**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP THỰC PHẨM TP.HCM**

**KHOA: CÔNG NGHỆ THÔNG TIN**

-----o0o----

****

**ĐỀ CƯƠNG ĐỀ TÀI:**

**HỆ THỐNG TÌM KIẾM, PHÁT HIỆN VÀ NGĂN NGỪA XÂM NHẬP**

**TÊN ĐỀ TÀI : Tìm hiểu và triển khai công cụ solarwind sercurity event manager**

**NHÓM : 2**

**Thành phố Hồ Chí Minh, tháng 5 năm 2022**

**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP THỰC PHẨM TP.HỒ CHÍ MINH**

**KHOA: CÔNG NGHỆ THÔNG TIN**

-----o0o----

****

**TÊN ĐỀ TÀI : Tìm hiểu và triển khai công cụ solarwind sercurity event manager**

**Thành phố Hồ Chí Minh, tháng 5 năm 2022**

**BẢNG ĐÁNH GIÁ MỨC ĐỘ HOÀN THÀNH**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| STT | HỌ VÀ TÊN | LỚP | MÃ SỐ SV | NỘI DUNG  PHỤ TRÁCH | MỨC ĐỘ ĐÓNG GÓP | XÁC NHẬN |
| 1 | Đặng Hoàng Duy | 10DHBM2 | 2033190158 | Tìm hiểu Solarwinds SEM thuyết trình | **20%** | Duy |
| 2 | Đinh Phạm Quốc Quyền | 10DHBM1 | 2033190112 | Tìm hiểu về công cụ Solarwinds SEM , thuyết trình | **20%** | Quyền |
| 3 | Giáp Đức Tài | 10DHBM2 | 2033192280 | Tiến hành làm lab 3 , làm power point | **20%** | Tài |
| 4 | Trần Minh  Trí | 10DHBM2 | 2033190135 | Tiến hành làm lab 3 | **20%** | Trí |
| 5 | Phạm Huy Trường | 10DHBM2 | 2033190042 | Tìm hiểu Solarwinds SEM , làm word | **20%** | Trường |

**LỜI CẢM ƠN**

Lời đầu tiên chúng em xin gửi lời cảm ơn chân thành đến quý thầy,cô giáo trong khoa Công nghệ Thông Tin trường Đại học Công nghiệp thực phẩm Tp Hồ Chí Minh đã truyền đạt kiến thức và kinh nghiệm quý báu cho chúng em trong suốt quá trình học tập và rèn luyện .

Đặc biệt chúng em xin gởi lời cảm ơn đến thầy Bùi Duy Cương, người đã trực tiếp hướng dẫn và tận tình giúp đỡ chúng em trong suốt thời gian học môn “Hệ Thống Tìm Kiếm, Phát Hiện Và Ngăn Ngừa Xâm Nhập” cũng như trong thời gian chúng em thực hiện thực bài tập kết thúc môn học.

Mặc dù đã cố gắng trong quá trình làm bài nhưng không thể tránh khỏi những sai sót. Chúng em mong nhận được sự góp ý,nhận xét của quý thầy cô và các bạn về nội dung cũng như hình thức trình bày để bài báo cáo được hoàn thiện.

Chúng em xin chân thành cảm ơn thầy cô và các bạn

MỤC LỤC

[PHẦN MỞ ĐẦU 1](#_Toc105757612)

[PHẦN NỘI DUNG 2](#_Toc105757613)

[1. IPS là gì? 2](#_Toc105757614)

[1.1. Khái quát về IPS 2](#_Toc105757615)

[1.2. IPS có thể ngăn chặn những loại tấn công nào? 2](#_Toc105757616)

[1.3. IPS sẽ làm gì nếu phát hiện ra một cuộc tấn công? 2](#_Toc105757617)

[1.4. Ưu và nhược điểm của hệ thống IPS 2](#_Toc105757618)

[1.5. Sự khác nhau của IPS và IDS ? 3](#_Toc105757619)

[2. Solari 4](#_Toc105757620)

[2.1. Công cụ bảng điều khiển quản lý Solaris 4](#_Toc105757621)

[2.2. Công cụ mở rộng đáng tin cậy trong Bảng điều khiển quản lý Solaris 5](#_Toc105757622)

[2.3. Công cụ Security Templates 6](#_Toc105757623)

[2.4. Công cụ Trusted Network Zones 7](#_Toc105757624)

[2.5. Giao tiếp máy khách-máy chủ với bảng điều khiển quản lý Solaris 7](#_Toc105757625)

[3. Demo 7](#_Toc105757626)

### PHẦN MỞ ĐẦU

Trong thời đại công nghiệp 4.0 hiện nay, thì vai trò của Công nghệ Thông tin nói chung và Internet nói riêng ngày càng vô cùng quan trọng. Điều này kéo theo đa phần các doanh nghiệp, công ty hay các tổ chức đều phải phụ thuộc vào máy vi tính. Nhu cầu truy cập từ xa (ngoài văn phòng công ty) để làm việc cũng ngày càng phổ biến. Đó là nhu cầu rất thiết thực, giúp con người chủ động hơn trong công việc và ngăn chặn các cuộc tấn công mạng . Để ngăn ngừa điều đó thì

### PHẦN NỘI DUNG

# 1. IPS là gì?

## 1.1. Khái quát về IPS

IPS là tên viết tắt của Intrusion Prevention Systems, nó là một hệ thống ngăn ngừa xâm nhập mạng đang được ứng dụng phổ biến hiện nay. IPS được biết đến như một hệ thống kiểm soát, vì nó có thể phát hiện các mối đe dọa tiềm ẩn đối với hệ thống và cơ sở hạ tầng mạng, nó sẽ tìm cách để chủ động chặn bất kì các kết nối nào được cho là các mối đe dọa.

## 1.2. IPS có thể ngăn chặn những loại tấn công nào?

Các hệ thống phòng chống xâm nhập có thể tìm kiếm và bảo vệ chống lại nhiều loại tấn công nguy hiểm tiềm ẩn. Chúng có khả năng phát hiện và chặn các [cuộc tấn công từ chối dịch vụ (DoS), tấn công từ chối dịch vụ phân tán (DDoS)](https://quantrimang.com/tim-hieu-ve-tan-cong-tu-choi-dich-vu-dos-34926), bộ công cụ exploit, worm, virus máy tính và những loại phần mềm độc hại khác.

## 1.3. IPS sẽ làm gì nếu phát hiện ra một cuộc tấn công?

Một hệ thống ngăn chặn xâm nhập có thể phát hiện nhiều cuộc tấn công khác nhau bằng cách phân tích các gói và tìm kiếm những chữ ký phần mềm độc hại cụ thể, mặc dù nó cũng có thể tận dụng khả năng theo dõi hành vi để tìm kiếm hoạt động bất thường trên mạng, cũng như giám sát bất kỳ giao thức và chính sách bảo mật cấp quản trị nào, cũng như [liệu](https://www.semtek.com.vn/du-lieu-la-gi/) chúng có bị vi phạm hay không.

Nếu bất kỳ phương pháp nào trong số này phát hiện ra một cuộc tấn công tiềm ẩn, IPS có thể ngay lập tức chấm dứt kết nối đến. Địa chỉ IP vi phạm sau đó có thể bị chặn nếu IPS được cấu hình để làm như vậy hoặc người dùng liên kết với nó bị cấm truy cập lại vào mạng và bất kỳ tài nguyên nào được kết nối.

IPS cũng có thể thay đổi cài đặt [tường lửa](https://www.semtek.com.vn/tuong-lua-la-gi/) cục bộ để phát hiện lại các cuộc tấn công như vậy và thậm chí có thể loại bỏ mọi tàn tích của cuộc tấn công bằng cách loại bỏ những header bị ảnh hưởng bởi phần mềm độc hại, file đính kèm bị nhiễm virus, cũng như những liên kết độc hại khỏi file và email [server](https://www.semtek.com.vn/server/).

## 1.4. Ưu và nhược điểm của hệ thống IPS

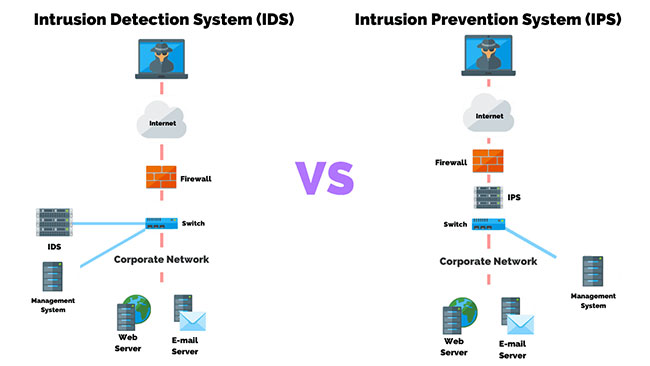
Ưu điểm:

IPS giúp bảo vệ toàn diện tài nguyên hệ thống. Nó sẽ mang đến công dụng phòng ngừa và ngăn chặn kịp thời các hoạt động tấn công đến hệ thống mạng.

Nhược điểm:

IPS cũng có thể gây ra những phát hiện nhầm, nó có thể không cho người dùng ở thiết bị khác có thể truy cập hệ thống.

## 1.5. Sự khác nhau của IPS và IDS ?



[Hệ thống phát hiện xâm nhập (IDS)](https://quantrimang.com/he-thong-phat-hien-xam-pham-ids-phan-1-37334) và hệ thống ngăn chặn xâm nhập (IPS) đều có thể liên quan đến bảo mật, nhưng chúng có các mục tiêu và phương tiện hoàn toàn khác nhau.

` Có nhiều loại IDS cũng như IPS và tất cả chúng đều hoạt động hơi khác nhau một chút. Đối với IDS, có các hệ thống phát hiện xâm nhập mạng (NIDS), đặt tại các điểm chiến lược trong mạng để phát hiện những cuộc tấn công tiềm ẩn khi chúng đang diễn ra trong mạng. HIDS hay hệ thống phát hiện xâm nhập máy chủ chạy trên các hệ thống và thiết bị riêng lẻ, chỉ giám sát hoạt động trên mạng đi và đến hệ thống cụ thể đó.

Trong cả hai trường hợp, IDS phát hiện ra một cuộc tấn công tiềm ẩn sẽ thông báo cho quản trị viên hệ thống.

Hệ thống IPS sẽ đóng một vai trò tương tự như IDS - và có thể được sử dụng kết hợp để giám sát mạng tốt hơn - nhưng sẽ đóng vai trò tích cực hơn trong việc bảo vệ mạng. IPS cũng sẽ thông báo cho quản trị viên nếu phát hiện các cuộc tấn công, nhưng chúng cũng sẽ thực hiện những hành động trừng phạt đối với bất kỳ hệ thống, tài khoản cá nhân hoặc lỗ hổng tường lửa nào để đảm bảo rằng cuộc tấn công đã bị chặn và mọi file liên quan bị xóa khỏi mạng.

Các hệ thống phát hiện xâm nhập được thiết kế để cho bạn biết liệu có khả năng và khi nào một cuộc tấn công xảy ra, để bạn có thể xử lý vấn đề theo cách thủ công. Hệ thống ngăn chặn xâm nhập được thiết kế để chủ động bảo vệ hệ thống của bạn khỏi các cuộc tấn công và ngăn chặn những cuộc tấn công trong tương lai thông qua việc điều chỉnh các thông số mạng.

# 2. Solarwind

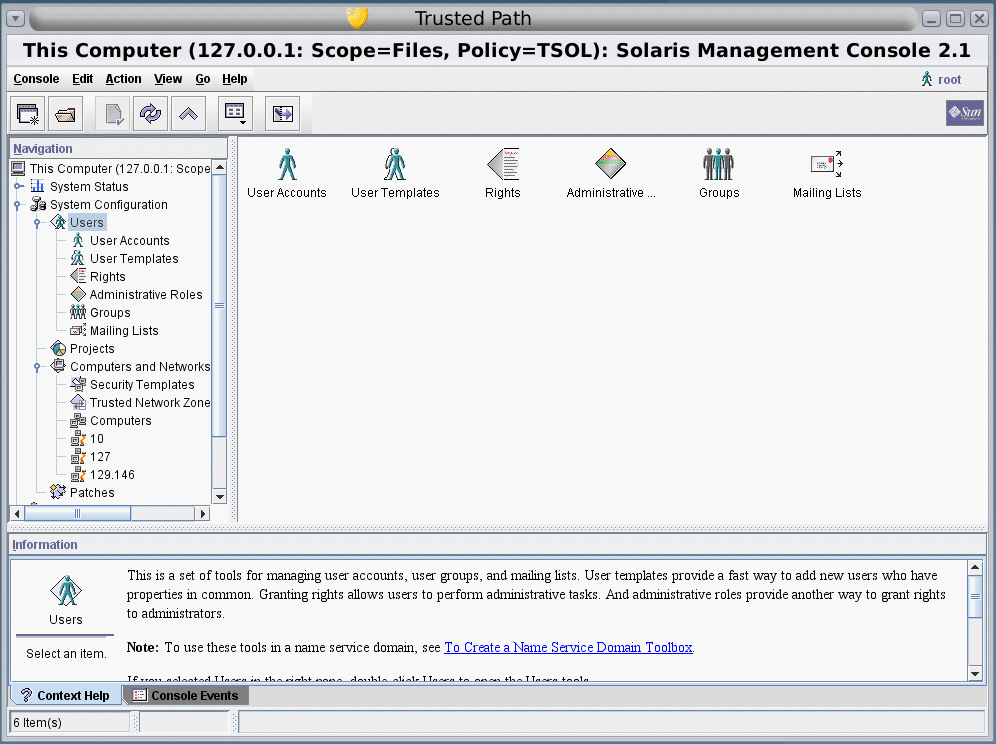
## 2.1. Công cụ bảng điều khiển quản lý Solarwind

Bảng điều khiển quản lý Solarwind cung cấp quyền truy cập vào các hộp công cụ của các công cụ quản trị dựa trên GUI. Các công cụ này cho phép bạn chỉnh sửa các mục trong các cơ sở dữ liệu cấu hình khác nhau. Trong Trusted Extensions, Solaris Management Console là giao diện quản trị cho người dùng, vai trò và cơ sở dữ liệu mạng đáng tin cậy.

Phần mở rộng đáng tin cậy mở rộng Bảng điều khiển quản lý Solaris:

* Trusted Extensions sửa đổi bộ công cụ Solaris Management Console Users.
* Trusted Extensions thêm công cụ Security Templates và công cụ Trusted Network Zones vào bộ công cụ Computers and Networks.

Các công cụ Solaris Management Console được thu thập vào các hộp công cụ theo phạm vi và chính sách bảo mật. Để quản lý Tiện ích mở rộng đáng tin cậy, Trusted Extensions cung cấp các hộp công cụ có Chính sách =TSOL. Bạn có thể truy cập các công cụ theo phạm vi, nghĩa là, theo dịch vụ đặt tên. Các phạm vi có sẵn là máy chủ địa phương và LDAP.



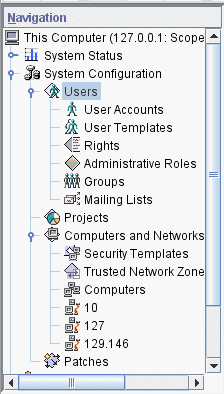
Hộp công cụ mở rộng đáng tin cậy điển hình trong Bảng điều khiển quản lý Solaris

## 2.2. Công cụ mở rộng đáng tin cậy trong Bảng điều khiển quản lý Solarwind

Trusted Extensions thêm các thuộc tính bảo mật có thể cấu hình cho ba công cụ:

* User Accounts tool – Là giao diện quản trị để thay đổi nhãn của người dùng, thay đổi chế độ xem nhãn của người dùng và để kiểm soát việc sử dụng tài khoản.
* Administrative Roles tool – Là giao diện quản trị để thay đổi phạm vi nhãn của vai trò và hành vi khóa màn hình khi nhàn rỗi.
* Rights tool – Bao gồm các hành động CDE có thể được gán cho hồ sơ quyền. Các thuộc tính bảo mật có thể được gán cho các hành động này.

Trusted Extensions thêm hai công cụ vào bộ công cụ Máy tính và Mạng:

* Security Templates tool – Là giao diện quản trị để quản lý các khía cạnh nhãn của máy chủ và mạng. Công cụ này sửa đổi cơ sở dữ liệu tnrhtp và tnrhdb, thực thi độ chính xác cú pháp và cập nhật hạt nhân với những thay đổi.
* Trusted Network Zones tool – Là giao diện quản trị để quản lý các khía cạnh nhãn của các khu vực. Công cụ này sửa đổi cơ sở dữ liệu tnzonecfg, thực thi độ chính xác cú pháp và cập nhật hạt nhân với những thay đổi.

Máy tính và Công cụ Mạng được đặt trong Bảng điều khiển quản lý Solaris

## 2.3. Công cụ Security Templates

Một mẫu bảo mật mô tả một tập hợp các thuộc tính bảo mật có thể được gán cho một nhóm máy chủ. Công cụ Mẫu Bảo mật cho phép bạn thuận tiện gán một sự kết hợp cụ thể của các thuộc tính bảo mật cho một nhóm máy chủ. Những thuộc tính này kiểm soát cách dữ liệu được đóng gói, truyền và giải thích. Các máy chủ được gán cho một mẫu có thiết đặt bảo mật giống hệt nhau.

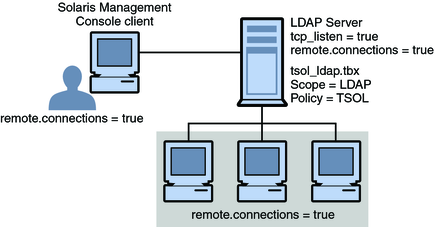
Các máy chủ được xác định trong công cụ Máy tính. Các thuộc tính bảo mật của máy chủ được gán trong công cụ Mẫu Bảo mật. Hộp thoại Sửa đổi Mẫu có hai tab:

* General tab – Mô tả mẫu. Bao gồm tên, loại máy chủ, nhãn mặc định, tên miền giải thích (DOI), phạm vi công nhận và bộ nhãn nhạy cảm rời rạc.
* Hosts Assigned to Template tab – Liệt kê tất cả các máy chủ trên mạng mà bạn đã gán cho mẫu này.

## 2.4. Công cụ Trusted Network Zones

Công cụ Trusted Network Zones xác định các vùng trên hệ thống của bạn. Ban đầu, khu vực toàn cầu được liệt kê. Khi bạn thêm vùng và nhãn của chúng, tên vùng sẽ hiển thị trong ngăn. Tạo vùng thường xảy ra trong quá trình cấu hình hệ thống. Gán nhãn, cấu hình cổng đa cấp và chính sách nhãn được cấu hình trong công cụ này. Để biết chi tiết, hãy xem [Chương 10, Quản lý Vùng trong Phần mở rộng Đáng tin cậy (Nhiệm vụ)](https://docs.oracle.com/cd/E23823_01/html/819-0872/managezones-1.html#scrolltoc).

## 2.5. Giao tiếp máy khách-máy chủ với bảng điều khiển quản lý Solaris

Thông thường, một khách hàng Solaris Management Console quản lý hệ thống từ xa. Trên một mạng sử dụng LDAP làm dịch vụ đặt tên, máy khách Solaris Management Console kết nối với máy chủ Solaris Management Console chạy trên máy chủ LDAP.

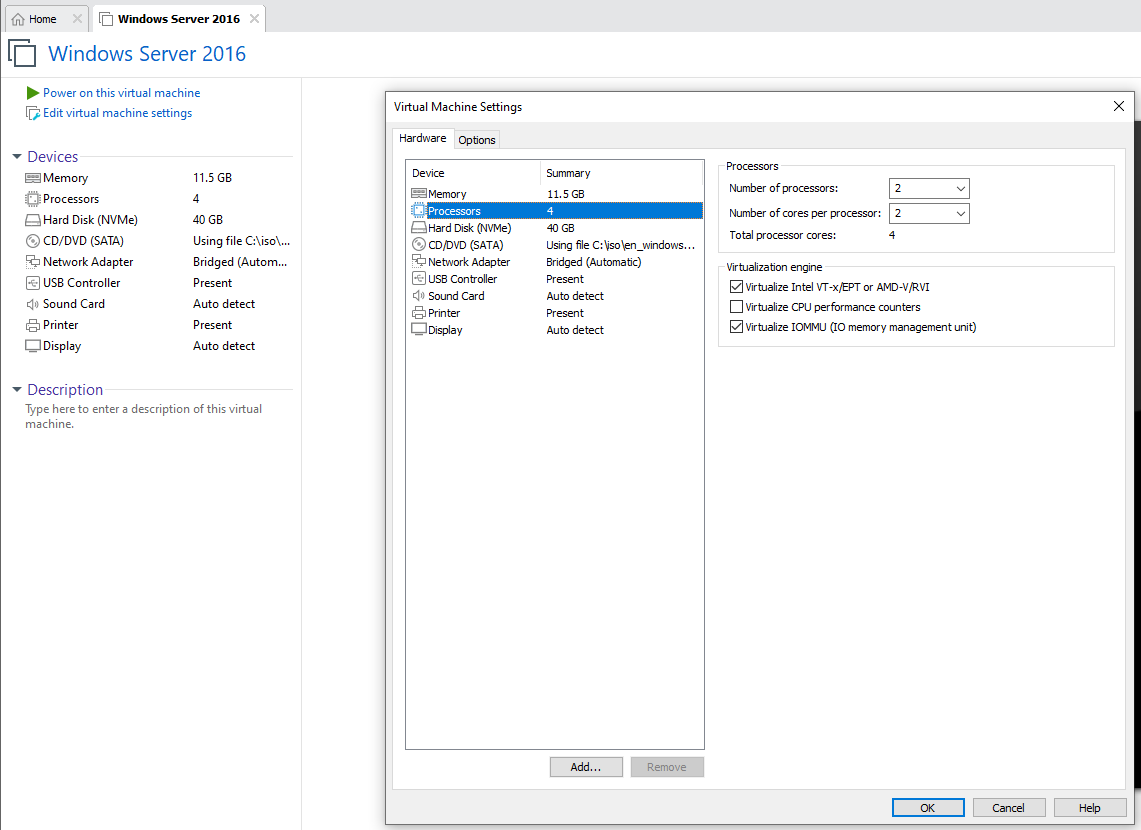
Solaris Quản lý Máy khách sử dụng máy chủ LDAP để quản lý mạng

solaris Management Console Khách hàng quản lý các hệ thống từ xa riêng lẻ trên mạng

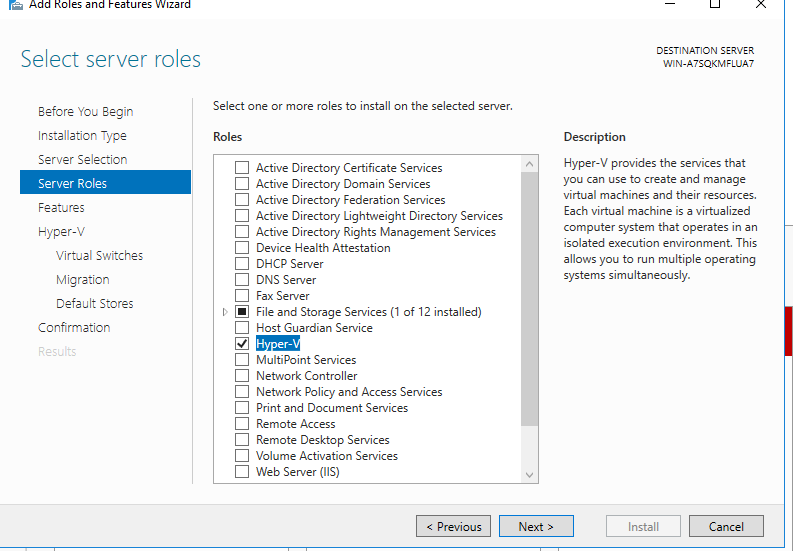
# 3. Demo

***Lab 03 : Ta cần 2 máy ảo , 1 máy để chạy hyper cho solarwind và 1 máy ảo để kết nối vào solarwind***

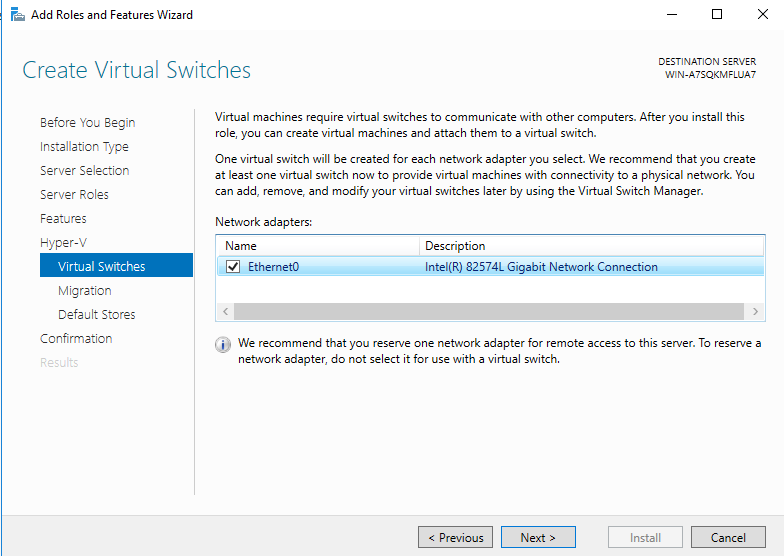
Ta sẽ tiến hành cài đặt Solarwinds SEM trên máy windowserver trước khi cài thì ta phải cài đặt hyper-V cho máy



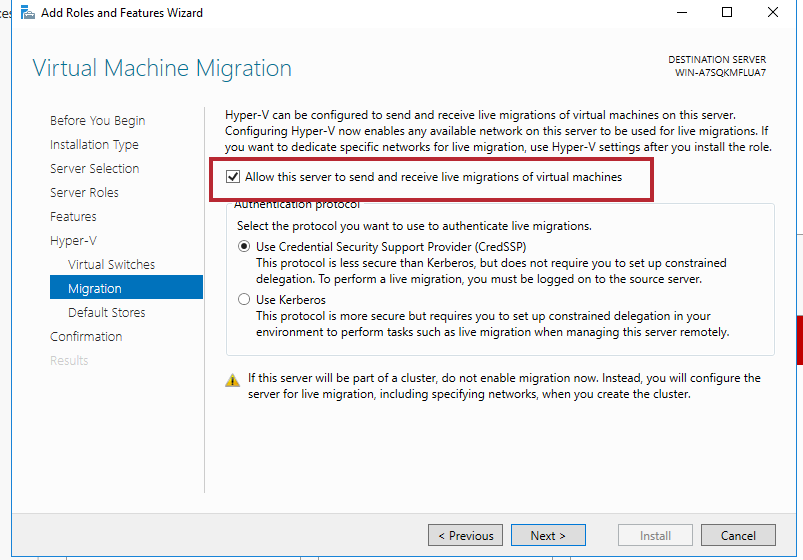
Hình 1: Đầu tiên ta cần bật các công nghệ ảo hóa lên



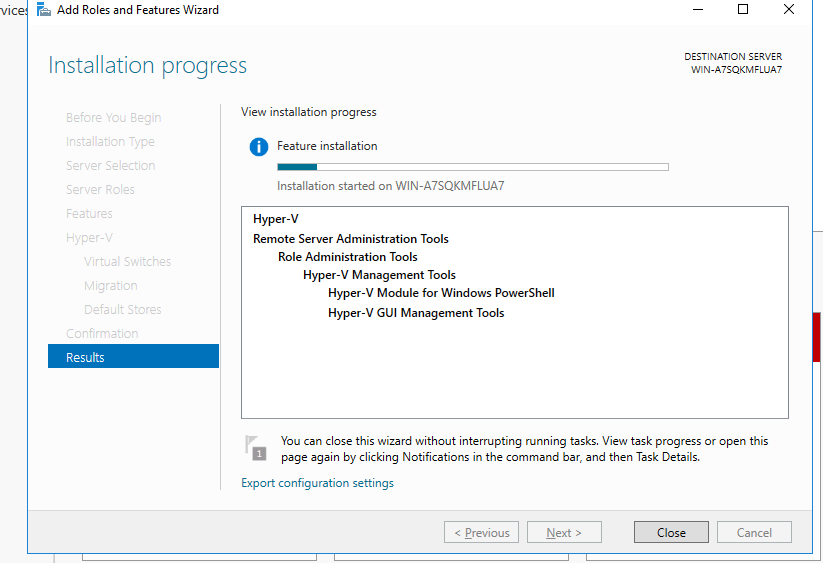
Hình 2: Add Features cho nó



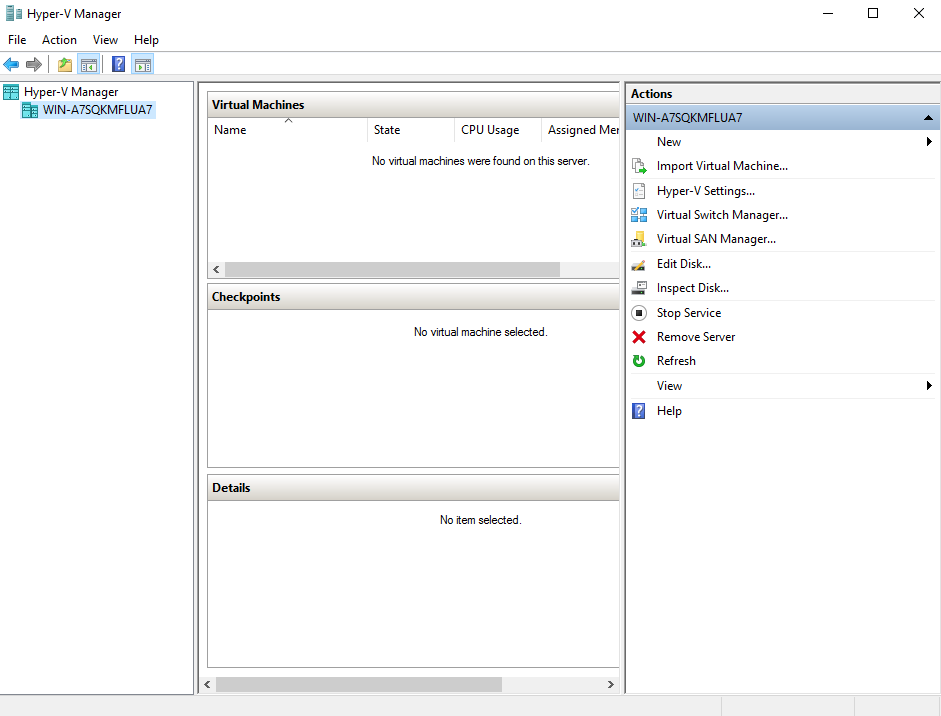
Hình 3: Ta chọn card mạng máy



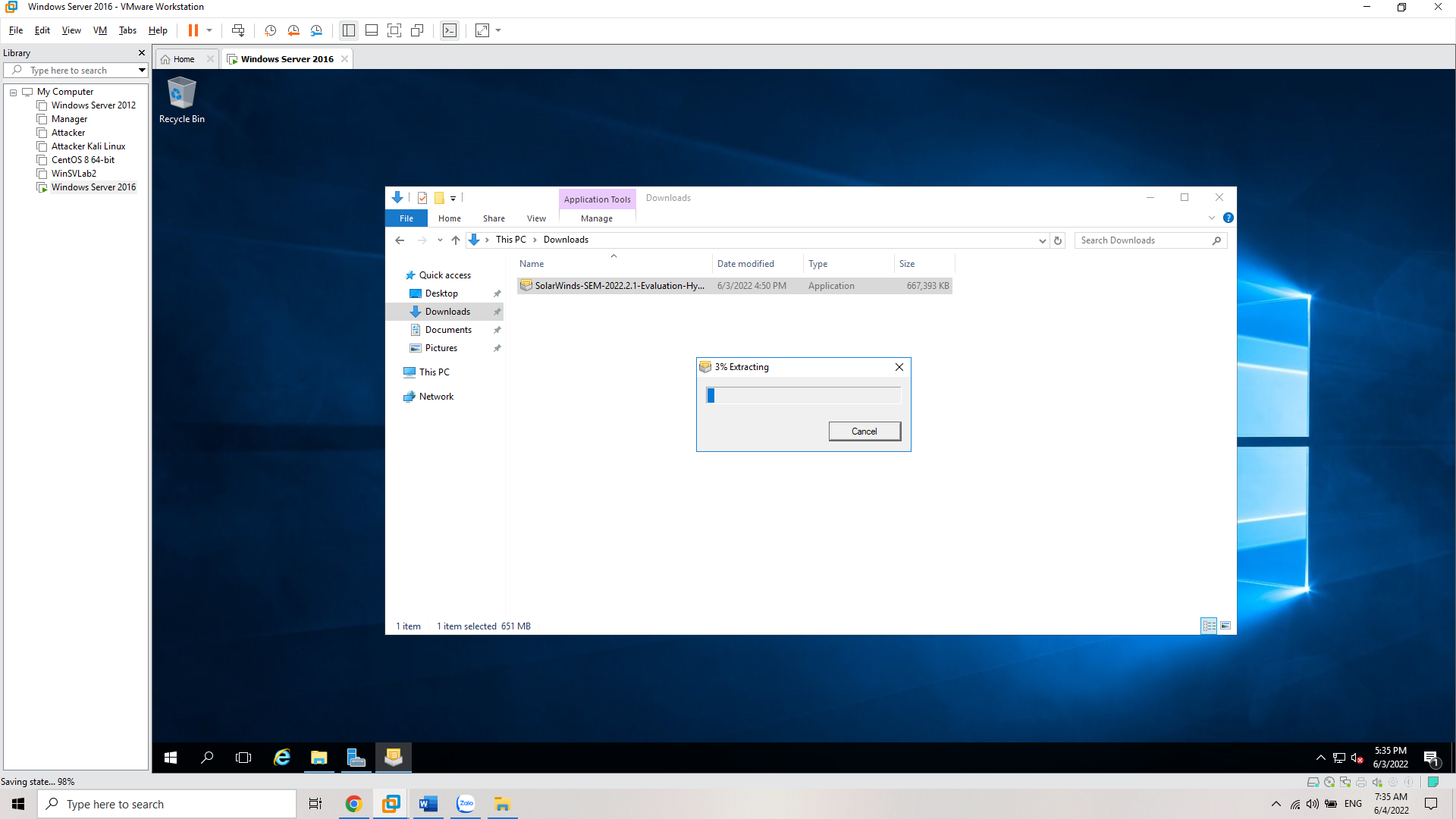
Hình 4: Cho phép máy chủ này gửi và nhận quá trình di chuyển trực tiếp của các máy ảo



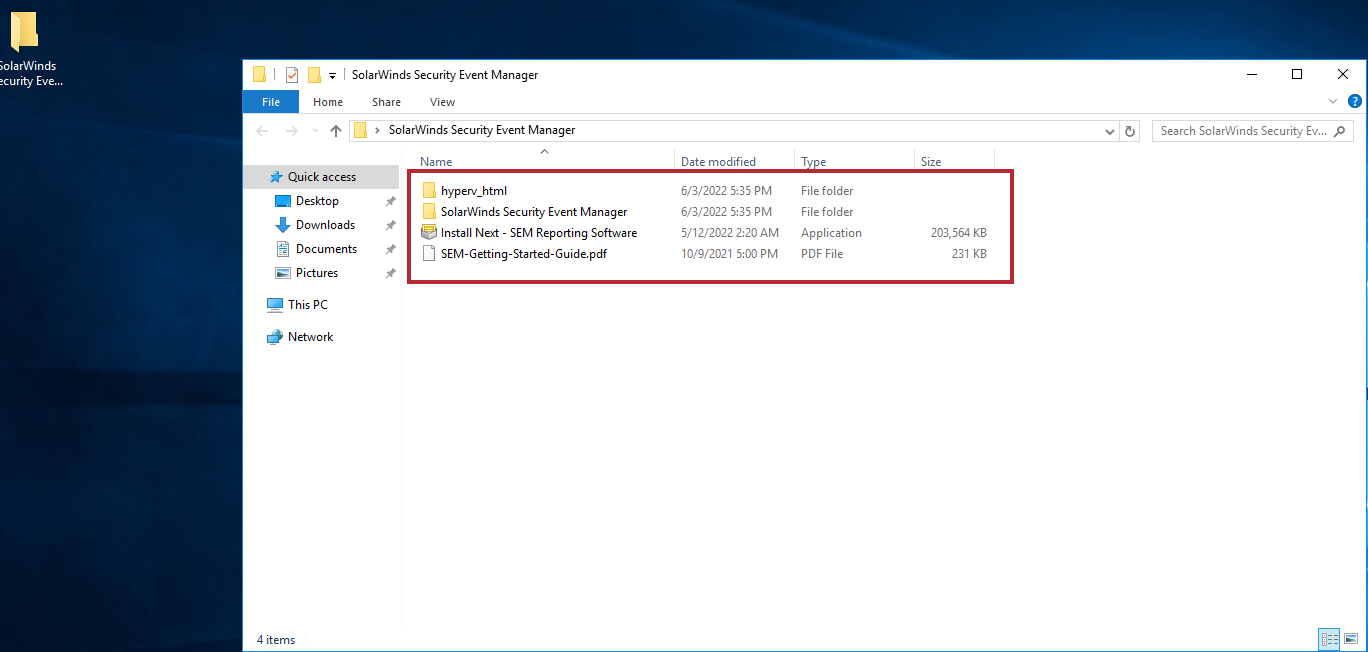
Hình 5: Chờ cài đặt



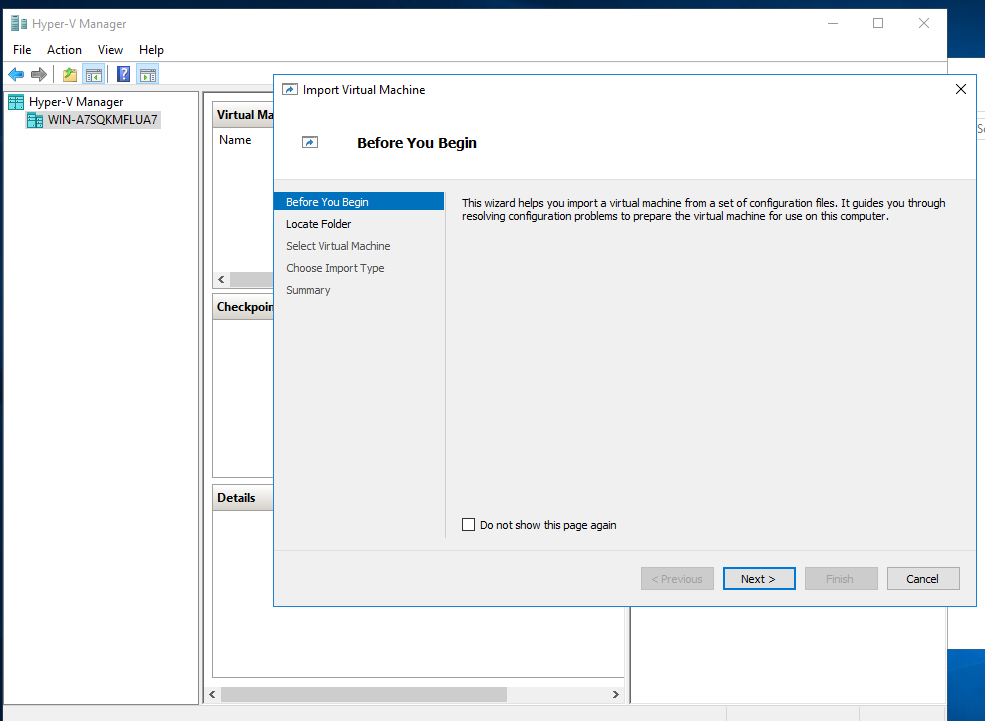
Hình 6: Tiến hành khởi động lại máy sau khi cài xong và mở Hyper-V



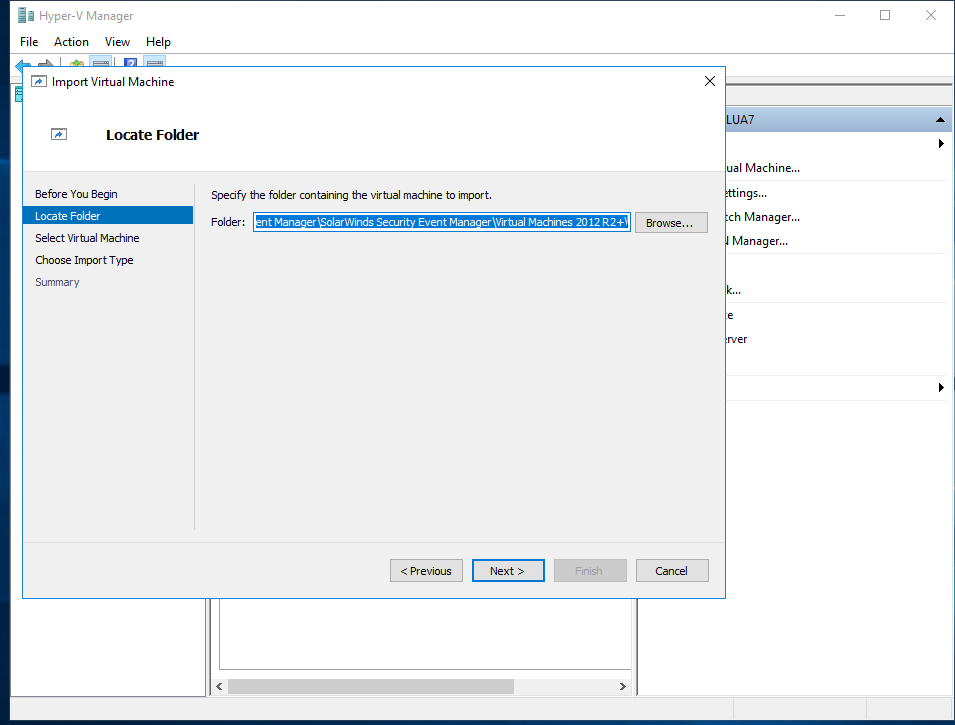
Hình 7: Cài đặt solarwinds SEM ta sẽ click vào để giải nén file này ra



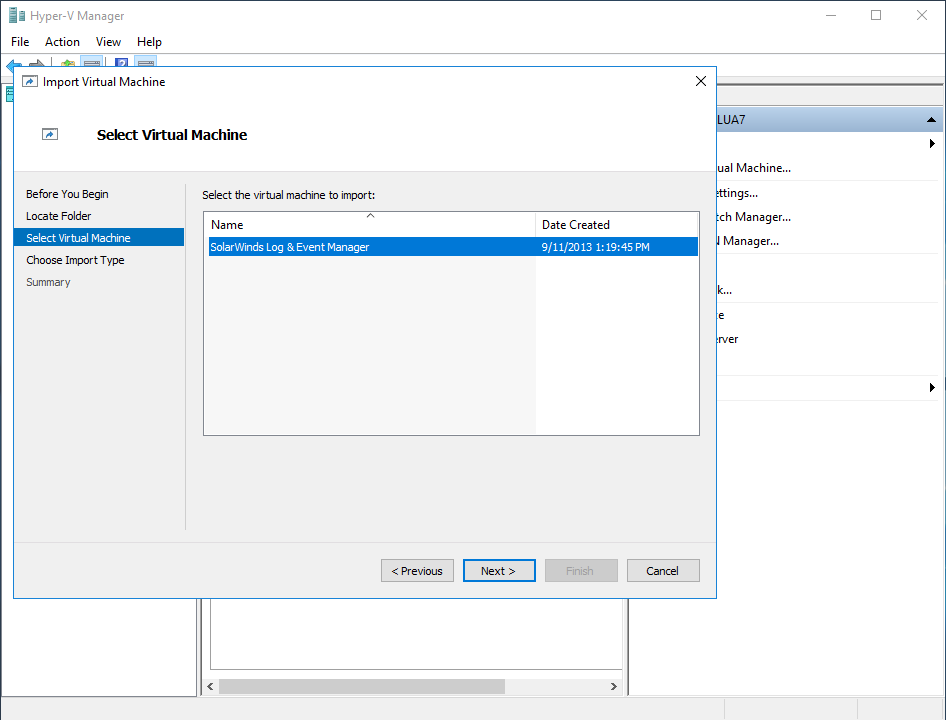
Hình 8: Sau khi giải nén xong ta có



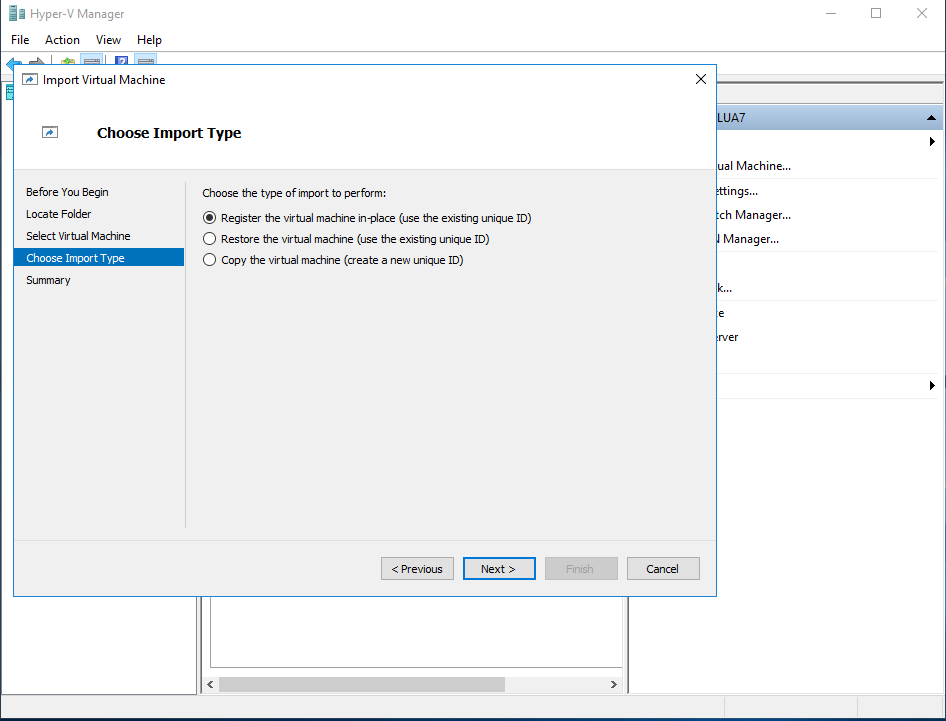
Hình 9: Ta sẽ import máy ảo vào solarwind bằng Hyper-V



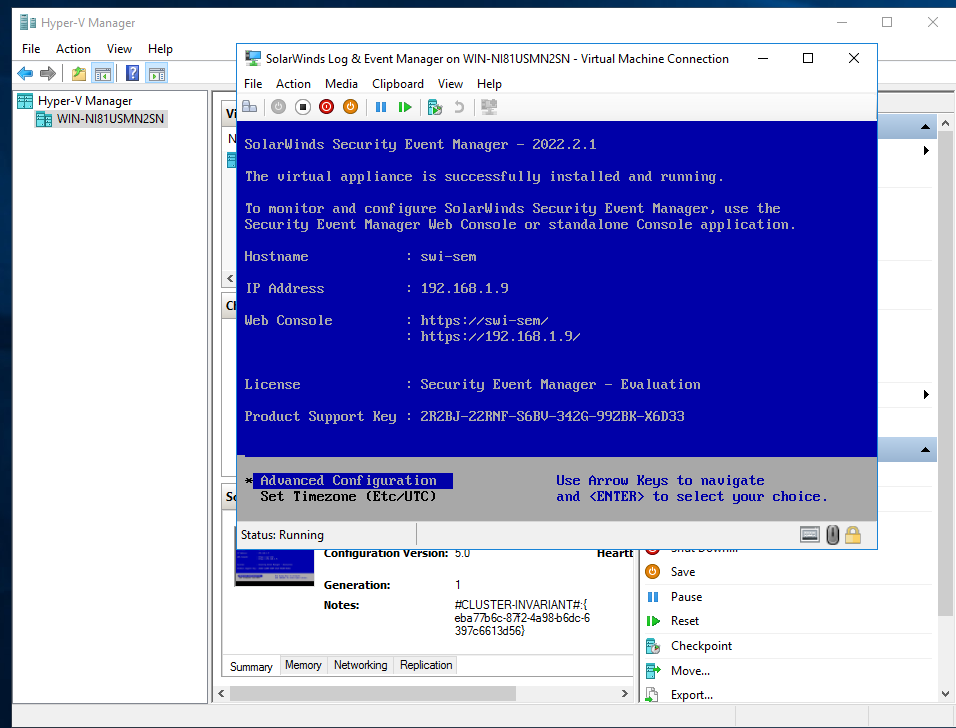
Hình 10: Vào kiếm file chứa máy ảo solarwinds



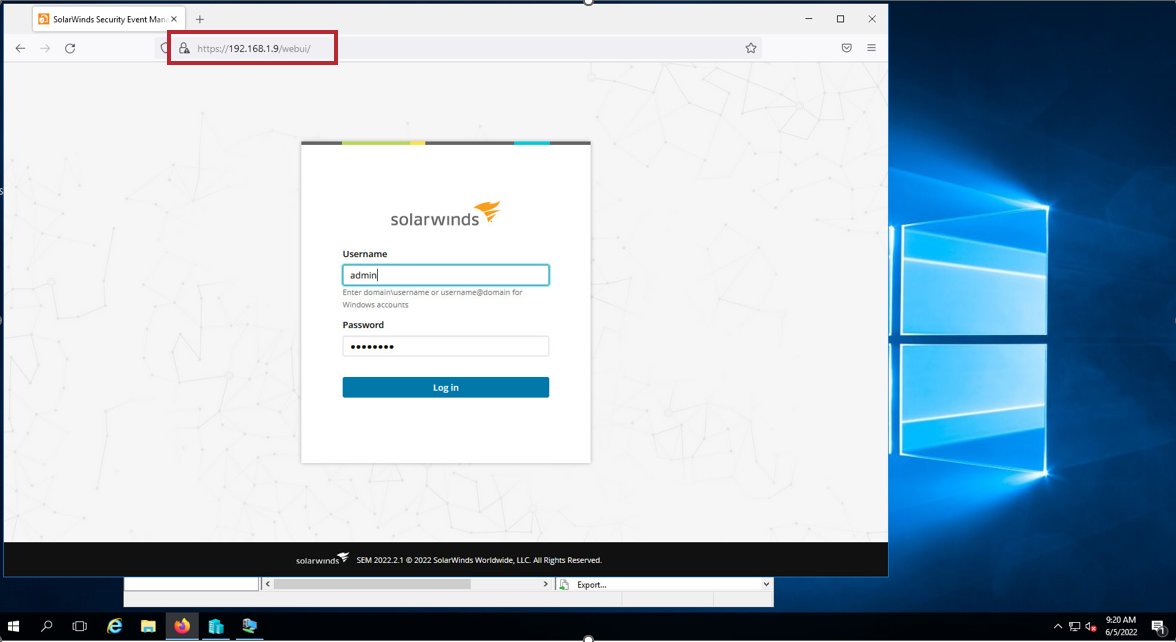
Hình 11: Tên máy tìm được khi chỏ đúng máy



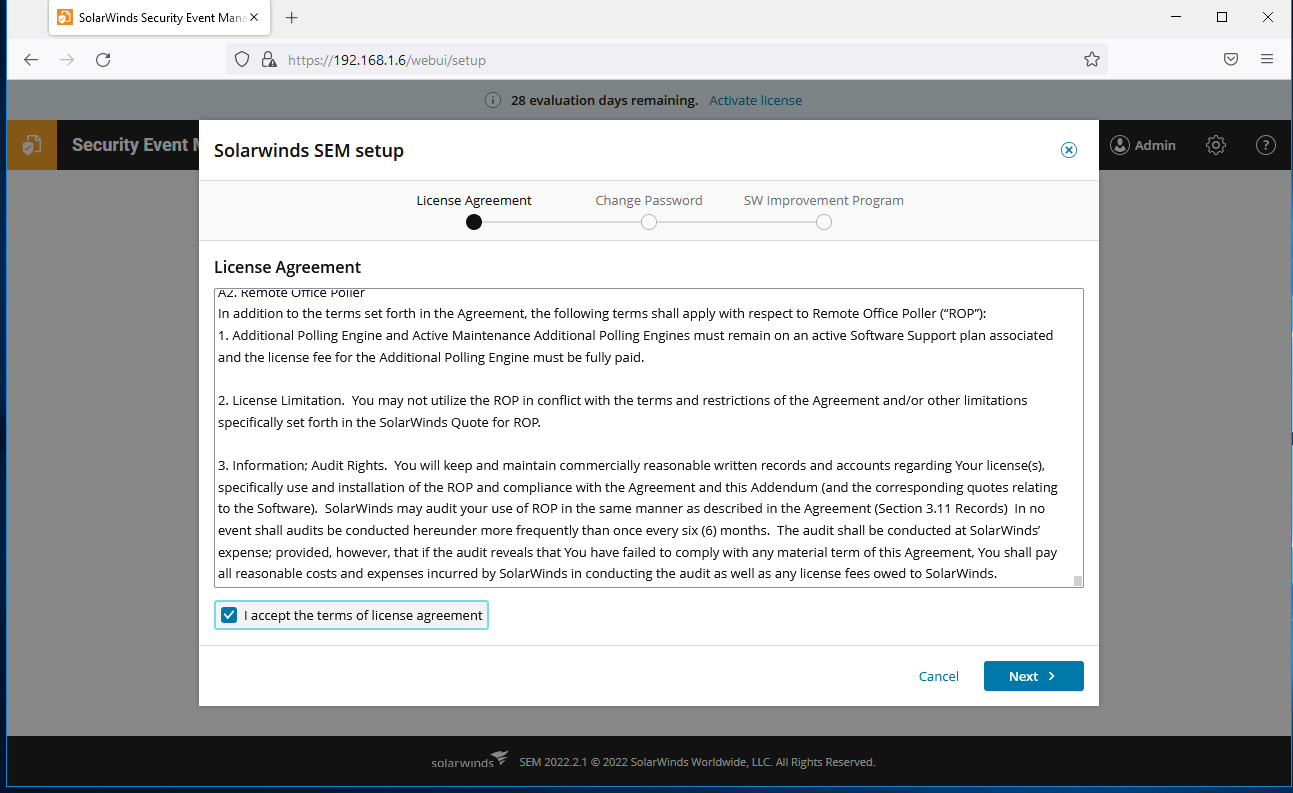
Hình 12: Chọn kiểu kiểu import



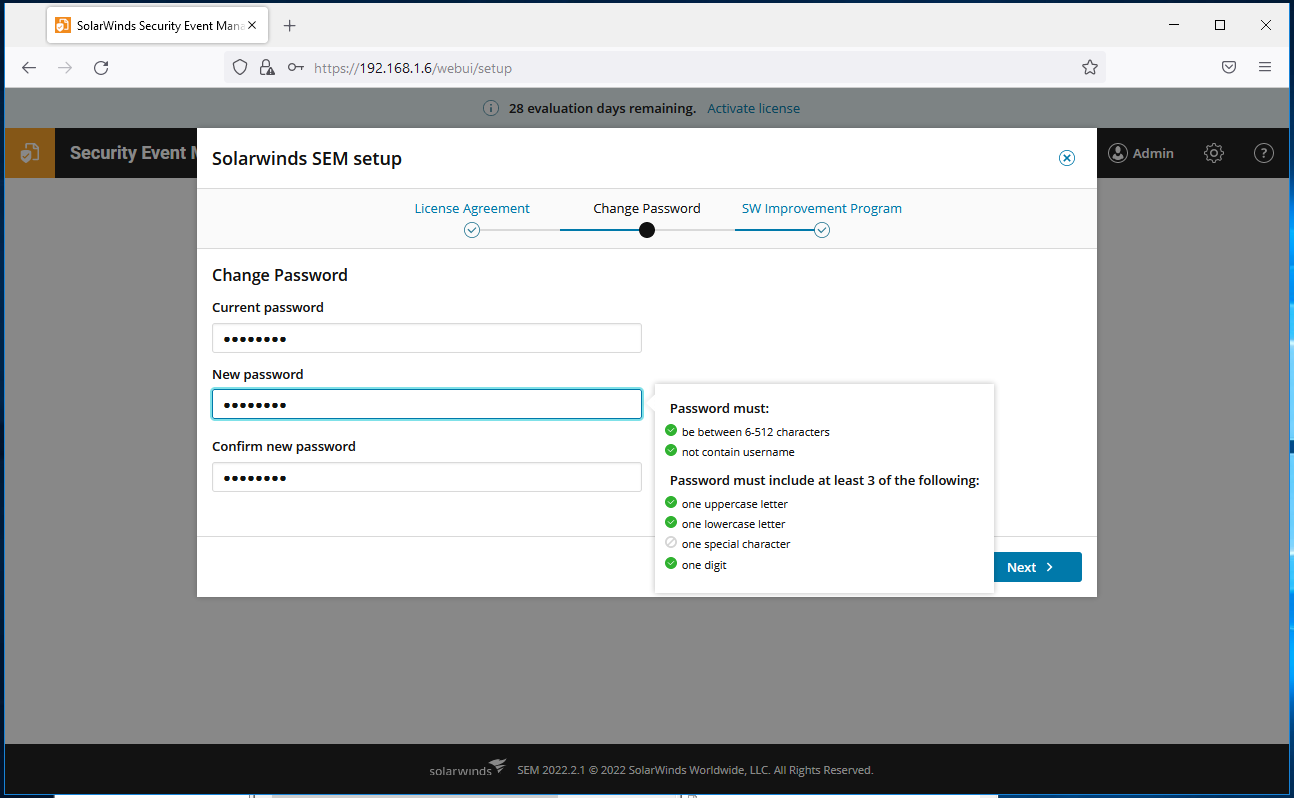
Hình 13: Mở máy ảo và tiến hành truy cập vào web để cấu hình



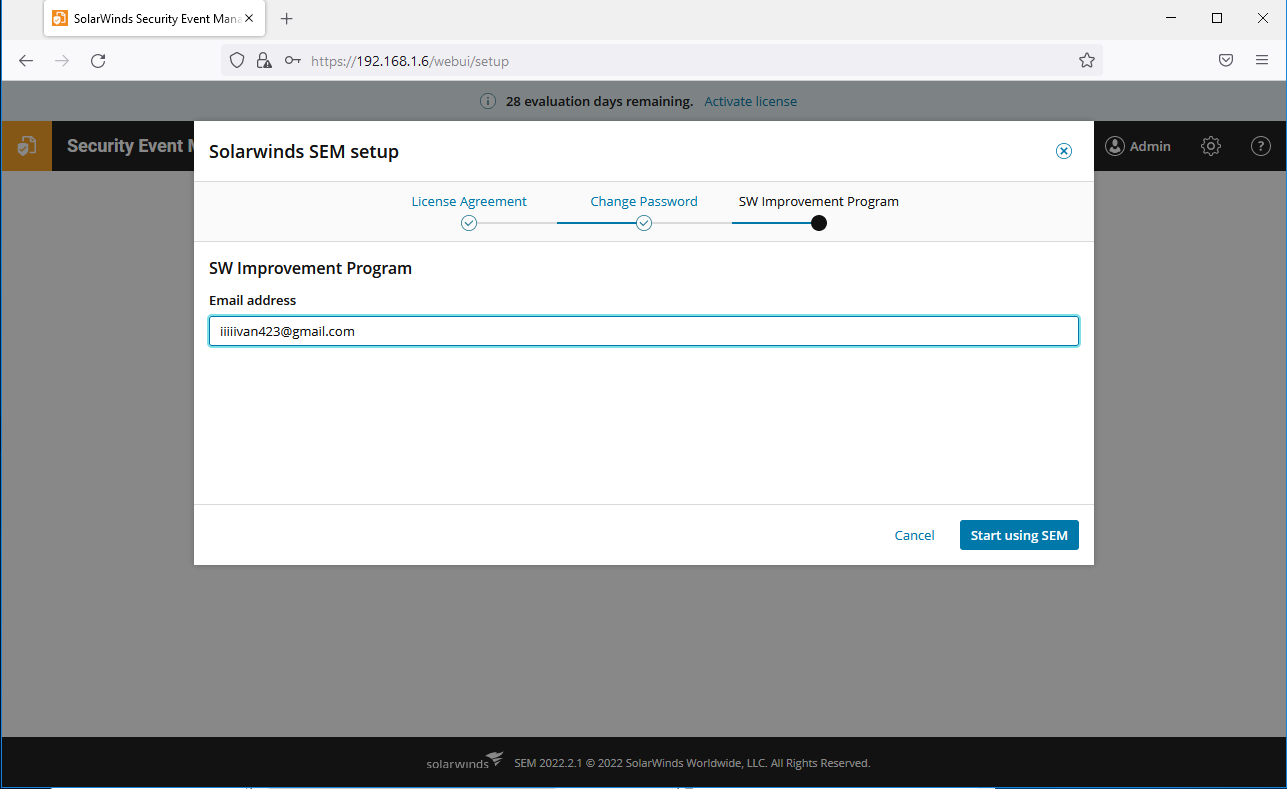
Hình 14: Truy cập web với địa chỉ 192.168.1.9 nhưng xài ip động



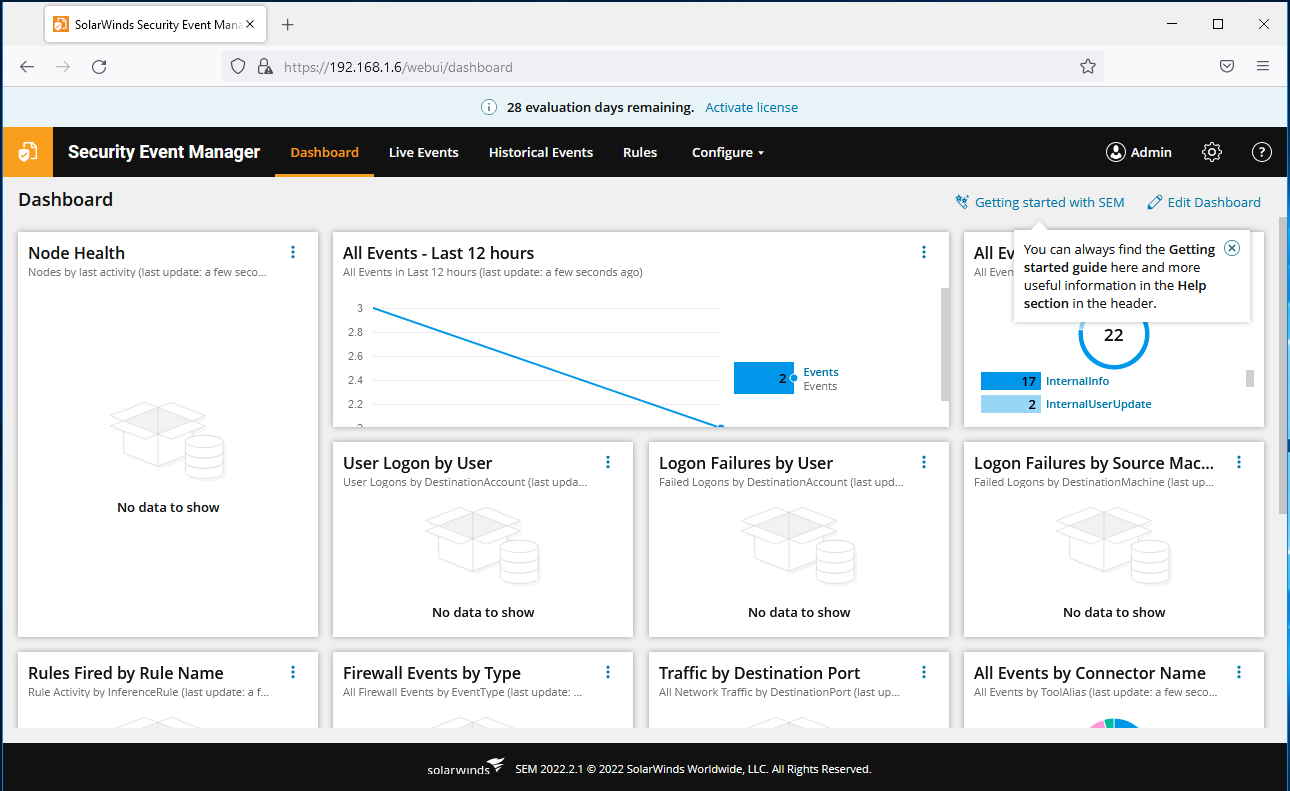
Hình 15: Thiết lập đồng ý với các license



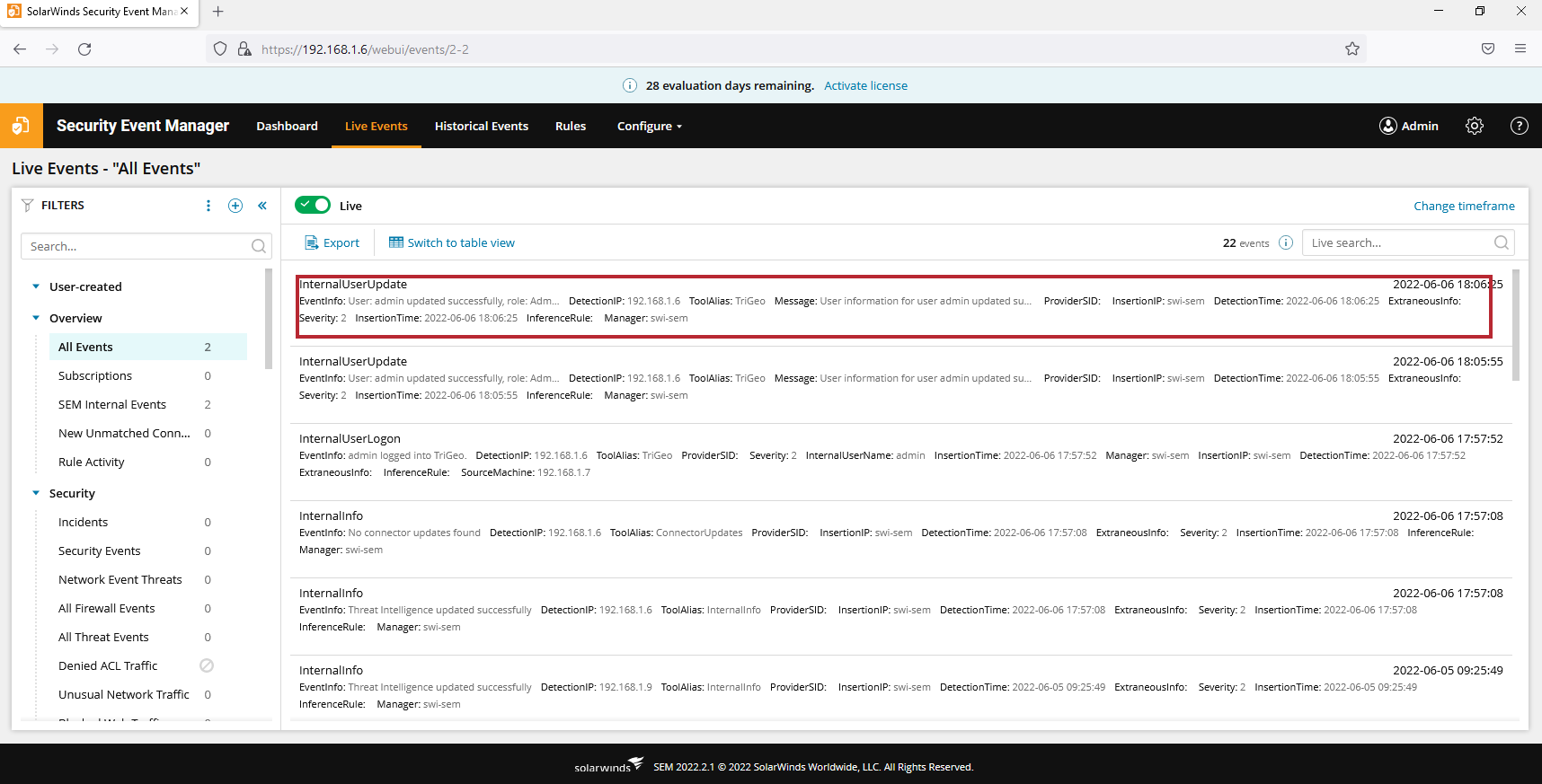
Hình 16: Thay đổi mật khẩu



Hình 17: Cài đặt gmail



Hình 18: Còn free 28 ngày



Hình 19: Vào phần event ta thấy nó ghi lại các sự kiện như vậy ta đã cấu hình xong