**Ngân Hàng**

**Tài Liệu Triển Khai**

**Hệ Thống Forescout**

|  |  |  |
| --- | --- | --- |
|  |  |  |

Thông tin phiên bản

|  |  |  |  |
| --- | --- | --- | --- |
| Dự án |  | | |
| Quản trị dự án |  | | |
| Người viết |  | Ngày |  |
| Người phê duyệt |  | Ngày |  |
| Phiên bản |  | Ngày ban hành |  |
| Tên file |  | | |

Phân phối tài liệu

| Chuyển tới | Ngày | Phone/Fax |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Lịch sử phiên bản

| Phiên bản | Ngày ban hành | Mô tả |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Xác nhận của các bên liên quan

|  |  |  |  |
| --- | --- | --- | --- |
| **Đại diện** | | **Đại diện** | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | |  | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | |  | |
|  | |  | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | |  | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**MỤC LỤC**

[Thông tin phiên bản 2](#_Toc56120264)

[Xác nhận của các bên liên quan 3](#_Toc56120265)

[1 Sơ đồ kết nối vật lý 6](#_Toc56120266)

[2 Sơ đồ kết nối logic 7](#_Toc56120267)

[3 Sơ đồ luồng dữ liệu 8](#_Toc56120268)

[4 Triển khai cài đặt chi tiết hệ thống Forescout 10](#_Toc56120269)

[4.1 Chuẩn bị môi trường VMware ESXi 10](#_Toc56120270)

[4.1.1 Cài đặt OS cho server CounterACT DC-NacACT-01 11](#_Toc56120271)

[4.1.2 Cài đặt OS cho server CounterACT DC-NacACT-02 30](#_Toc56120272)

[4.1.3 Cài đặt OS cho server quản trị Enterprise Manager DC-NacENT-01 50](#_Toc56120273)

[4.1.4 Đặt password cho tài khoản root 70](#_Toc56120274)

[4.2 Cài đặt cơ bản ban đầu 74](#_Toc56120275)

[4.3 Cài đặt High Availability (HA) 89](#_Toc56120276)

[4.4 Cài đặt channel (dùng cho SPAN) 94](#_Toc56120277)

[4.4.1 Chuẩn bị cấu hình SPAN 94](#_Toc56120278)

[4.4.2 Cấu hình SPAN 94](#_Toc56120279)

[4.4.3 Cấu hình Channel 95](#_Toc56120280)

[4.5 Cấu hình hình tích hợp switch 97](#_Toc56120281)

[4.6 Cài đặt HPS Inspection Engine 106](#_Toc56120282)

[4.7 Phân dải segment cho hệ thống 107](#_Toc56120283)

[4.8 Thiết lập Policy 113](#_Toc56120284)

[4.8.1 Phân loại các thiết bị trong hệ thống 113](#_Toc56120285)

[4.8.2 Phân loại hệ điều hành 135](#_Toc56120286)

[4.8.3 Phân loại cái thiết bị có join domain hay chưa 137](#_Toc56120287)

[4.8.4 Phân loại phiên bản hệ điều hành Windows 139](#_Toc56120288)

[4.8.5 Phân loại các thiết bị cài đặt Antivirus 140](#_Toc56120289)

[4.8.6 Phân loại các thiết bị tắt firewall local 142](#_Toc56120290)

[4.8.7 Phân loại các thiết bị cài đặt phần mềm lưu trữ Cloud Storage 143](#_Toc56120291)

[4.8.8 Phân loại các thiết bị cài đặt phần mềm nhắn tin Instant Messenger: 144](#_Toc56120292)

[4.8.9 Phân loại các thiết bị cập nhật Windows Update 146](#_Toc56120293)

[4.8.10 Thực thi chính sách thông báo đến các thiết bị không cài đặt Antivirus 148](#_Toc56120294)

[4.8.11 Thực thi chính sách thông báo đến các thiết bị chưa update Windows 150](#_Toc56120295)

[4.8.12 Thực thi chính sách thông báo đến các thiết bị bật Local Firewall 151](#_Toc56120296)

[4.8.13 Thực thi chính sách thông báo đến các thiết bị cài đặt ứng dụng blacklist như Google Drive, Dropbox và Zalo 152](#_Toc56120297)

[4.8.14 Thực thi chính sách block port đối với những thiết bị không cài đặt chương trình Antivirus 154](#_Toc56120298)

[4.8.15 Thực thi chính sách move VLAN 156](#_Toc56120299)

[4.8.16 Phân loại các thiết bị tồn tại lỗ hổng bảo mật WannaCry 157](#_Toc56120300)

[4.8.17 Phân loại các thiết bị tồn tại lỗ hổng bảo mật Spectre 159](#_Toc56120301)

[4.8.18 Phân loại các thiết bị tồn tại lỗ hổng bảo mật Meltdown 163](#_Toc56120302)

[4.9 Thiết lập Dashboard 168](#_Toc56120303)

[4.9.1 Dashboard panel BVB General 173](#_Toc56120304)

[4.9.2 Dashboard panel BVB Compliance 181](#_Toc56120305)

[4.9.3 Dashboard BVB Vulnerability 189](#_Toc56120306)

[4.10 Thiết lập report 194](#_Toc56120307)

[4.11 Export policy và segment 205](#_Toc56120308)

[4.11.1 Export policy 205](#_Toc56120309)

[4.11.2 Export segment 206](#_Toc56120310)

[4.12 Cấu hình bổ sung 208](#_Toc56120311)

[4.12.1 Cấu hình danh sách whitelisted IP 208](#_Toc56120312)

[4.12.2 Cấu hình tài khoản console 212](#_Toc56120313)

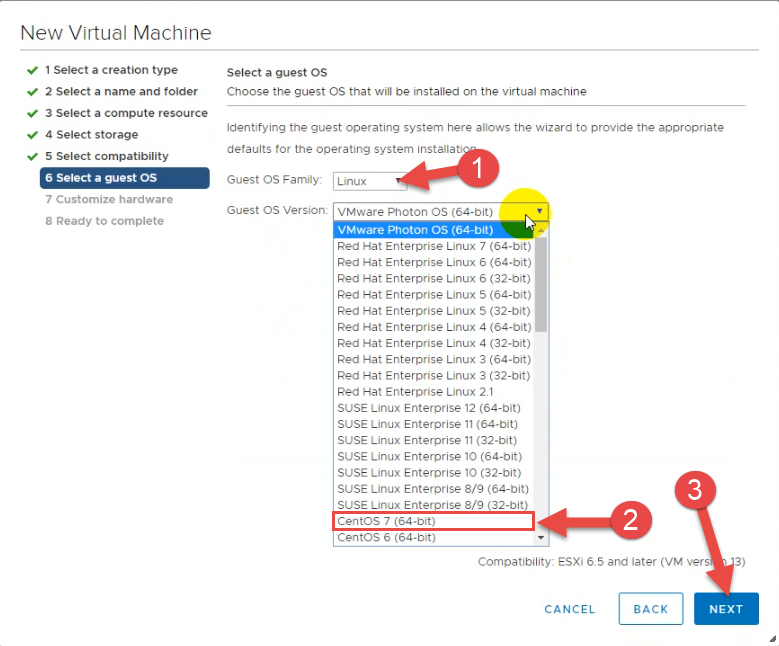
[4.12.3 Cấu hình Certification cho HTTPS Web 215](#_Toc56120314)

# 

### Cài đặt OS cho server quản trị Enterprise Manager

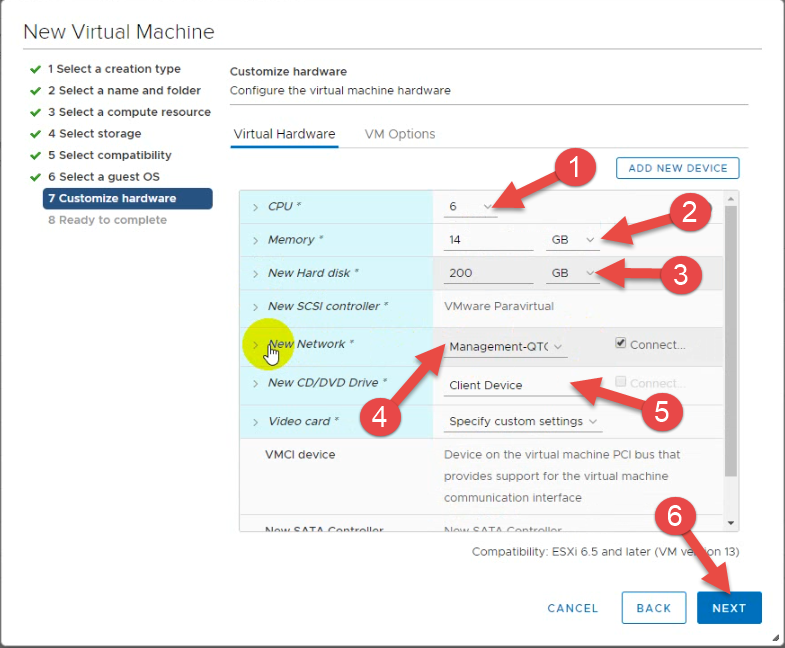
Ghi chú:

Phần **Guest OS Family** chọn Linux, phần **Version** chọn **CentOS 7 (64-bit)**

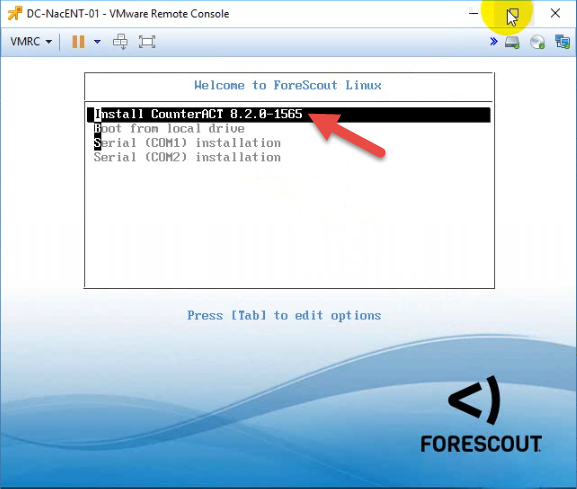


Thông số cấu hình sẽ chọn tương tự như bảng cấu hình định sẵn:

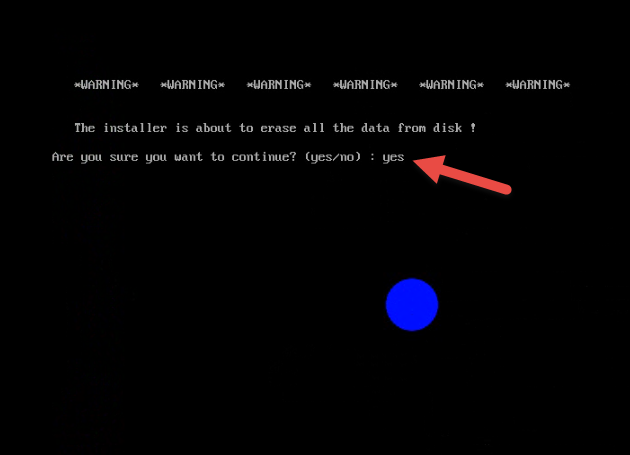
* CPU: 6
* Memory: 14 GB
* Hard disk: 200 GB
* 1 card mạng: Management
* CD/DVD: thêm vào file iso của Forescout



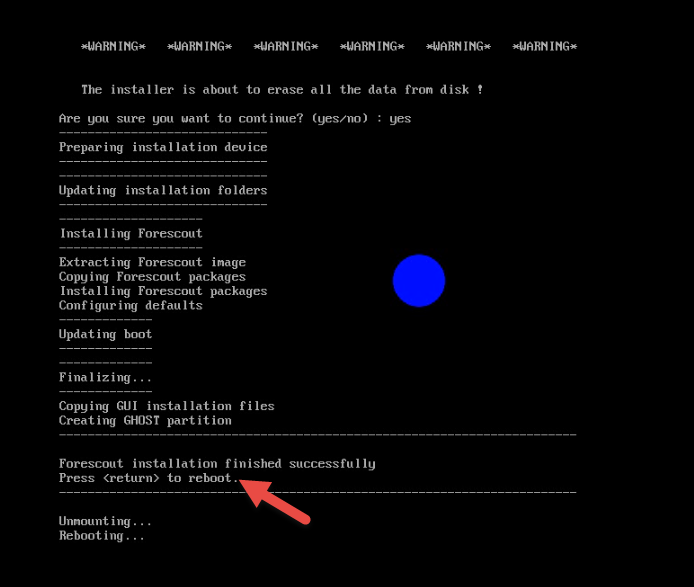
Sau khi tạo máy ảo, tiến hành khởi động máy lên. Màn hình hiển thị cài đặt OS sẽ hiển thị, chọn **Install CounterACT**



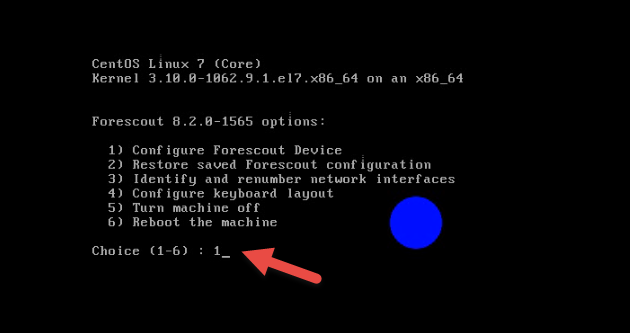
Nhập vào: yes



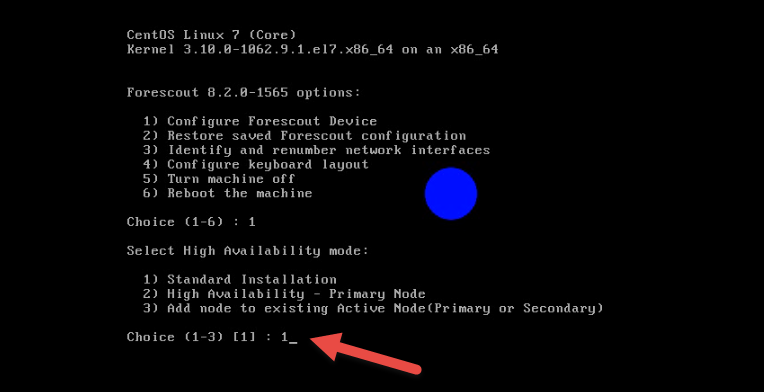
Chờ một vài phút để file cài đặt được giải nén, sau khi hoàn tất nhấn **Enter**:



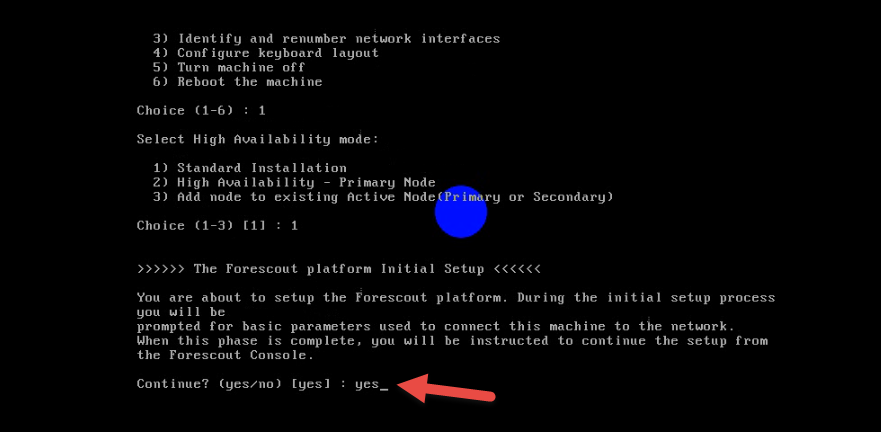
Chọn **Configure Forescout Device**, nhập vào tùy chọn: 1



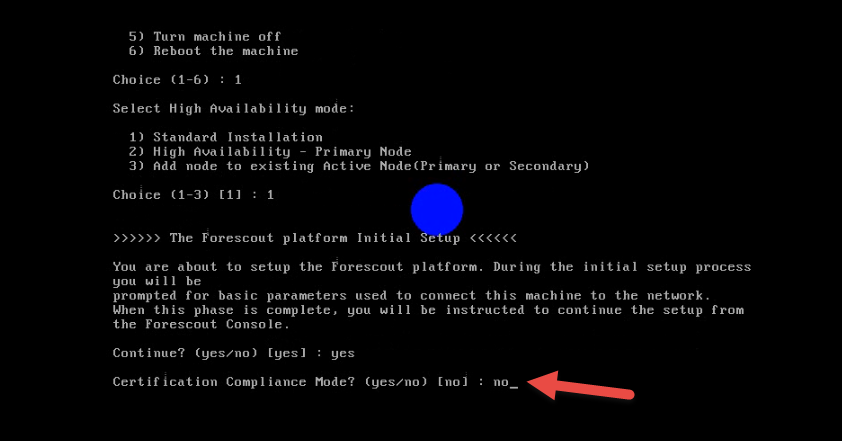
Chọn chế độ **Standard Installation**, nhập vào tùy chọn: 1



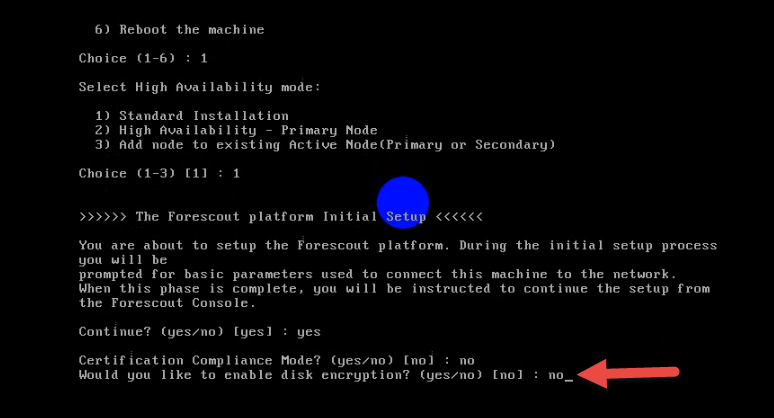
Xác nhận cài đặt, nhập vào: yes



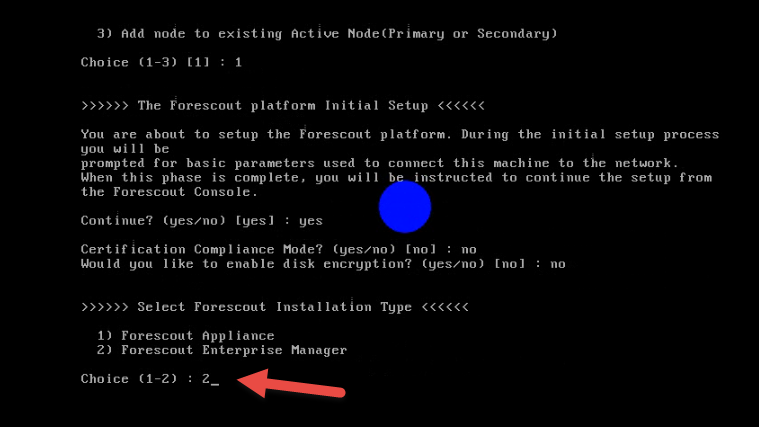
Nhập vào tùy chọn: no



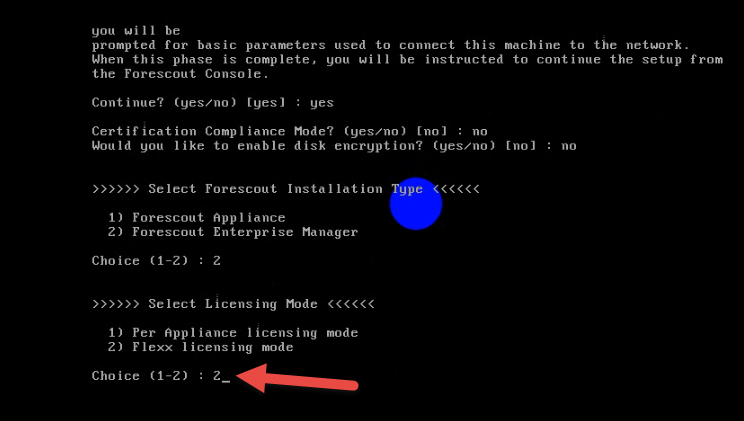
Tắt chế độ mã hóa ổ đĩa, nhập vào tùy chọn: no



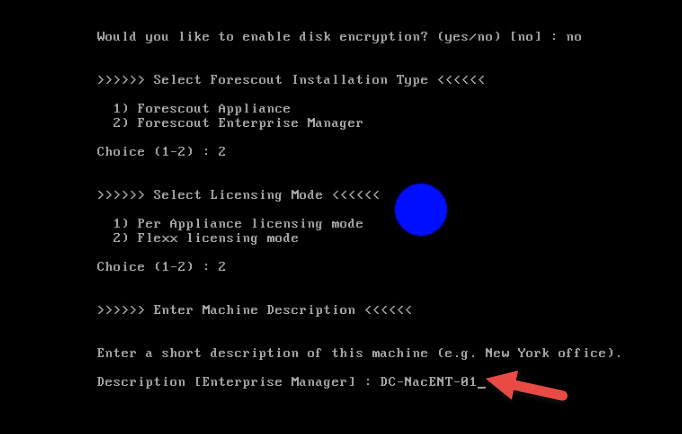
Chọn chế độ cài đặt **Forescout Enterprise Manager**, chọn tùy chọn: 2



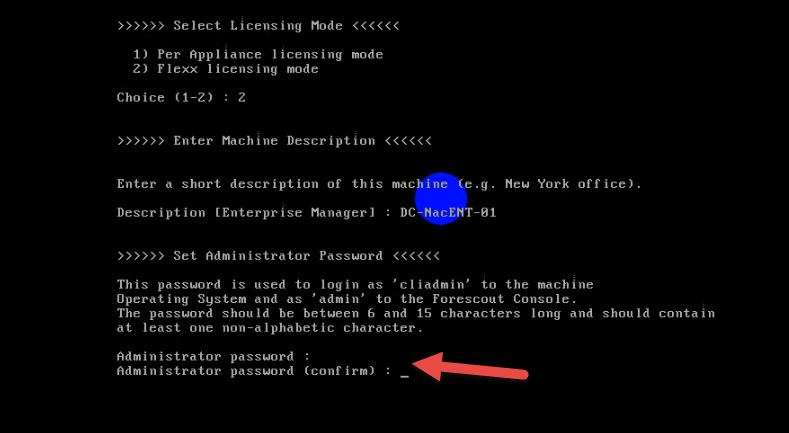
Chọn chế độ bản quyền **Flexx licensing mode**, nhập vào tùy chọn: 2



Nhập vào miêu tả: Nac-EM



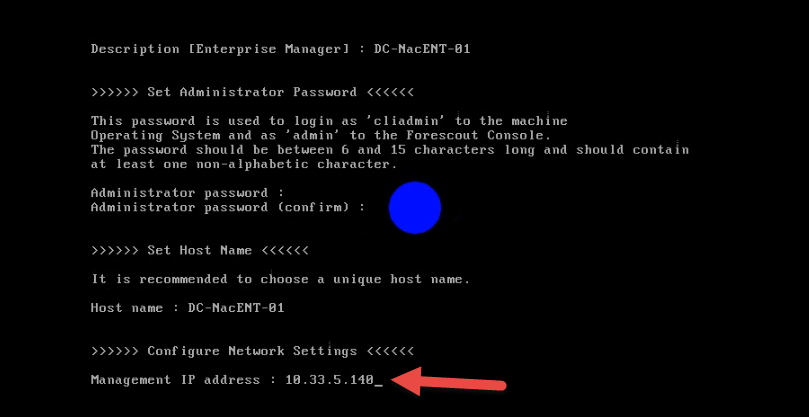
Nhập vào password, password được nhập vào sẽ được sử dụng chung cho tài khoản admin (dùng để đăng nhập vào giao diện console) và cliadmin (dùng để đăng nhập quản trị hệ điều hành CentOS 7):



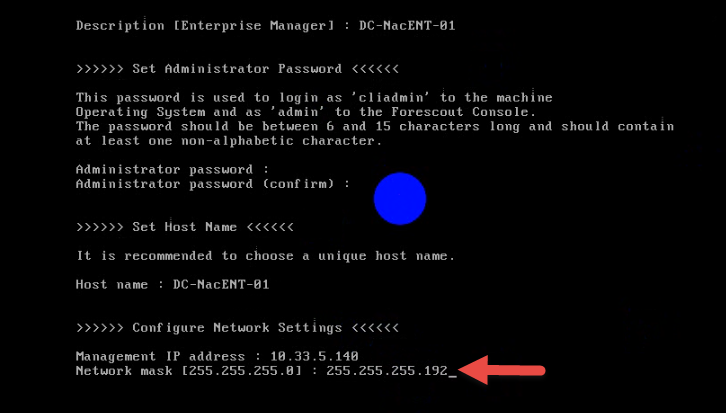
Nhập vào tên Host name: Nac-EM



Nhập vào IP quản trị: 10.68.61.34



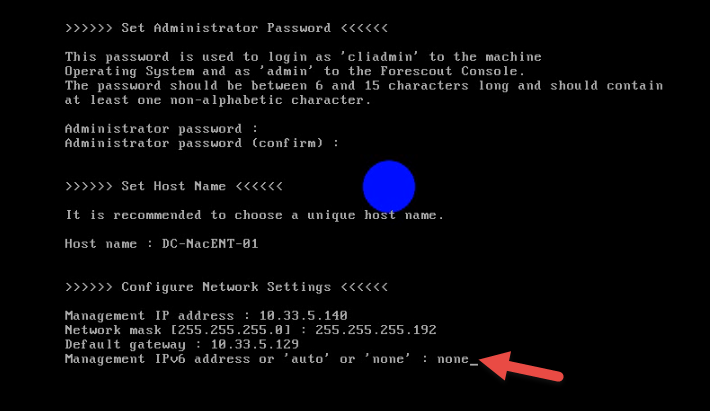
Nhập vào subnet mask : 255.255.255.0



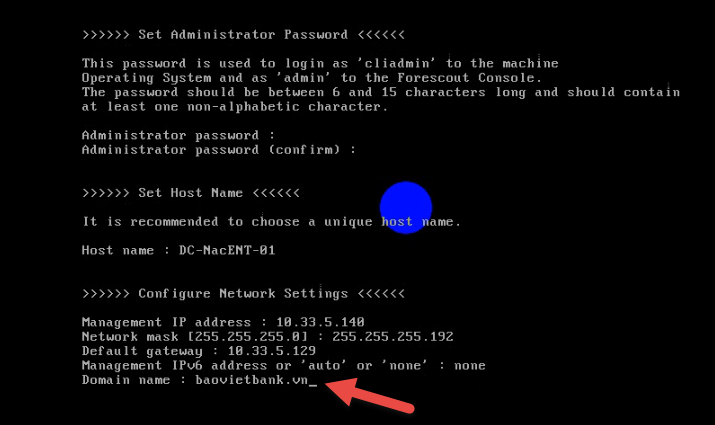
Nhập vào default gateway: 10.68.61.1



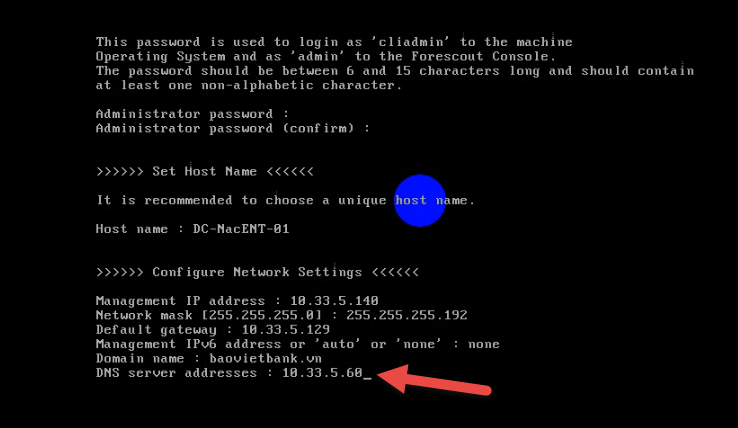
Tắt IPv6, nhập vào: none



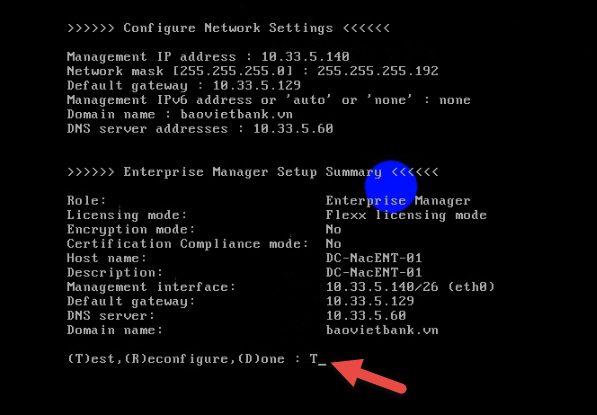
Nhập vào tên domain: pgbank.com.vn



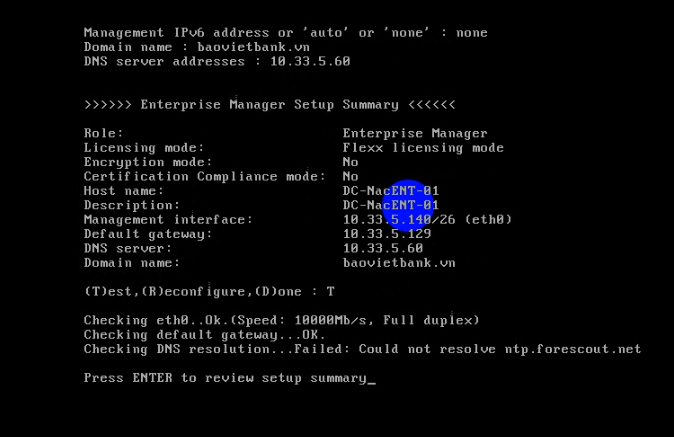
Nhập vào địa chỉ IP server DNS: 10.68.8.8 / 10.68.4.4



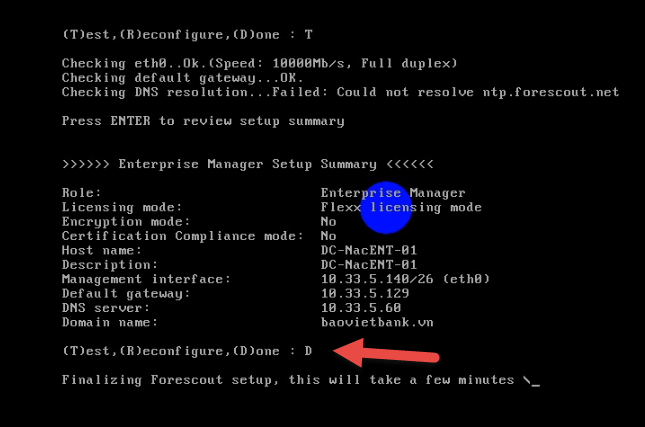
Để kiểm tra lại các kết nối đã thông suốt hay chưa, nhập vào tùy chọn: T



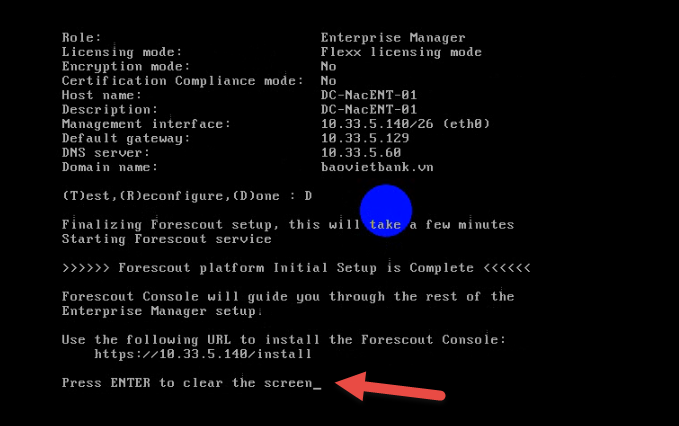
Bảng hiển thị kết quả đã thông suốt kết nối tới default gateway (có thể bỏ qua kết quả check DNS, vì DNS server hiện tại không cho phân giải IP ở ngoài Internet), nhấn **Enter** để xác nhận:



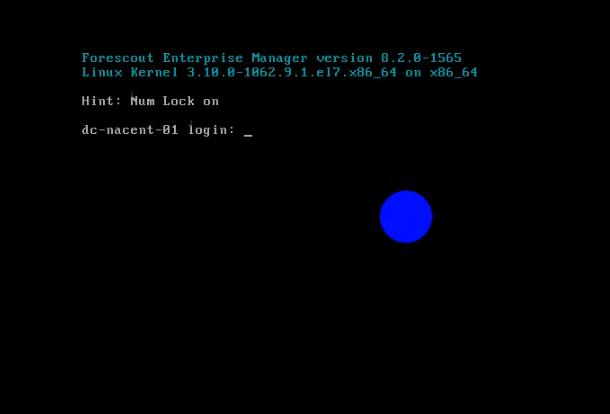
Để xác nhận bắt đầu quá trình cài đặt, nhập vào tùy chọn: D



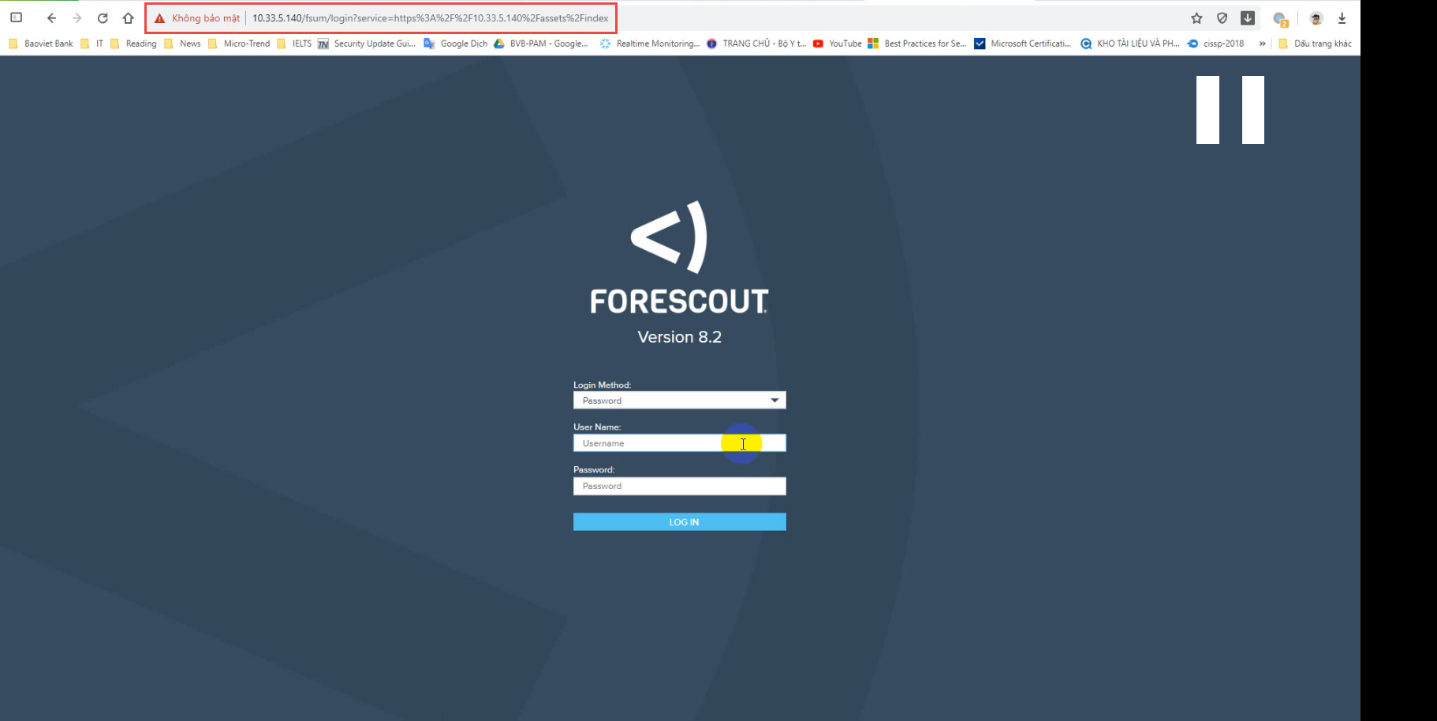
Chờ một vài phút để cho tiến trình cài đặt được diễn ra thành công, sau đó nhấn **Enter**:



Giao diện hiển thị đăng nhập:

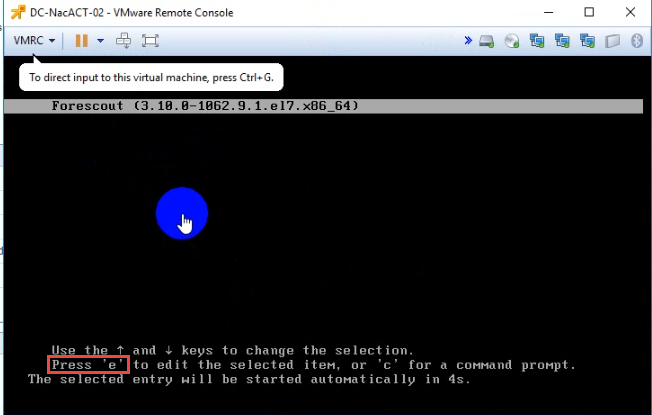


Mở trình duyệt lên và truy cập vào giao diện quản trị: **https://x.x.x.x**

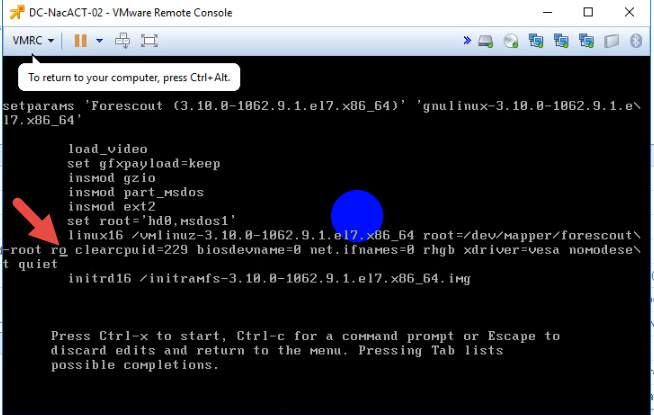


### Đặt password cho tài khoản root

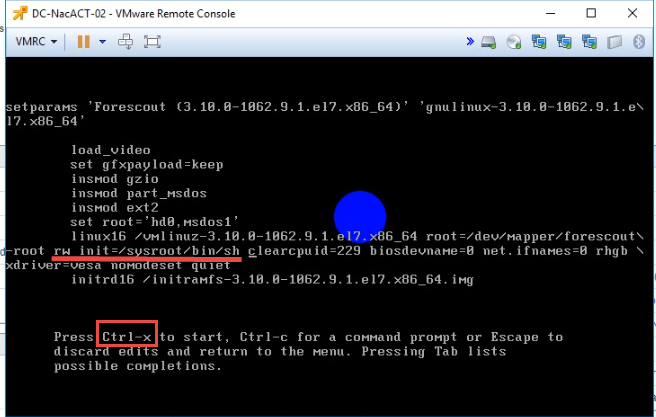
Để đặt password cho tài khoản root của máy chủ, ta khởi động lại máy, ngay tại giao diện chọn OS để khởi động, trong vòng 5 giây nhanh tay nhấn: E



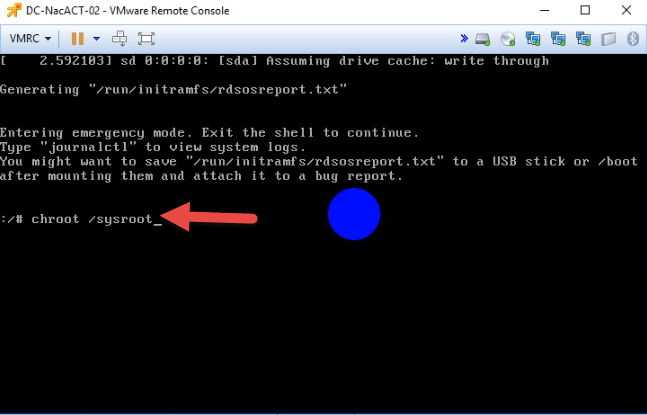
Đưa trỏ chuột đến phần: -root ro



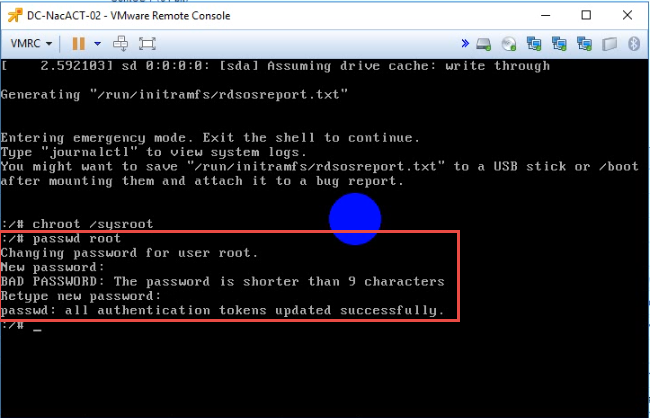
Đổi thành **-root rw init=/sysroot/bin/sh**. Sau đó nhấn tổ hợp phím **Ctrl + X** để bắt đầu:



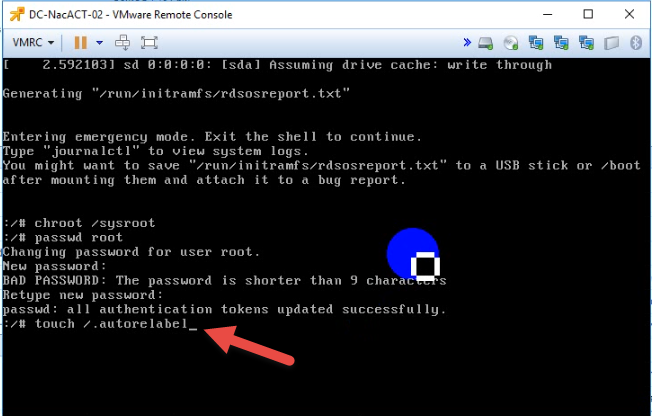
Nhập vào: **chroot /sysroot**



Nhập vào mật khẩu cho tài khoản root:



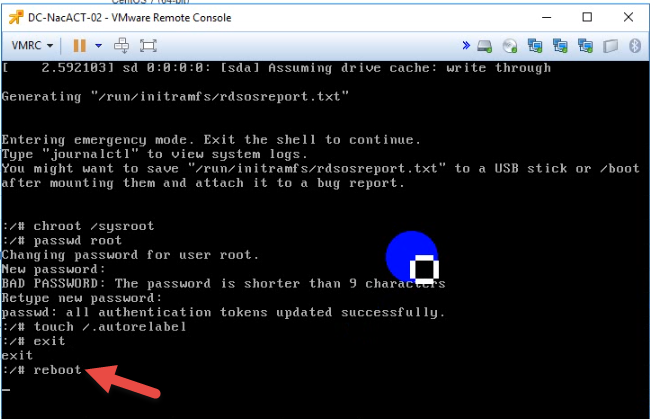
Nhập vào: **touch /.autorelabel**



Nhập vào: **exit**



Khởi động lại thiết bị, nhập vào: **reboot**



Thiết bị khởi động cho đến màn hình đăng nhập, nhập vào tài khoản root để kiểm tra:

