)

ตรวจสอบว่าระบบ PAM มีการแจ้งเตือนและตอบสนองต่อเหตุการณ์ที่ผิดปกติ:

- พฤติกรรมที่ผิดปกติ (Anomalies)

- ทดสอบการแจ้งเตือนเมื่อมีการล็อกอินผิดปกติ (เช่น จากประเทศที่ไม่ได้รับอนุญาต)

- การปิดกั้นการเข้าถึง (Access Lockdown)

- ตรวจสอบว่าระบบสามารถล็อกบัญชีได้ทันทีเมื่อเกิดเหตุการณ์ที่ต้องสงสัย

- การแจ้งเตือนแบบเรียลไทม์ (Real-time Alerts)

- ทดสอบว่าผู้ดูแลระบบได้รับการแจ้งเตือนแบบเรียลไทม์เมื่อเกิดเหตุการณ์

5. การทดสอบการรวมระบบ (Integration Testing)

ทดสอบว่าระบบ PAM สามารถทำงานร่วมกับระบบอื่นในองค์กรได้ เช่น:

- Active Directory (AD)

- Single Sign-On (SSO)

- Security Information and Event Management (SIEM)

ตัวอย่างสถานการณ์การทดสอบ

1. สถานการณ์: ผู้ใช้ขอสิทธิ์การเข้าถึงบัญชี privileged

- ระบบต้องตรวจสอบ MFA และอนุญาตการเข้าถึงเฉพาะในเวลาที่กำหนด

- ต้องมีการบันทึกกิจกรรมทั้งหมด

2. สถานการณ์: มีการเปลี่ยนรหัสผ่านบัญชี privileged

- ทดสอบว่ารหัสผ่านใหม่ถูกจัดเก็บและเข้ารหัส

- ระบบต้องแจ้งเตือนผู้ดูแลระบบเกี่ยวกับการเปลี่ยนแปลง

3. สถานการณ์: ผู้ใช้พยายามเข้าถึงระบบจากไอพีที่ไม่ได้รับอนุญาต

- ระบบต้องปฏิเสธการเข้าถึงและแจ้งเตือนทันที

4. สถานการณ์: ระบบต้องเผชิญกับการโจมตี Brute Force

- ระบบต้องล็อกบัญชีที่ถูกโจมตีและแจ้งเตือนผู้ดูแลระบบ

เครื่องมือที่ใช้ในการทดสอบ PAM

- Metasploit: สำหรับจำลองการโจมตี

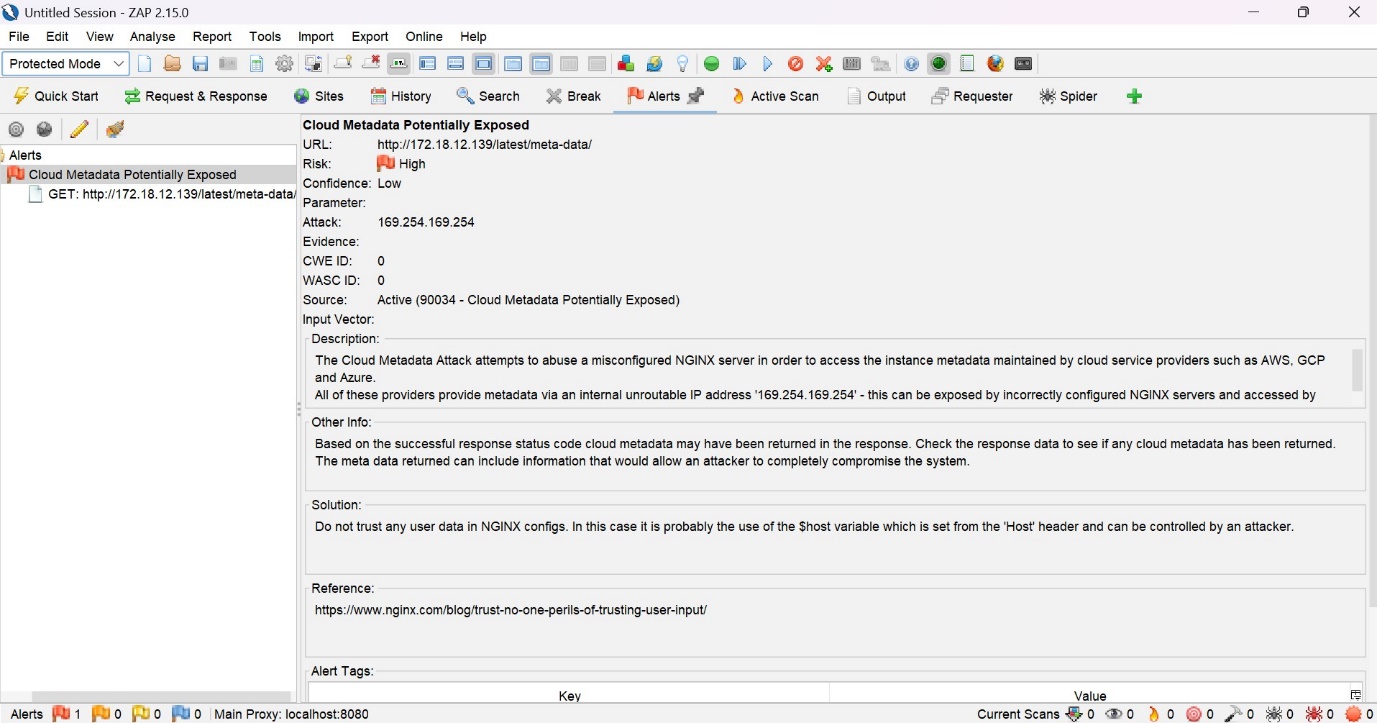
- Burp Suite: สำหรับทดสอบความปลอดภัยของเว็บแอปพลิเคชัน PAM

- OWASP ZAP: สำหรับตรวจสอบช่องโหว่ในระบบ

- Apache JMeter: สำหรับทดสอบประสิทธิภาพ

- Splunk หรือ ELK Stack: สำหรับวิเคราะห์บันทึกเหตุการณ์

**zap pentest result**

****

**Des:** **https://www.zaproxy.org/docs/alerts/90034/**

การประเมินผล

1. ระบุจุดที่ระบบ PAM ยังทำงานไม่ตรงตามที่กำหนด

2. เสนอแนวทางแก้ไข เช่น การปรับปรุงนโยบาย หรือเพิ่มฟีเจอร์ด้านความปลอดภัย

3. ทำการทดสอบซ้ำหลังจากปรับปรุง เพื่อยืนยันความถูกต้อง

**6. แผนการบำรุงรักษา**

1) Update version Software ให้เป็นปัจจุบัน

2) ทดสอบสิทธิ์การที่เข้าถึงที่ได้กำหนดไว้

3) ตรวจสอบความเพียงพอของการใช้ทรัพยากรของเครื่อง

**7. ข้อเสนอแนะและแนวทางพัฒนาต่อ**

การพัฒนาระบบควบคุมการเข้าถึงระยะไกล (Remote Access Control) สำหรับโรงพยาบาลจำเป็นต้องคำนึงถึงความปลอดภัยของข้อมูลผู้ป่วยและความมั่นคงของระบบสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตและการโจมตีทางไซเบอร์ ดังนั้น แนวทางการพัฒนาควรประกอบด้วย:

1. การประเมินความเสี่ยงและการจัดการ

- การค้นหาและประเมินความเสี่ยง: ดำเนินการค้นหาและประเมินช่องโหว่หรือจุดอ่อนในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล เพื่อระบุความเสี่ยงที่อาจเกิดขึ้น

- การวางแผนกลยุทธ์จัดการความเสี่ยง: พัฒนากลยุทธ์เพื่อจัดการและลดความเสี่ยงที่ระบุได้ โดยคำนึงถึงผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของโรงพยาบาล

2. การพัฒนานโยบายและมาตรฐานความปลอดภัย

- การจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์: กำหนดนโยบายที่ชัดเจนเกี่ยวกับการเข้าถึงระยะไกล รวมถึงมาตรการป้องกันและการตอบสนองต่อเหตุการณ์ที่อาจเกิดขึ้น

- การสร้างความตระหนักรู้: จัดการฝึกอบรมและสร้างความตระหนักรู้ให้แก่บุคลากรเกี่ยวกับความสำคัญของความปลอดภัยไซเบอร์และวิธีปฏิบัติตามนโยบายที่กำหนด

3. การใช้เทคโนโลยีและมาตรการป้องกัน

- การใช้ระบบยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication - MFA): เพิ่มความปลอดภัยในการเข้าถึงระบบโดยการยืนยันตัวตนผ่านหลายปัจจัย เช่น รหัสผ่านและการยืนยันผ่านอุปกรณ์มือถือ

- การเข้ารหัสข้อมูล: ใช้การเข้ารหัสข้อมูลทั้งในระหว่างการส่งผ่านและการจัดเก็บ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

- การติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS): เฝ้าระวังและป้องกันการโจมตีหรือการเข้าถึงที่ผิดปกติ

4. การตรวจสอบและปรับปรุงอย่างต่อเนื่อง

- การทดสอบการเจาะระบบ (Penetration Testing): ดำเนินการทดสอบเพื่อประเมินความแข็งแกร่งของระบบและระบุช่องโหว่ที่อาจมีอยู่

- การตรวจสอบและบำรุงรักษา: ดำเนินการตรวจสอบระบบอย่างสม่ำเสมอ และปรับปรุงตามความจำเป็นเพื่อรับมือกับภัยคุกคามใหม่ ๆ

การดำเนินการตามแนวทางเหล่านี้จะช่วยให้ระบบควบคุมการเข้าถึงระยะไกลของโรงพยาบาลมีความปลอดภัยและมีประสิทธิภาพสูงสุด

**คู่มือการใช้งาน**

**Quickstart Guide**

- <https://www.jumpserver.com/docs/quickstart>

**One-line installation**

- <https://www.jumpserver.com/docs/installation>

**Upgrade**

- <https://www.jumpserver.com/docs/upgrade>