**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HƯỚNG DẪN BỘ TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT ĐỂ
ĐÁNH GIÁ VÀ LỰA CHỌN NỀN TẢNG ĐIỆN TOÁN ĐÁM MÂY PHỤC VỤ CHÍNH PHỦ ĐIỆN TỬ/CHÍNH QUYỀN ĐIỆN TỬ**

(*Kèm theo Công văn số /BTTTT-CATTT ngày tháng 3 năm 2020
của Bộ Thông tin và Truyền thông)*

**Hà Nội, 2020**

CHƯƠNG 1
PHẠM VI, ĐỐI TƯỢNG ÁP DỤNG

# 1.1. Phạm vi áp dụng

Tài liệu hướng dẫn này đưa ra các tiêu chí, chỉ tiêu kỹ thuật để đánh giá, lựa chọn giải pháp nền tảng điện toán đám mây. Căn cứ vào các tiêu chí, chỉ tiêu kỹ thuật này, cơ quan, tổ chức nhà nước có cơ sở để đánh giá, lựa chọn giải pháp hoặc thuê dịch vụ điện toán đám mây (sau đây viết tắt là ĐTĐM) phục vụ phát triển Chính phủ điện tử/Chính quyền điện tử (CPĐT/CQĐT).

# 1.2. Đối tượng áp dụng

a) Các cơ quan, tổ chức nhà nước xây dựng, triển khai giải pháp nền tảng điện toán đám mây phục vụ CPĐT/CQĐT.

b) Doanh nghiệp cung cấp giải pháp, dịch vụ nền tảng điện toán đám mây phục vụ CPĐT/CQĐT.

c) Khuyến khích cơ quan, tổ chức khác tham khảo xây dựng, triển khai giải pháp nền tảng điện toán đám mây.

1.3. Thuật ngữ, định nghĩa

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Từ****viết tắt** | **Thuật ngữ tiếng Anh** | **Thuật ngữ tiếng Việt** |
| 1 | CPU | Central Processing Unit | Bộ xử lý trung tâm |
| 2 | API | Application Programming Interface | Giao diện lập trình ứng dụng |
| 3 | BCP | Business Continuity Plan | Kế hoạch duy trì hoạt động kinh doanh |
| 4 | CaaS | Communications as a Service | Giao tiếp như dịch vụ |
| 5 | CPU | Central Processing Unit | Khối xử lý trung tâm |
| 6 | IOPS | Input/output operations per second | Đơn vị đo hiệu năng xử lý vào ra cho thiết bị lưu trữ |
| 7 | SPAN | Switched Port Analyzer | Tính năng phân tích lưu lượng mạng tại cổng Switch |
| 8 | DNS | Domain Name System | Hệ thống tên miền |
| 9 | ETS | Emergency Telecommunications Service | Dịch vụ truyền thông khẩn cấp |
| 10 | I/O | Input/Output | Cổng vào/ra |
| 11 | IaaS | Infrastructure as a Service | Dịch vụ điện toán đám mây cung cấp cơ sở hạ tầng |
| 12 | IAM | Identity and Access Management | Quản lý định danh và truy cập |
| 13 | ICT | Information and Communication Technology | Công nghệ thông tin và Truyền thông |
| 14 | IP | Internet Protocol | Giao thức Internet |
| 15 | iSCSI | Internet Small Computer System Interface | Giao diện hệ thống máy tính nhỏ kết nối Internet |
| 16 | IT | Information Technology | Công nghệ thông tin |
| 17 | LAN | Local Area Network | Mạng cục bộ |
| 18 | NaaS | Network as a Service | Mạng như dịch vụ |
| 19 | NAS | Network Attached Storage | Thiết bị lưu trữ kết nối mạng |
| 20 | TLS | Transport Layer Security | Giao thức bảo mật tầng giao vận |
| 21 | NTP | Network Time Protocol | Giao thức đồng bộ thời gian mạng |
| 22 | OS | Operating System | Hệ điều hành |
| 23 | PaaS | Platform as a Service | Dịch vụ điện toán đám mây cung cấp dịch vụ nền tảng |
| 24 | SaaS | Software as a Service | Dịch vụ điện toán đám mây cung cấp dịch vụ phần mềm |
| 25 | RSPAN | Remote Switched Port Analyzer | Tính năng phân tích lưu lượng mạng tại cổng Switch từ xa |

1.4. Tài liệu tham khảo

|  |  |
| --- | --- |
| 1 | ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services (*ISO/IEC 27017:2015* *Công nghệ thông tin – Các kỹ thuật an toàn - Quy phạm thực hành kiểm soát bảo mật thông tin dựa trên ISO/IEC 27002 dành cho dịch vụ đám mây*) |
| 2 | ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (*ISO/IEC 27018:2019* *Công nghệ thông tin – Các kỹ thuật an toàn - Quy phạm thực hành bảo vệ thông tin có thể định danh cá nhân (PII) trên đám mây công cộng có chức năng xử lý PII*) |
| 3 | ISO/IEC 20000-9:2015 Information technology — Service management — Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services (*ISO/IEC 20000-9:2015* *Công nghệ thông tin – Quản lý dịch vụ - Phần 9: Hướng dẫn áp dụng tiêu chuẩn* *ISO/IEC 20000-1 cho dịch vụ điện toán đám mây)* |
| 4 | ISO/IEC 19086-1:2016 Information technology — Cloud computing — Service level agreement (SLA) framework — Part 1: Overview and concepts (*ISO/IEC 19086-1:2016* *Công nghệ thông tin – Điện toán đám mây – Khung thỏa thuận mức dịch vụ - Phần 1: Tổng quan và các khái niệm)* |
| 5 | TCVN ISO 22301:2018 (ISO/IEC 22301:2012) An ninh xã hội - Hệ thống quản lý kinh doanh liên tục - Các yêu cầu |
| 6 | TCVN ISO/IEC 27001:2018 Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Các yêu cầu |
| 7 | NIST 800-171 Revision 1 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (*NIST 800-171 Sửa đổi 1 Bảo vệ thông tin chưa được kiểm soát của các hệ thống thông tin và tổ chức không thuộc khối Chính phủ*) |
| 8 | ITU Y.3500-Y.3999 Cloud Computing (*ITU Y.3500-Y.3999 Điện toán đám mây)* |

# 1.5. Bộ tiêu chí, chỉ tiêu kỹ thuật đánh giá nền tảng ĐTĐM

Tài liệu này đưa ra bộ tiêu chí, chỉ tiêu kỹ thuật để đánh giá, lựa chọn nền tảng ĐTĐM bao gồm các tiêu chí, chỉ tiêu kỹ thuật và an toàn thông tin.

Các tiêu chí, chỉ tiêu kỹ thuật được mô tả tại Chương 3 tài liệu này, bao gồm các nhóm tính năng liên quan đến: (1) Máy ảo, (2) Thiết bị lưu trữ, (3) Mạng và mạng định nghĩa bằng phần mềm, (4) Máy vật lý, (5) Quản trị và vận hành, (6) Tích hợp và các yêu cầu khác liên quan.

Các tiêu chí, chỉ tiêu kỹ thuật an toàn thông tin được mô tả tại Chương 4 tài liệu này, bao gồm yêu cầu liên quan đến: (1) Yêu cầu cơ bản về tính năng an toàn thông tin, (2) Yêu cầu thiết lập cấu hình bảo mật cho cơ sở hạ tầng điện toán đám mây.

Cơ quan, tổ chức có thể sử dụng bộ tiêu chí, chỉ tiêu kỹ thuật này để xây dựng các yêu cầu kỹ thuật trong việc đánh giá, lựa chọn bên cung cấp dịch vụ ĐTĐM hoặc triển khai xây dựng hạ tầng ĐTĐM.

Đối với doanh nghiệp cung cấp dịch vụ ĐTĐM căn cứ vào bộ tiêu chí, chỉ tiêu kỹ thuật này để đánh giá khả năng đáp ứng các yêu cầu đối với hệ thống của mình, trên cơ sở đó đề xuất Bộ Thông tin và Truyền thống đánh giá làm cơ sở khuyến nghị cơ quan, tổ chức sử dụng dịch vụ.

 Bộ tiêu chí, chỉ tiêu kỹ thuật này phù hợp để đánh giá các mô hình ĐTĐM được mô tả tại Mục 2.2 và 2.3 tài liệu này.

CHƯƠNG 2
TỔNG QUAN VỀ NỀN TẢNG ĐIỆN TOÁN ĐÁM MÂY

# 2.1. Khái niệm điện toán đám mây

a) Điện toán đám mây là mô hình dịch vụ cho phép sử dụng tài nguyên điện toán dùng chung (mạng, máy chủ, lưu trữ, ứng dụng, dịch vụ) thông qua kết nối mạng. Tài nguyên điện toán đám mây này có thể được thiết lập hoặc hủy bỏ bởi người dùng mà không cần sự can thiệp của Nhà cung cấp dịch vụ.

b) Đặc điểm cơ bản của ĐTĐM:

- *Tự phục vụ theo yêu cầu* (On-demand self-service): Cho phép người dùng đưa ra các yêu cầu đối với hệ thống để đáp ứng nhu cầu sử dụng của mình như: thời gian sử dụng máy chủ, tài nguyên hệ thống và chính sách truy cập mạng...

- *Truy cập mạng diện rộng* (Broad network access): Cho phép truy cập, quản lý và sử dụng dịch vụ qua kết nối mạng.

- *Dùng chung tài nguyên và không phụ thuộc vị trí vật lý*: Tài nguyên của nhà cung cấp dịch vụ được dùng chung, phục vụ cho nhiều người dùng (mô hình multi-tenant). Mô hình này cho phép tài nguyên phần cứng và tài nguyên ảo hóa được cấp phát theo nhu cầu của người dùng mà không phụ thuộc vào vị trí vật lý.

- *Khả năng đáp ứng yêu cầu thay đổi nhanh chóng*(Rapid elasticity): Khả năng này cho phép thay đổi hệ thống một cách nhanh chóng theo nhu cầu của người sử dụng. Khả năng này cho phép nhà cung cấp sử dụng tài nguyên hiệu quả, tận dụng triệt để tài nguyên dư thừa, phục vụ được nhiều người sử dụng. Đối với người sử dụng dịch vụ, thì khả năng này giúp họ giảm chi phí khi sử dụng.

- *Kiểm soát dịch vụ**(*Measured service): Hệ thống điện toán đám mây có khả năng tự điều khiển và tinh chỉnh tài nguyên sử dụng bằng cách áp dụng các biện pháp kiểm soát cho từng loại dịch vụ. Tài nguyên sử dụng được giám sát, kiểm soát cho phép tính toán tài nguyên thực sự mà người dùng sử dụng nhằm tối ưu tài nguyên hệ thống.

# 2.2. Phân loại một số phương pháp triển khai ĐTĐM



*Hình 1 –Các mô hình triển khai điện toán đám mây*

a) ĐTĐM công cộng (Public Cloud): Đây là hạ tầng ĐTĐM được dùng cho tất cả các khách hàng trên hạ tầng dùng chung của nhà cung cấp dịch vụ. Khách hàng sẽ đăng ký với nhà cung cấp và trả phí sử dụng dựa theo chính sách giá của nhà cung cấp căn cứ vào yêu cầu về tài nguyên của bên sử dụng dịch vụ.

ĐTĐM công cộng phù hợp với đối tượng khách hàng có quy mô vừa và nhỏ, dữ liệu của khách hàng không yêu cầu bảo mật ở mức cao. Ví dụ khách hàng có thể thuê một máy chủ ảo để phục vụ hoạt động bán hàng trực tuyến.

b) ĐTĐM riêng (Private Cloud): Đây là hạ tầng ĐTĐM được dành cho chỉ duy nhất một khách hàng. Hệ thống này có thể được đặt ở TTDL của cơ quan, tổ chức hoặc tại TTDL của nhà cung cấp dịch vụ và quản lý bởi khách hàng, nhà cung cấp hoặc bên thứ ba. Ví dụ tường hợp khách hàng thuê không gian vật lý tại TTDL của doanh nghiệp để đặt hệ thống của mình hoặc thuê hạ tầng riêng tại TTDL của doanh nghiệp và tự quản lý, vận hành.

Mô hình ĐTĐM riêng phù hợp với đối tượng khách hàng có dữ liệu quan trọng, yêu cầu bảo mật cao. Tuy nhiên, mô hình này yêu cầu khách hàng có đội ngũ nhân sự có chuyên môn để quản lý vận hành hệ thống. Trách nhiệm liên quan đến bảo đảm an toàn thông tin mạng là trách nhiệm của khách hàng. Nhà cung cấp dịch vụ chỉ bảo đảm về mặt hạ tầng và các thành phần mà nhà cung cấp dịch vụ quản lý vận hành.

Trường hợp khách hàng tự triển khai xây dựng và quản lý vận hành hạ tầng ĐTĐM riêng của mình thì nên thuê dịch vụ chuyên nghiệp của nhà cung cấp dịch vụ trong quá trình xây dựng và thiết lập hệ thống. Nhà cung cấp dịch vụ sẽ chuyển giao công nghệ, đào tạo, hướng dẫn quản lý vận hành cho khách hàng sau khi hoàn thiện hệ thống.

c) ĐTĐM lai (Hybrid Cloud): Là sự kết hợp của ĐTĐM riêng và ĐTĐM công cộng. Phương án này cho phép các khách hàng có thể tối ưu việc sử dụng dịch vụ trên cơ sở sử dụng kết hợp giữa hai mô hình. Ví dụ đối với những thành phần hệ thống có xử lý dữ liệu quan trọng, yêu cầu bảo mật cao thì sử dụng ĐTĐM riêng. Đối với hệ thống thành phần xử lý dữ liệu ít quan trọng, yêu cầu bảo mật không cao thì có thể sử dụng ĐTĐM công cộng. Theo cách này khách hàng sẽ tiết kiệm được chi phí, tối ưu về tài nguyên hệ thống.

d) ĐTĐM liên kết các nền tảng (Multicloud): Là hạ tầng ĐTĐM được thiết lập trên cơ sở kết nối nhiều đám mây chung của các nhà cung cấp dịch vụ khác nhau. Việc này cho phép khách hàng có thể sử dụng bất kỳ ĐTĐM chung của nhà cung cấp nào trong ĐTĐM liên kết các nền tảng và không phụ thuộc vào các nhà cung cấp còn lại. Điển hình là việc doanh nghiệp triển khai các ứng dụng gốc trên nhiều nhà cung cấp dịch vụ đám mây khác nhau đồng thời như Amazon Web Service, Azure Mirosoft, Google Cloud Platform…

# 2.3. Phân loại các mô hình cung cấp dịch vụ ĐTĐM

a) Dịch vụ điện toán đám mây cung cấp cơ sở hạ tầng (IaaS - Infrastructure-as-a-Service): Là khái niệm về dịch vụ cung cấp hạ tầng điện toán đám mây. Khách hàng thuê dịch vụ cơ sở hạ tầng và chỉ phải chi trả những gì họ sử dụng. Trong mô hình này, khách hàng toàn quyền quản trị hạ tầng máy chủ bao gồm hệ điều hành, ứng dụng và dữ liệu trên máy chủ.

Mô hình cung cấp dịch vụ này phù hợp với mô hình triển khai ĐTĐM riêng, đối với các khách hàng yêu cầu hạ tầng, hệ thống độc lập.

b) Dịch vụ điện toán đám mây cung cấp dịch vụ nền tảng (PaaS - Platform as a Service): Là khái niệm về dịch vụ cho thuê nền tảng điện toán đám mây. Nhà cung cấp có nhiệm vụ quản trị và vận hành toàn bộ cơ sở hạ tầng dịch vụ và cung cấp cho khách hàng các nền tảng phần mềm để chạy các ứng dụng và dịch vụ. Khách hàng chỉ việc sử dụng nền tảng đã thuê để xây dựng các ứng dụng và dịch vụ cho người dùng mà không cần quan tâm đến hiệu năng, khả năng mở rộng và nâng cấp của hệ thống.

Mô hình cung cấp dịch vụ này phù hợp với mô hình triển khai ĐTĐM công cộng, đối với các khách hàng có quy mô vừa và nhỏ và không yêu cầu bảo mật dữ liệu ở mức cao.

c) Dịch vụ điện toán đám mây cung cấp dịch vụ phần mềm (SaaS - Software as a Service): Là khái niệm cho thuê ứng dụng trên nền điện toán đám mây. Người dùng chỉ đơn giản thuê và sử dụng ứng dụng mà không cần quan tâm các vấn đề về hạ tầng hay nền tảng phần mềm họ sử dụng. Ví dụ, dịch vụ Office online cho phép người dùng thuê và sử dụng Office online thông qua giao diện website mà không cần phải cài đặt bất kỳ phần mềm hay ứng dụng nào.

Mô hình cung cấp dịch vụ này phù hợp với mô hình triển khai ĐTĐM công cộng, đối với người dùng đầu cuối sử dụng dịch vụ ĐTĐM như một ứng dụng dịch vụ.

# 2.4. Lựa chọn phương án triển khai nền tảng ĐTĐM

Việc triển khai nền tảng ĐTĐM có thể triển khai theo phương án tự xây dựng và quản lý, vận hành hoặc thuê dịch vụ chuyên nghiệp của doanh nghiệp.

Đối với phương án tự triển khai, quản lý vận hành thì yêu cầu cơ quan, tổ chức có đội ngũ chuyên gia có kinh nghiệm và năng lực để có thể xây dựng, quản lý, vận hành, duy trì và bảo đảm an toàn thông tin cho nền tảng. Do đó, cơ quan, tổ chức được khuyến nghị triển khai theo hướng thuê dịch vụ chuyên nghiệp của doanh nghiệp.

Tuy nhiên, đối với một số hệ thống thông tin có yêu cầu đặc thù riêng, yêu cầu đơn vị chủ quản tự quản lý, vận hành hệ thống, thì cơ quan, tổ chức cần xem xét phương án thuê doanh nghiệp triển khai xây dựng hạ tầng ĐTĐM. Sau khi hệ thống được xây dựng hoàn thiện thì doanh nghiệp sẽ bàn giao, chuyển giao công nghệ, đào tạo và hướng dẫn quản lý vận hành hệ thống.

Trường hợp cơ quan, tổ chức thuê dịch vụ dịch vụ hạ tầng điện toán đám mây của doanh nghiệp, Bộ Thông tin và Truyền thông khuyến nghị cơ quan, tổ chức ưu tiên lựa chọn doanh nghiệp trong danh sách được Bộ Thông tin và Truyền thông công bố các doanh nghiệp cung cấp dịch vụ ĐTĐM đáp ứng các tiêu chí, chỉ tiêu kỹ thuật.

Doanh nghiệp được lựa chọn phải tuân thủ các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ theo quy định tại tại Luật An toàn thông tin mạng, Nghị định 85/2016/NĐ-CP ngày 01/7/2016, Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 và các quy định khác liên quan; có phương án bảo đảm an toàn thông tin đáp ứng các yêu cầu cơ bản tại tiêu chuẩn quốc gia TCVN 11930:2017; tuân thủ các tiêu chuẩn kỹ thuật được quy định tại Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 và đáp ứng các tiêu chí, chỉ tiêu kỹ thuật tại văn bản hướng dẫn này.

CHƯƠNG 3
TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT TỐI THIỂU
CHO CƠ SỞ HẠ TẦNG ĐIỆN TOÁN ĐÁM MÂY

Cơ quan, tổ chức, doanh nghiệp khi xây dựng, triển khai, cung cấp dịch vụ nền tảng ĐTĐM phải đáp ứng các tiêu chí, chỉ tiêu kỹ thuật trong tài liệu này và các tiêu chuẩn, quy chuẩn kỹ thuật khác liên quan.

Yêu cầu về các tiêu chí, chỉ tiêu kỹ thuật cụ thể với từng tính năng và phương pháp đánh giá được mô tả chi tiết tại Phụ lục 1 tài liệu này.

# 3.1. Yêu cầu máy chủ ảo

***3.1.1. Tạo máy ảo***

Cho phép tạo máy chủ ảo thông qua giao diện đồ họa (GUI), qua giao diện dòng lệnh (CLI) và giao diện lập trình ứng dụng (API) tích hợp với hệ thống khác*.*

***3.1.2. Tạo nhiều máy ảo cùng một lúc***

Cho phép người dùng tạo nhiều máy ảo một lúc với số lượng loại hệ điều hành khác nhau.

***3.1.3. Tùy biến máy ảo***

Cho phép người dùng tạo máy ảo từ tệp tin hệ điều hành mà hệ thống hỗ trợ; tùy biến máy ảo muốn tạo và lưu lại máy ảo sau khi tùy biến thành tệp tin hệ điều hành; lưu trữ tệp tin hệ điều hành do người dùng tạo ra trong nhóm tệp tin hệ điều hành tùy biến; sử dụng giao diện cổng thông tin quản trị (web portal) để tạo máy ảo tùy ý.

***3.1.4. Nhập / xuất máy ảo***

 Cho phép người dùng tải lên và tạo máy ảo từ những tệp tin hệ điều hành khác nhau; lưu lại máy ảo đang chạy thành các tệp tin hệ điều hành có định dạng cho phép người dùng tải xuống các tệp tin hệ điều hành.

***3.1.5. Chuyển đổi định dạng tệp tin hệ điều hành***

Yêu cầu này cho phép người dùng chuyển đổi qua lại các định dạng tệp tin hệ điều hành khác nhau cùng một lúc.

***3.2.6. Triển khai máy ảo có cấu hình cao***

Hỗ trợ triển khai các máy ảo có số lượng lớn nhân xử lý và có bộ nhớ kích thước lớn mà nặng về bộ nhớ (memory-intensive) hoặc nặng về nhân xử lý (processor-intensive).

***3.1.7. Thay đổi cấu hình phần cứng máy ảo***

 Cho phép người dùng thay đổi cấu hình phần cứng máy ảo trong khi các máy ảo đang chạy, không yêu cầu đối với trường hợp giảm kích thước ổ cứng.

***3.1.8. Di chuyển máy ảo giữa các máy chủ vật lý***

Yêu cầu này cho phép di chuyển dữ liệu của một máy ảo đang chạy từ máy vật lý này sang máy vật lý khác mà không phải tắt hoặc khởi động lại máy ảo.

***3.1.9. Di chuyển dữ liệu máy ảo giữa các bộ lưu trữ khác nhau***

Yêu cầu này cho phép di chuyển dữ liệu của một máy ảo đang chạy từ thiết bị lưu trữ này sang thiết bị lưu trữ khác mà không phải tắt hoặc khởi động lại.

***3.1.10. Khôi phục máy ảo sau khi có lỗi xảy ra***

Yêu cầu cho phép khôi phục / khởi động lại tự động máy ảo (khi cơ sở hạ tầng vật lý phát sinh lỗi) phải thỏa mãn 02 điều kiện kèm theo.

***3.1.11. Tính năng phân bổ máy ảo trên các máy vật lý khác nhau (anti-affinity)***

Yêu cầu này cho phép người dùng cấu hình các thông số trên máy ảo để xác định vị trí triển khai các máy ảo khác nhau trên các máy vật lý hoặc trung tâm dữ liệu khác nhau (nhằm phòng tránh sự ảnh hưởng của vấn đề nào đó về phần cứng hoặc cơ sở hạ tầng đối với tất cả các máy ảo cùng một lúc).

***3.1.12. Tự động thay đổi cấu hình hệ thống mức cơ bản***

Tự động thay đổi theo chiều ngang thông qua 03 cách bao gồm bật / tắt máy ảo; tạo ra các máy ảo mới dựa theo kế hoạch được lập thủ công trước đó; các tiêu chí sử dụng tài nguyên do người dùng định nghĩa; Cho phép người dùng thiết lập số lượng tối đa máy ảo mới được tạo.

***3.1.13. Tính năng phân bổ máy ảo trên cùng máy vật lý (affinity)***

Cho phép người dùng định nghĩa các quy tắc hợp tác trao đổi dữ liệu giữa các máy ảo; Hỗ trợ triển khai các máy ảo thường xuyên trao đổi dữ liệu với nhau trên cùng một máy vật lý.

***3.1.14. Truy cập vào máy ảo thông qua giao diện bảng điều khiển (console)***

Cho phép người dùng truy cập vào máy ảo thông qua giao diện bảng điều khiển (console) với các trình duyệt phổ biến.

***3.1.15. Gắn các tệp tin định dạng ISO trên máy ảo***

Cho phép gắn các tệp tin định dạng ISO trên máy ảo (các tệp tin định dạng ISO có thể nằm trên một kho dữ liệu riêng của giải pháp).

***3.1.16. Sao lưu/khôi phục máy ảo***

Cho phép người dùng sao lưu máy ảo thành các bản chụp (snapshot) theo kế hoạch được lập thủ công hoặc định kỳ trước đó; lưu trữ bản chụp (snapshot) được tạo ra dựa theo thông tin về thời điểm tạo; sao lưu máy ảo thông qua cổng thông tin quản trị hoặc CLI; khôi phục máy ảo từ bản chụp (snapshot).

***3.1.17. Giới hạn IOPS và băng thông ổ đĩa của máy ảo***

Cho phép người quản trị và người dùng giới hạn IOPS của máy ảo và giới hạn băng thông ổ đĩa của máy ảo.

***3.1.18. Giới hạn băng thông mạng của máy ảo***

Yêu cầu này cho phép người dùng giới hạn băng thông mạng của máy ảo cho cả hai luồng lưu lượng mạng vào/ra.

***3.1.19. Triển khai máy ảo cần sử dụng các công nghệ tăng tốc (accelerator)***

Hỗ trợ cấu hình NUMA và Transparent Hugepage, PCI Pass through, SR-IOV, OVS-DPDK, CPU pinning, DPDK và Direct I/O khi triển khai các máy ảo cần sử dụng các công nghệ tăng tốc (accelerator).

***3.1.20. Tự động chọn máy chủ vật lý khi tạo một máy ảo mới***

Cho phép tự động chọn máy chủ vật lý để triển khai máy ảo mới tạo nhằm cân bằng tải giữa các máy chủ vật lý.

***3.1.21. Thiết lập hoặc thiết lập lại mật khẩu cho tài khoản quản trị của máy ảo***

Cho phép quản trị viên nhập mật khẩu cho tài khoản quản trị của máy ảo.

***3.1.22. Định nghĩa, cấu hình và khởi tạo cụm gồm nhiều máy ảo***

Yêu cầu này cho phép người dùng định nghĩa một cluster mới tùy ý. Ví dụ: một cụm máy chủ ảo 3 tầng gồm 06 máy ảo (02 máy chạy ứng dụng ở mạng công cộng, 02 máy chạy các dịch vụ backend ở mạng cục bộ và 02 máy chạy cơ sở dữ liệu ở mạng cục bộ) có thể được tích hợp với tính năng tự động thay đổi cấu hình hệ thống.

# 3.2. Yêu cầu thiết bị lưu trữ

***3.2.1. Tích hợp các thiết bị lưu trữ truyền thống và giải pháp lưu trữ bằng phần mềm***

Hỗ trợ giải pháp lưu trữ bằng phần mềm (SDS-Software-Defined Storage); tích hợp các thiết bị SAN (Storage Area Network) và NAS (Network-Attached Storage).

***3.2.2. Tích hợp các dịch vụ lưu trữ***

Hỗ trợ lưu trữ dạng khối (block storage); lưu trữ dạng đối tượng (object storage) và lưu trữ dạng tệp tin (file storage).

***3.2.3. Áp dụng chính sách đối với các dịch vụ lưu trữ phân tầng***

Cho phép người dùng thiết lập chính sách đối với các dịch vụ lưu trữ phân tầng. Ví dụ: một quản trị viên về việc lưu trữ dữ liệu có thể lập kế hoạch lưu những dữ liệu không thường xuyên sử dụng trên thiết bị SATA chậm hơn và ít tốn kém hơn.

***3.2.4. Gắn bộ nhớ trên nhiều máy ảo***

Cho phép gắn một ổ cứng ảo (từ SAN hoăc SDS) trên nhiều máy ảo ổ cứng ảo có thể ở chế độ chỉ đọc); gắn một hệ thống tệp tin chia sẻ dùng chung trên nhiều máy ảo một cách linh hoạt và tự động.

***3.2.5. Quản lý, phân bổ các tham số hiệu năng của ổ cứng ảo***

Cho phép người dùng chọn một phân lớp hiệu năng cho các ổ cứng ảo. Ví dụ: IOPS hoặc băng thông (đo bằng Mbps).

***3.2.6. Tự động phân bổ dữ liệu trên vùng lưu trữ***

Cho phép tự động phân bổ dữ liệu trên vùng lưu trữ để phân tải cho các ổ đĩa.

***3.2.7. Mở rộng vùng lưu trữ***

Cho phép người dùng tăng dung lượng của một vùng lưu trữ đã có sẵn.

***3.2.8. Mở rộng các ổ cứng ảo***

Cho phép người dùng tăng kích thước của một ổ cứng ảo (ổ cứng ảo của thiết bị SAN hoặc SDS) đã có sẵn mà không phải cấp thêm ổ cứng ảo mới hoặc sao chép dữ liệu sang ổ cứng ảo mới.

***3.2.9. Di dời dữ liệu giữa các vùng lưu trữ khi hệ thống đang vận hành***

Cho phép quản trị viên di chuyển dữ liệu giữa các vùng lưu trữ khi hệ thống đang vận hành.

***3.2.10. Sao lưu ổ cứng ảo***

Cho phép người dùng sao lưu ổ cứng ảo tại một thời điểm bất kỳ thành các bản chụp (snapshot) thông qua các cách thức tự thao tác (self-service.); sử dụng các bản chụp (snapshot) thông qua cách thức tự thao tác (self-service) với mục đích để cấp thêm máy ảo mới; sao lưu dữ liệu trên ổ cứng ảo.

***3.2.11. Khả năng cung cấp lưu trữ dạng đối tượng (Object storage)***

Cho phép lưu trữ và truy xuất dữ liệu thông qua API trên dịch vụ web; hỗ trợ khả năng thay đổi đối với từng đối tượng đơn lẻ và toàn bộ lưu trữ dạng đối tượng (Object storage).

***3.2.12. Mã hóa dữ liệu***

Cho phép người dùng mã hóa dữ liệu hoặc cấu trúc dữ liệu.

***3.2.13. Sao lưu đối tượng***

Cho phép người dùng sao lưu đối tượng thành nhiều phiên bản tại những thời điểm khác nhau nhằm mục đích phòng ngừa việc mất mát dữ liệu do ghi đè hoặc xóa đối tượng; cấu hình việc sao lưu thông qua CLI, GUI hoặc API đối với từng đối tượng.

# 3.3. Yêu cầu mạng

***3.3.1. Quản lý hiệu năng mạng***

Yêu cầu này cho phép người dùng quản lý hiệu năng đối với từng mạng mà máy ảo kết nối đến bao gồm việc giới hạn băng thông, độ trễ, quản lý chất lượng dịch vụ (QoS).

***3.3.2. Tích hợp nhiều cổng giao tiếp mạng ảo trên vNIC một máy ảo***

Cho phép nhiều địa chỉ IP khác nhau được gán cho một máy ảo thông qua tích hợp nhiều cổng giao tiếp mạng ảo; định nghĩa nhiều phân đoạn mạng ảo, nhiều mạng con cho mỗi mạng ảo.

***3.3.3. Hỗ trợ khả năng dự phòng từ mức vật lý cho các mạng mà máy ảo kết nối đến***

Hỗ trợ khả năng dự phòng từ mức vật lý (ít nhất ở mức cổng vật lý – NIC) cho các mạng mà máy ảo kết nối đến; hoạt động ở mức active-active hoặc active-standby để cải thiện băng thông và bảo đảm tính sẵn sàng.

***3.3.4. Cấp phát địa chỉ IP***

Cho phép một máy ảo được gán địa chỉ IP động và địa chỉ IP này phải luôn không đổi giá trị trong suốt quá trình hoạt động của máy ảo.

***3.3.5. Liên kết với bộ chuyển mạch và bộ định tuyến thông thường***

Cung cấp tính năng SDN hoặc liên kết với các bộ chuyển mạch và bộ định tuyến thông thường của nhiều hãng khác nhau.

***3.3.6. Phòng chống tấn công giả mạo địa chỉ IP và giả mạo gói tin ARP***

Cung cấp tính năng phòng chống tấn công giả mạo địa chỉ IP và giả mạo gói tin ARP đối với mạng nội bộ của máy ảo hoặc các mạng mà máy ảo và máy vật lý kết nối đến.

***3.3.7. Hỗ trợ VLAN và VXLAN***

Cung cấp tính năng cho phép người dùng định nghĩa các mạng ảo bao gồm cả VLAN và VXLAN.

***3.3.8. Hỗ trợ bộ định tuyến ảo***

Cho phép người dùng sử dụng các chức năng của bộ định tuyến (NAT, định tuyến giữa các VLAN,…) để quản lý kết nối giữa các mạng.

***3.3.9. Tích hợp dịch vụ cân bằng tải***

Yêu cầu này cho phép người dùng sử dụng dịch vụ cân bằng tải đã được tích hợp sẵn (dịch vụ bao gồm các chức năng cấu hình giám sát, cấu hình cho thiết bị đầu cuối và tương thích với nhiều máy ảo đang kết nối với nhiều mạng ảo khác nhau).

***3.3.10. Cấu hình chính sách truy cập cho từng cổng trên máy ảo***

Yêu cầu này cho phép người dùng cấu hình chính sách truy cập cho từng cổng (thuộc cổng giao tiếp mạng ảo trên vNIC) trên những máy ảo đang chạy.

***3.3.11. Tích hợp dịch vụ tường lửa***

Cho phép người dùng sử dụng dịch vụ tường lửa đã được tích hợp sẵn (dịch vụ phải hoạt động bình thường trên tầng IP và Domain).

***3.3.12. Hỗ trợ IPv6 cho cả mạng vật lý và mạng ảo***

Cung cấp tính năng hỗ trợ máy ảo hoặc cổng kết nối (ví dụ: bộ cân bằng tải) sử dụng IPv6 trên cả mạng vật lý và mạng ảo.

***3.3.13. Tách biệt các mạng ảo với nhau***

Cung cấp tính năng tách biệt hoàn toàn các mạng ảo khác nhau.

***3.3.14. Đảm bảo sự hao phí băng thông đường truyền kết nối giữa các mạng không vượt quá 10%***

Cung cấp tính năng đảm bảo sự hao phí băng thông đường truyền kết nối giữa máy ảo với máy ảo và máy ảo với thành phần bên ngoài. Ví dụ: nếu thiết lập 02 mạng VXLAN cho 02 máy ảo khác nhau trong mạng vật lý có băng thông là 10 Gbps thì băng thông thực tế của đường truyền kết nối giữa các máy ảo này phải > 9 Gbps.

***3.3.15. Đảm bảo hạ tầng kỹ thuật cho máy chủ vật lý và máy ảo có tính sẵn sàng cao***

Cung cấp tính năng đảm bảo máy chủ vật lý và máy ảo chạy trên hạ tầng kỹ thuật có tính sẵn sàng cao, đảm bảo tính nguyên vẹn và tính bí mật của dữ liệu.

***3.3.16. Hỗ trợ cấu trúc liên kết mạng có tính phân cấp do người dùng định nghĩa***

Cho phép người dùng tự thiết kế các thành phần và sơ đồ mạng bao gồm tường lửa ảo, VLAN / VXLAN / GRE, mạng con, NAT, r bộ cân bằng tải ảo.

***3.3.17. Hỗ trợ SDN***

Cung cấp tính năng tạo bộ chuyển mạch ảo và bộ định tuyến ảo.

 ***3.3.18. Tách biệt các mặt phẳng SDN với nhau***

Cung cấp tính năng tách biệt các mặt phẳng điều khiển, mặt phẳng chuyển tiếp và mặt phẳng quản trị với nhau.

***3.3.19. Hỗ trợ Open Flow hoặc tương đương***

Cung cấp tính năng hỗ trợ OpenFlow cho SDN hoặc tương đương.

***3.3.20. Hỗ trợ tích hợp nền tảng điện toán đám mây***

Cung cấp tính năng hỗ trợ API sử dụng nền tảng điện toán đám mây để tạo bộ chuyển mạch ảo và bộ định tuyến ảo.

***3.3.21. Quản trị và điều khiển bộ chuyển mạch ảo và bộ định tuyến ảo***

Cung cấp tính năng quản trị và điều khiển bộ chuyển mạch ảo và bộ định tuyến ảo.

***3.3.22. Tự động tạo và quản trị bộ chuyển mạch ảo và bộ định tuyến ảo***

Cung cấp tính năng tự động tạo và quản trị bộ chuyển mạch ảo và bộ định tuyến ảo.

***3.3.23. Hỗ trợ AAA***

Cung cấp tính năng tích hợp các thành phần để xác thực, phân quyền, ghi log hoạt động (authenticate, authorize, account – AAA) người dùng.

***3.3.24. Quản trị các thành phần trong mạng***

Cho phép người dùng sử dụng SNMP, Netconf hoặc tương đương có chức năng quản trị các thành phần khác trong mạng.

***3.3.25. Đảm bảo bộ điều khiển có tính sẵn sàng cao***

Cung cấp tính năng đảm bảo bộ điều khiển cho SDN có tính sẵn sàng cao.

***3.3.26. Hỗ trợ Jumbo Frame***

Cung cấp tính năng sử dụng Jumbo Frame (các khung có kích thước gói tin lớn nhất – MTU – có thể lên đến 9000 byte) trong việc truyền tải gói tin.

***3.3.27. Tích hợp CLI và GUI***

Cho phép người dùng cấu hình, quản lý các thành phần trong mạng, bộ điều khiển cho SDN thông qua CLI và GUI.

***3.3.28. Hỗ trợ các chức năng của bộ chuyển mạch ảo và bộ định tuyến ảo***

Hỗ trợ SPAN, RSPAN hoặc tương đương; LACP (mode 1, 2, 3, 4) từ máy ảo, máy vật lý, 802.1Q VLAN with trunking, multicast snooping, LLDP, STP, RSTP, quản lý chất lượng dịch vụ (QoS), VXLAN.

# 3.4. Máy chủ vật lý

***3.4.1. Tự động cài đặt hệ điều hành và phần mềm giám sát máy ảo (hypervisor)***

Cho phép tự động cài đặt hệ điều hành và phần mềm giám sát máy ảo sau khi có những thiết bị (ảo hoặc vật lý) mới truy cập mạng. Cho phép người dùng hoặc các thiết bị khác trong mạng có thể sử dụng, giao tiếp với chúng.

***3.4.2. Triển khai nhiều phiên bản hệ điều hành Windows và Linux cho máy chủ vật lý***

Cho phép triển khai nhiều phiên bản hệ điều hành Windows và Linux cho máy chủ vật lý bao gồm: Windows 8 và 10, 2012 và 2016, Ubuntu 14.04, 16.04 và 18.04, CentOS 6.x và 7.x, RHEL 6 và 7, Oracle Linux 6 và 7 và các phiên bản hiện hành của các hệ điều hành được liệt kê ở trên.

***3.4.3. Quản trị qua kênh truyền tín hiệu riêng biệt (out-of-band)***

Cho phép quản trị qua kênh truyền tín hiệu riêng biệt sử dụng các giao diện quản lý nền tảng như iRMC, iLO, IDRAC, UCS và các giao diện khác tương đương.

***3.4.4. Truy cập vào máy chủ vật lý thông qua giao diện bảng điều khiển***

Cho phép người dùng truy cập vào máy chủ vật lý thông qua giao diện bảng điều khiển (console).

***3.4.5. Cấu hình cơ chế dự phòng cho ổ cứng trên máy chủ vật lý***

Cho phép người dùng cấu hình RAID trên máy chủ vật lý.

# 3.5. Yêu cầu quản trị và vận hành

***3.5.1. Định nghĩa các hành động sau khi tạo hoặc xóa máy ảo***

Cho phép quản trị viên định nghĩa các hành động sau khi tạo hoặc xóa máy ảo.

***3.5.2. Thực hiện một hành động do người dùng chỉ định sẵn sau khi quá trình khởi động hoàn thành***

Cung cấp tính năng thực hiện một hành động do người dùng chỉ định sẵn thông qua cách thức tự hành (self-service) sau khi quá trình khởi động lần đầu hoàn thành đối với máy ảo mới tạo.

***3.5.3. Hỗ trợ quản trị cấu hình***

Hỗ trợ quản trị cấu hình (thông qua Ansible, Puppet, Chef hoặc SaltStack) bao gồm: Hoạt động như một dịch vụ được tích hợp sẵn để cho phép người dùng quản lý, kiểm tra các cấu hình và quy trình triển khai; Tự động hóa toàn bộ quy trình triển khai, nâng cấp, cập nhật và vá lỗi; Tích hợp các thành phần vận hành tự động có khả năng được cấu hình thông qua các ngôn ngữ lập trình (như YAML,…).

***3.5.4. Quản lý tài nguyên***

Cho phép quản trị viên giám sát, đánh giá lịch sử sử dụng tài nguyên của các máy ảo; đưa ra các khuyến nghị về việc cấp thêm tài nguyên khi cần thiết.

***3.5.5. Quản lý bản vá***

Cho phép tự động tạo thống kê, báo cáo về các bản vá đã được cập nhật; tự động áp dụng các bản vá lên nhiều máy chủ một lúc; khôi phục các bản vá đã cập nhật.

***3.5.6. Tích hợp giao diện cổng thông tin quản trị***

Cho phép tích hợp giao diện cổng thông tin quản trị có tính tự hành cho người dùng đầu cuối (để người dùng tự quản lý tài nguyên được cấp) và giao diện cổng thông tin quản trị cho quản trị viên; hỗ trợ giao diện cổng thông tin quản trị.

***3.5.7. Tùy biến giao diện cổng thông tin quản trị***

Cung cấp tính năng cho phép người dùng tùy biến giao diện cổng thông tin quản trị về hiển thị các thông số, tiêu chí như trạng thái, hiệu năng, tính sẵn sàng của tập hợp các máy chủ, dịch vụ.

***3.5.8. Quản lý, giám sát nền tảng hạ tầng dịch vụ điện toán đám mây***

Cho phép hiển thị theo thời gian thực các thông số giám sát về hiệu năng hệ thống; cấu hình tùy theo ý muốn về cảnh báo hoặc báo cáo khi có sự cố xảy ra; cấu hình khoảng thời gian lấy mẫu các thông số giám sát; giám sát được các thành phần của cơ sở hạ tầng vật lý bao gồm bộ chuyển mạch, bộ định tuyến, tủ chứa máy chủ và các thiết bị lưu trữ.

***3.5.9. Cảnh báo khi có sự kiện / sự cố về cơ sở hạ tầng xảy ra***

Cung cấp tính năng gửi cảnh báo cho người dùng khi có sự kiện / sự cố về cơ sở hạ tầng xảy ra theo giá trị ngưỡng; cho phép người dùng thiết lập các giá trị ngưỡng đối với từng thành phần một; cho phép cảnh báo tới người dùng thông qua email, SMS.

***3.5.10. Thu thập và lưu trữ log hệ thống***

Cung cấp tính năng thu thập, lưu trữ và xoay vòng định kỳ log hệ thống về các tác vụ tạo, đọc, cập nhật, xóa - CRUD (Create, Read, Update, Delete – tạo, đọc, cập nhật, xóa), tài nguyên được sử dụng,…

***3.5.11. Tích hợp API giám sát dữ liệu***

Cung cấp tính năng tích hợp API dành cho giám sát dữ liệu (bao gồm các thông số về trạng thái hoạt động hiện tại và trong quá khứ đối với từng thành phần được giám sát) để cho phép người dùng giám sát, phân tích dữ liệu thông qua các hệ thống giám sát in-house hoặc của bên thứ ba sử dụng API đó.

***3.5.12. Ghi log về các sự kiện liên quan đến tài khoản***

Cung cấp tính năng ghi log về các sự kiện liên quan đến tài khoản như: các thao tác đăng nhập tài khoản, quản lý tài khoản bao gồm tạo / xoá / lập nhóm / gắn thẻ cho tài khoản người dùng và các thao tác khác; Cho phép người dùng xem các bản ghi log thông qua giao diện có tính tự hành và khả năng xuất các bản ghi log để lưu giữ lâu hơn.

# 3.6. Yêu cầu tích hợp

***3.6.1. Tích hợp giao diện tương tác với thành phần quản lý chức năng mạng ảo (Virtual Network Function – VNF)***

Cung cấp tính năng tích hợp giao diện tương tác với thành phần VNF từ nhiều hãng (như Nokia, Ericsson, Huawei, ZTE,…) mà tuân theo kiến trúc ETSI MANO để hỗ trợ quản lý vòng đời VNF cũng như khả năng mở rộng.

***3.6.2. Tích hợp CLI và API tương tác với hệ thống***

Cung cấp tính năng tích hợp CLI và API cho phép quản trị viên thực hiện các thao tác trên hệ thống.

***3.6.3. Hỗ trợ thư viện phục vụ cho lập trình, phát triển phần mềm tương tác với hệ thống***

Cung cấp tính năng hỗ trợ các thư viện (mã nguồn mở hoặc tự cloud provider tạo) phục vụ cho lập trình, phát triển phần mềm tương tác với hệ thống như tương thích với các ngôn ngữ lập trình phổ biến Java, .NET, Perl, Node.js, PHP, Python, Ruby và PowerShell.

# 3.7. Các yêu cầu khác

***3.7.1. Đảm bảo khả năng mở rộng***

Cung cấp tính năng thay đổi hệ thống bao gồm cấp thêm máy chủ, thiết bị lưu trữ, các thiết bị mạng mà không thay đổi kiến trúc.

***3.7.2. Đảm bảo tính sẵn sàng cao của các thành phần dịch vụ***

Cung cấp tính năng đảm bảo tính năng sẵn sàng cao của các thành phần như giao diện quản lý của quản trị viên, API, các thành phần điều khiển tập trung.

***3.7.3. Đảm bảo tính sẵn sàng cao của hệ thống***

Cung cấp tính năng đảm bảo hệ thống có tính sẵn sàng cao theo tỷ lệ thời gian đáp ứng.

***3.7.4. Hỗ trợ máy chủ có kiến trúc CPU x86\_64***

Cung cấp tính năng hỗ trợ cài đặt, triển khai, vận hành hệ thống trên máy chủ trên nhiều nền tảng kiến trúc khác nhau.

***3.7.5. Đồng bộ thời gian***

Cung cấp tính năng đồng bộ thời gian cho tất cả các thành phần trong hệ thống.

CHƯƠNG 4
TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN
CHO CƠ SỞ HẠ TẦNG ĐIỆN TOÁN ĐÁM MÂY

Việc bảo đảm an toàn thông tin cho hạ tầng ĐTĐM phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin theo cấp độ được quy định tại Luật An toàn thông tin mạng, Nghị định 85/2016/NĐ-CP ngày 01/7/2016, Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 và các quy định khác liên quan.

Phương án bảo đảm an toàn thông tin cần đáp ứng các yêu cầu an toàn tại tiêu chuẩn quốc gia TCVN 11930:2017 và các tiêu chuẩn, quy chuẩn liên quan theo quy định.

Trường hợp hạ tầng điện toán đám mây có kết nối vào mạng Truyền số liệu chuyên dụng thì phải đáp ứng các quy định tại Thông tư 12/2019/TT-BTTTT ngày 05/11/2019, hướng dẫn của Bộ Thông tin và Truyền thông tại Công văn số 1694/BTTTT-CATTT ngày 31/5/2019 và các quy định khác liên quan.

Việc bảo đảm an toàn thông tin cho hạ tầng ĐTĐM phải đáp ứng các tiêu chí, chỉ tiêu kỹ thuật an toàn thông tin tại Mục 4.4 của văn bản hướng dẫn này.

# 4.1. Các nguy cơ mất an toàn thông tin đối với nền tảng điện toán đám mây

Các nguy cơ mất an toàn thông tin đối với nền tảng ĐTĐM là khả năng gây thiệt hại cho các tài sản thông tin, quy trình và hệ thống của cơ quan, tổ chức. Các nguy cơ có thể có nguồn gốc tự nhiên hoặc con người; có thể là vô tình hoặc cố ý; có thể phát sinh từ bên trong hoặc từ bên ngoài tổ chức.

Ngoài ra còn nhiều nguy cơ mất an toàn thông tin khác đối với việc cung cấp và sử dụng nền tảng ĐTĐM, dưới đây là một số nguy cơ phổ biến liên quan đến bảo đảm an toàn thông tin cho hạ tầng ĐTĐM đối với bên sử dụng và bên cung cấp dịch vụ và các bên liên quan.

***4.1.1. Các nguy cơ mất an toàn thông tin đối với người sử dụng dịch vụ đám mây***

1. *Mất hoặc rò rỉ dữ liệu*

Dịch vụ đám mây thường là một hạ tầng dùng chung cho nhiều đối tượng khác nhau. Do đó việc mất hoặc rò rỉ dữ liệu giữa các người dùng trên cùng nền tảng hoặc các người dùng ở các nền tảng ĐTĐM khác là một nguy cơ rất lớn đối với các khách hàng.

Việc thiếu quản lý thông tin mật mã thích hợp, chẳng hạn như khóa mã hóa, mã xác thực và đặc quyền truy cập, có thể dẫn đến việc mất hoặc rò rỉ dữ liệu ra bên ngoài. Ví dụ, không đủ xác thực, ủy quyền và kiểm soát kiểm toán; sử dụng không nhất quán mã hóa và/hoặc khóa xác thực.

1. *Truy cập dịch vụ không an toàn*

Việc quản lý, vận hành hạ tầng, hệ thống dịch vụ, ứng dụng trên nền tảng ĐTĐM thường được khách hàng thực hiện từ xa qua mạng Internet. Do đó, kết nối mạng để thực hiện việc trên có thể dẫn tới nguy cơ mất an toàn trong trường hợp kết nối mạng đó không an toàn, không có cơ chế mã hóa, xác thực hoặc tồn tại điểm yếu an toàn thông tin.

Việc sử dụng kết nối mạng không an toàn có thể dẫn tới việc mất tài khoản quản trị hệ thống thông qua các dạng tấn công mạng như MITM (Man-in-the-middle attack). Trường hợp giao thức mạng có hỗ trợ cơ chế mã hóa xác thực nhưng có tồn tại điểm yếu an toàn thông tin thì tin tặc cũng có thể khai thác điểm yếu để lấy thông tin quản trị hoặc chiếm quyền điều khiển hệ thống.

1. *Mối đe dọa nội bộ*

Nguy cơ mất an toàn thông tin từ phía người sử dụng là phổ biến, chiếm tỷ lệ cao nhất. Nguyên nhân là do người sử dụng của khách hàng có nhận thức hạn chế về an toàn thông tin, còn thiếu những kiến thức cơ bản về an toàn thông tin. Một số trường hợp khác là do người sử dụng cố tình thực hiện các hành động dẫn tới nguy cơ mất an toàn thông tin cho hệ thống để có mục đích xấu. Một số ví dụ điển hình như nhân viên của khách hàng chia sẻ mật khẩu quản trị, đặt mật khẩu quản trị không đủ mạnh hoặc truy cập các trang thông tin độc hại bị cài mã độc.

***4.1.2. Các nguy cơ mất an toàn thông tin đối với nhà cung cấp dịch vụ đám mây***

1. *Truy cập quản trị trái phép*

Dịch vụ điện toán đám mây sẽ bao gồm các giao diện và các thành phần phần mềm cho phép nhân viên của khách hàng quản lý các dịch vụ, ứng dụng trên ĐTĐM thông qua các giao diện quản trị hệ thống. Do đó, việc chiếm quyền, truy cập trái phép thông qua việc tấn công khai thác giao diện quản trị hệ thống, vượt quyền từ tài khoản thường sang tài khoản quản trị là nguy cơ mất an toàn thông tin mà các nhà cung cấp dịch vụ cần phải đối mặt.

1. *Mối đe dọa nội bộ*

Tương tự đối với nguy cơ mất an toàn thông tin từ trong nội bộ như khách hàng thì đối với nhà cung cấp dịch vụ cũng có những nguy cơ tương tự.

Khi con người có liên quan, luôn có nguy cơ các cá nhân hành động theo cách độc hại hoặc bất cẩn khiến an toàn thông tin của dịch vụ gặp rủi ro.

Tuy nhiên, đối với nhà cung cấp dịch vụ thì nguy cơ mất an toàn thông tin từ nội bộ ở mức độ nguy hiểm hơn nhiều so với khách hàng. Lý do là nhà cung cấp dịch vụ có những cán bộ quản trị có quyền truy cập và quản trị hệ thống. Do đó, nguy cơ mất an toàn thông tin từ nội bộ của nhà cung cấp dịch vụ sẽ dẫn tới hậu quả rất nghiêm trọng.

# 4.2. Thách thức đối với việc bảo đảm an toàn thông tin cho ĐTĐM

***4.2.1. Thánh thức bảo mật đối với người sử dụng dịch vụ đám mây***

1. *Vấn đề liên quan đến trách nhiệm của các bên*

Khách hàng sử dụng nhiều dịch vụ ĐTĐM với các mô hình triển khai khác nhau, đối với từng loại dịch vụ và mô hình cụ thể thì phạm vi quản lý và trách nhiệm của khách hàng và nhà cung cấp dịch vụ là khác nhau. Do đó khi sử dụng dịch vụ và cung cấp dịch vụ, việc xác định phạm vi trách nhiệm khách hàng và nhà cung cấp dịch vụ là một thách thức lớn và phải được thể hiện trong hợp đồng thuê dịch vụ. Bất kỳ thiếu một định nghĩa rõ ràng về trách nhiệm giữa các khách hàng và nhà cung cấp dịch vụ có thể phát sinh mâu thuẫn giữa các bên.

1. *Sự tin tưởng vào bên cung cấp dịch vụ*

Việc sử dụng dịch vụ ĐTĐM cần có sự tin tưởng của khách hàng và nhà cung cấp dịch vụ , bởi vì việc sử dụng dịch vụ của khách hàng có thể coi như là sử dụng dịch vụ của một hộp đen, khi khách hàng không có thông tin và không có quyền quản trị các hệ thống bên trong hệ thống ĐTĐM mà chỉ dừng ở mức sử dụng dịch vụ. Đặc biệt trong trường hợp khách hàng có những dữ liệu nhạy cảm cần bảo vệ thì việc tin tưởng vào bên cung cấp dịch vụ là vấn đề rất quan trọng để lựa chọn đối tác phù hợp.

1. *Chia sẻ quyền quản trị hệ thống*

Khi khách hàng quyết định chuyển một phần của hệ thống CNTT của họ sang cơ sở hạ tầng ĐTĐM điều này có nghĩa nhà cung cấp dịch vụ sẽ có quyền kiểm soát nhất định đối với thành phần hệ thống của khách hàng trên hạ tầng ĐTĐM của nhà cung cấp dịch vụ. Do đó, việc kiểm soát hoặc phân quyền quản trị đối với nhà cung cấp dịch vụ vào thành phần của khách hàng thế nào là một vấn đề lớn, đặc biệt khi hệ thống của khách hàng là hệ thống thông tin quan trọng có chứa dữ liệu nhạy cảm. Do đó, khi sử dụng dịch vụ ĐTĐM, khách hàng có thể lo ngại về việc thiếu kiểm soát dữ liệu của họ được lưu trữ trong hệ thống của nhà cung cấp dịch vụ, ví dụ:

+ Khách hàng muốn xóa một tệp vì lý do pháp lý, nhưng nhà cung cấp dịch vụ giữ lại một bản sao mà khách hàng không biết.

+ Nhà cung cấp dịch vụ cung cấp cho các đặc quyền quản trị viên của khách hàng vượt ra ngoài chính sách của khách hàng.

1. *Lộ lọt thông tin bí mật*

Thông tin bí mật là loại thông tin yêu cầu bảo đảm an toàn thông tin ở mức độ cao nhất, đặc biệt là thông tin bí mật nhà nước. Do đó, việc bảo đảm an toàn thông tin bí mật khi sử dụng nền tảng ĐTĐM ngoài việc liên quan đến vấn đề kỹ thuật còn phải tuân thủ các quy định liên quan đến bảo vệ dữ liệu theo quy định của pháp luật.

Như đã phân tích tại Mục 4.1.1 thì các khách hàng có thể đối mặt với các nguy cơ lộ lọt thông tin bí mật khi sử dụng chung hạ tầng ĐTĐM với nhiều đối tượng khác nhau mà không có biện pháp bảo vệ phù hợp.

*đ) Tính khả dụng của hệ thống*

Nền tảng ĐTĐM yêu cầu tính khả dụng rất cao để có thể cung cấp các dịch vụ cho khách hàng. Tính khả dụng của hạ tầng ĐTĐM có thể bị ảnh hưởng từ nhiều yếu tố như hạ tầng vật lý, tấn công mạng hay các yếu tố liên quan đến chính sách, con người và quy trình.

Một vấn đề khác liên quan đến tính khả dụng khi sử dụng hạ tầng ĐTĐM là việc nhiều hệ thống của các khách hàng khác nhau cùng nằm trên một hạ tầng ĐTĐM của nhà cung cấp dịch vụ. Do đó, khi sự cố xảy ra đối với hệ thống của khách hàng này có thể làm ảnh hưởng chung đến hệ thống của các khách hàng khác. Ví dụ khi tin tặc thực hiện tấn công DDoS có thể làm mất tính khả dụng của cả một hạ tầng ĐTĐM.

1. *Sự phụ thuộc nền tảng ĐTĐM*

Khi khách hàng sử dụng dịch vụ của một nhà cung cấp dịch vụ mà chỉ nhà cung cấp đó có khả năng cung cấp dịch vụ do một số yêu cầu đặc thù hoặc hạ tầng ĐTĐM của nhà cung cấp đó được thiết kế không theo chuẩn nên không thể thay thế bởi nhà cung cấp khác. Vấn đề này sẽ dẫn đến rủi ro cho khách hàng khi dịch vụ của nhà cung cấp phụ thuộc đó phải dừng dịch vụ. Việc dừng dịch vụ của nhà cung cấp có thể dẫn tới từ nhiều yếu tố như bị tấn công mạng, môi trường vật lý hay do cơ quan chức năng yêu cầu dừng dịch vụ do vi phạm các quy định của pháp luật liên quan.

***4.2.2. Thách thức bảo mật cho các nhà cung cấp dịch vụ đám mây***

1. *Vấn đề liên quan đến trách nhiệm của các bên*

Tương tự đối với các khách hàng, vấn đề liên quan đến trách nhiệm của các bên cũng là một trong các thách thức đối với nhà cung cấp dịch vụ. Tuy nhiên, đối với các nhà cung cấp dịch vụ thì vấn đề này trở lên phức tạp và thách thức hơn do họ cung cấp dịch vụ cho nhiều đối tượng khách hàng khác nhau và yêu cầu trách nhiệm khác nhau. Bên cạnh đó, các nhà cung cấp dịch vụ cũng phải làm rõ trách nhiệm với các đối tác dịch vụ đám mây khi phối hợp cung cấp dịch vụ.

1. *Môi trường chia sẻ*

Ưu điểm của việc sử dụng hạ tầng ĐTĐM là tiết kiệm chi phí thông qua việc chia sẻ tài nguyên trên quy mô lớn. Tuy nhiên, vấn đề đặt ra là việc chia sẻ môi trường dùng chung sẽ dẫn đến các nguy cơ, thách thức liên quan đến việc bảo đảm an toàn thông tin cho các khách hàng như đã được đề cập tại mục 4.1.1, đặc biệt là các khách hàng có dữ liệu quan trọng và yêu cầu bảo mật thông tin cao. Ví dụ, nhiều máy ảo được lưu trữ trên một máy chủ vật lý chia sẻ cả đơn vị xử lý trung tâm (CPU) và tài nguyên bộ nhớ được ảo hóa bởi trình ảo hóa, do đó tin tặc có thể truy cập trái phép vào bộ nhớ hoặc lưu trữ của các máy ảo khác.

1. *Xung đột các cơ chế bảo vệ và không nhất quán*

Do kiến trúc phi tập trung của cơ sở hạ tầng ĐTĐM dẫn tới việc các cơ chế bảo vệ có thể không nhất quán giữa các mô-đun bảo mật phân tán. Ví dụ: quyền truy cập bị từ chối bởi một mô-đun bảo mật có thể được cấp bởi người khác. Sự không nhất quán này có thể gây ra sự cố cho người dùng và có thể bị kẻ tấn công lợi dụng để khai thác làm ảnh hưởng đến tính bảo mật, tính nguyên vẹn và tính sẵn sàng.

*d) Rủi ro di chuyển dịch vụ lên nền tảng ĐTĐM*

Di chuyển lên đám mây thường ngụ ý di chuyển một lượng lớn dữ liệu và thay đổi cấu hình của hệ thống. Việc di chuyển một phần của hệ thống CNTT sang nhà cung cấp dịch vụ bên ngoài có thể yêu cầu thay đổi trong thiết kế hệ thống (ví dụ: chính sách mạng và bảo mật). Việc tích hợp giữa hệ thống CNTT của nhà cung cấp dịch vụ với hạ tầng ĐTĐM của nhà cung cấp dịch vụ có thể xảy ra sự không tương thích hoặc thực thi chính sách bảo mật không thống nhất và có thể dẫn đến các nguy cơ mất an toàn thông tin cho hệ thống CNTT của khách hàng. Ví dụ: các máy ảo chạy phía sau tường lửa trong một trung tâm dữ liệu riêng tư không được kiểm soát truy cập và có thể kết nối với Internet trong đám mây của nhà cung cấp dịch vụ .

*e) Nguy cơ gây gián đoạn hoạt động*

ĐTĐM phân bổ tài nguyên và cung cấp chúng như một dịch vụ. Toàn bộ hệ sinh thái điện toán đám mây bao gồm nhiều phần phụ thuộc lẫn nhau. Sự gián đoạn của bất kỳ phần nào (chẳng hạn như mất điện, bị tấn công từ chối dịch vụ hoặc buộc dừng dịch vụ liên quan đến vấn đề pháp lý) có thể ảnh hưởng đến tính khả dụng của dịch vụ điện toán đám mây được kết nối sau đó gây gián đoạn hoạt động hệ thống của các khách hàng.

1. *Nguy cơ mất an toàn thông tin từ sản phẩm của đối tác*

Hạ tầng ĐTĐM của nhà cung cấp dịch vụ là một hệ thống thông tin lớn, sử dụng nhiều thành phần hạ tầng của các hãng các đối tác dịch vụ ĐTĐM khác nhau. Các thành phần này có thể tồn tại các lỗ hổng bảo mật mà các đối tác dịch vụ ĐTĐM không cung cấp bản vá kịp thời. Thậm chí một số sản phẩm của đối tác dịch vụ ĐTĐM có thể bị cài đặt sẵn mã độc (cửa hậu) để cho phép truy cập, điều khiển hệ thống từ xa. Do đó, các nguy cơ mất an toàn thông tin từ các sản phẩm của đối tác là một vấn đề bảo mật lớn đối với nhà cung cấp dịch vụ.

1. *Sự phụ thuộc giữa các thành phần phần mềm*

Khi nâng cấp thành phần của hạ tầng ĐTĐM trong trường hợp như phải nâng cấp để xử lý điểm yếu lỗ hổng bảo mật. Việc này có thể làm ảnh hưởng tới các thành phần phần mềm của hệ thống khách hàng đang sử dụng phiên bản ĐTĐM hiện tại. Việc nâng cấp một thành phần của hạ tầng ĐTĐM có thể làm mất tính tương thích với các thành phần khác trong hệ thống và gây ngưng trệ hệ thống.

 ***4.2.3. Thách thức bảo mật cho các đối tác dịch vụ đám mây***

1. *Vấn đề liên quan đến trách nhiệm của các bên*

Tương tự đối với các khách hàng và nhà cung cấp dịch vụ, vấn đề liên quan đến trách nhiệm của các bên cũng là một trong các thách thức đối với đối tác dịch vụ ĐTĐM. Trong trường hợp có sự kết hợp giữa phần mềm nhà cung cấp dịch vụ và đối tác dịch vụ ĐTĐM để cung cấp dịch vụ cho khách hàng, thì khi xảy ra sự cố đối với hệ thống của khách hàng thì việc xác định trách nhiệm giữa nhà cung cấp dịch vụ và đối tác dịch vụ ĐTĐM là một vấn đề đối với các bên. Bởi vì một số sự cố có thể là khó xác định nguyên nhân chỉ dựa vào các yếu tố kỹ thuật. Việc này có thể dẫn đến việc quy trách nhiệm cho nhau giữa nhà cung cấp dịch vụ và đối tác dịch vụ ĐTĐM dẫn đến các vi phạm tiếp theo nếu không tìm thấy nguyên nhân gốc rễ.

1. *Quyền sở hữu trí tuệ*

Khi các đối tác gửi phần mềm hoặc dữ liệu khác cho nhà cung cấp dịch vụ để thực thi, thách thức đặt ra là phần mềm hoặc dữ liệu có thể bị rò rỉ cho bên thứ ba hoặc bị chiếm dụng để sử dụng trái phép. Điều này có thể bao gồm vi phạm bản quyền hoặc tiết lộ bí mật thương mại.

1. *Tính nguyên vẹn dữ liệu*

Khi phần mềm, dữ liệu của đối tác dịch vụ ĐTĐM chạy trong hệ thống của nhà cung cấp dịch vụ, thì phần mềm hoặc dữ liệu có khả năng bị sửa đổi trái phép và nằm ngoài sự kiểm soát của đối tác dịch vụ ĐTĐM làm ảnh hưởng tới hoạt động bình thường của đối tác dịch vụ ĐTĐM. Khả năng này nằm ngoài tầm kiểm soát của đối tác dịch vụ ĐTĐM và có thể ảnh hưởng nghiêm trọng đến uy tín và hoạt động kinh doanh của họ.

# 4.3. Hướng dẫn bảo đảm an toàn thông tin tối thiểu cho hạ tầng ĐTĐM

Nội dung này hướng dẫn bảo đảm an toàn thông tin tối thiểu cho hạ tầng ĐTĐM, bao gồm các nội dung liên quan đến mô hình, phương án quản lý và bảo vệ dữ liệu và các biện pháp liên quan.

***4.3.1. Mô hình thực hiện***

Mô hình ủy thác là mô hình phù hợp, tin cậy cho bất kỳ hệ thống nào có nhiều nhà cung cấp hợp tác để cung cấp dịch vụ.

Do tính chất phân tán cao và nhiều bên liên quan của ĐTĐM nên cần sự kết hợp tổng thể, tin cậy giữa các thành phần. Mô hình tin cậy này sẽ cho phép tạo ra sự phân cấp hoặc chỉ định để cho phép các thành phần khác nhau trong hệ thống sẽ được xác thực, phần cấp và phân quyền phù hợp. Sự phân cấp hoặc phân quyền cụ thể sẽ dựa trên một hoặc nhiều đối tác tin cậy (ví dụ: cơ quan cấp chứng thư cơ sở hạ tầng khóa công khai (PKI)).

***4.3.2. Quản lý định danh và truy cập (IAM) và chống chối bỏ***

Hạ tầng ĐTĐM cần có biện pháp quản lý định danh và truy cập để phục vụ việc quản lý, vận hành và sử dụng hạ tầng ĐTĐM từ xa (từ hệ thống nội bộ của nhà cung cấp dịch vụ hoặc từ khách hàng bên ngoài). IAM cần cung cấp các tính năng xác thực và quản lý truy cập các thành phần hệ thống như mô-đun phần mềm, ứng dụng hoặc bộ dữ liệu đã tải xuống. IAM hỗ trợ triển khai phương thức, cơ chế xác thực và quản lý truy cập khác nhau trên các nền tảng, thành phần hệ thống khác nhau.

Bên cạnh đó, việc kiểm toán giao dịch cũng là tính năng bảo mật cho phép chống chối bỏ thông qua việc giám sát và phân tích các sự cố bảo mật nhằm ngăn chặn các cuộc tấn công mạng.

***4.3.3. Bảo đảm an toàn vật lý***

Hạ tầng ĐTĐM phải có biện pháp bảo vệ vật lý nhằm bảo đảm hoạt động ổn định và phòng, chống truy cập vật lý trái phép vào hệ thống. Quyền truy cập vào các thành phần trong hạ tầng ĐTĐM của nhà cung cấp dịch vụ phải được giới hạn, phân quyền truy cập phù hợp cho người quản lý, vận hành theo chức năng; đây là một phần của quy trình IAM. Phạm vi giới hạn, phân quyền truy cập vật lý phụ thuộc vào mức độ quan trọng của dữ liệu và thành phần người sử dụng được phép truy cập.

Cơ quan, tổ chức tham khảo yêu cầu an toàn cơ bản đối với hạ tầng vật lý tại tiêu chuẩn quốc gia TCVN 11930:2017 và TCVN 9250:2012, để có phương án thiết kế, thiết lập hạ tầng vật lý an toàn.

***4.3.4. Giao diện bảo mật***

Nhà cung cấp dịch vụ cần cung cấp giao diện bảo mật, an toàn để cho phép các khách hàng quản trị và sử dụng dịch vụ ĐTĐM an toàn từ xa. Giao diện an toàn cần đảm bảo không tồn tại các lỗ hổng, điểm yếu an toàn thông tin và cung cấp các chức năng cơ bản như mã hóa, xác thực và chống chối bỏ để bảo đảm việc truy cập và quản trị hệ thống từ xa được an toàn.

***4.3.5. Bảo đảm an toàn cho máy chủ ảo hóa***

Việc bảo đảm an toàn cho máy chủ ảo hóa liên quan đến việc bảo đảm an toàn cho thành phần quản lý máy ảo, môi trường lưu trữ của nhà cung cấp dịch vụ và HĐH, các ứng dụng của máy ảo của khách hàng. Nhà cung cấp dịch vụ có thể triển khai các giải pháp bảo vệ để bảo vệ chung cho các máy ảo của khách hàng mà không cần phải triển khai trên từng máy ảo riêng lẻ, ví dụ cung cấp chức năng phòng, chống mã độc và chống thư rác …Để tăng cường bảo đảm an toàn thông tin cho các máy ảo, các máy này sẽ được cấu hình tối ưu và tăng cường bảo mật (Hardening) như vô hiệu hóa các giao diện, giao diện lập trình ứng dụng (API) và các thành phần dịch vụ không sử dụng.

Cơ quan, tổ chức tham khảo yêu cầu an toàn cơ bản đối với máy chủ tại tiêu chuẩn quốc gia TCVN 11930:2017, để có phương án thiết kế, thiết lập cấu hình bảo mật phù hợp cho máy chủ.

***4.3.6. Bảo đảm an toàn mạng***

Hệ thống mạng là thành phần quan trọng để kết nối các thành phần khác nhau trong nền tảng ĐTĐM. Việc thiết kế, thiết lập hệ thống mạng cho phép phân tách các vùng mạng về vật lý, logic để có thể thiết lập chính sách, phân quyền truy cập phù hợp đối với từng đối tượng trong mỗi vùng mạng. Thêm nữa, việc trang bị các giải pháp bảo mật ở lớp mạng như một hạ tầng bảo mật, cho phép thiết lập chính sách và giải pháp bảo vệ chung cho các thành phần trong hạ tầng ĐTĐM.

Cơ quan, tổ chức tham khảo yêu cầu an toàn mạng tại tiêu chuẩn quốc gia TCVN 11930:2017 để có phương án thiết kế, thiết lập cấu hình bảo mật phù hợp cho hạ tầng mạng.

***4.3.7. An toàn dữ liệu***

Dữ liệu của các khách hàng khác nhau được lưu trữ chung trên nền tảng ĐTĐM của nhà cung cấp dịch vụ, do đó nhà cung cần có biện pháp quản lý truy cập và phân quyền truy cập dữ liệu phù hợp cho từng khách hàng. Việc này bảo đảm rằng khách hàng, các quản trị viên của nhà cung cấp dịch vụ không thể truy cập trái phép dữ liệu của khách hàng khác, thậm chí dữ liệu đó được mã hóa. Việc thực hiện quản lý cả người quản trị của nhà cung cấp dịch vụ có thể thực hiện trên cả môi trường vật lý và logic tùy thuộc vào yêu cầu, loại hình dịch vụ mà khách hàng sử dụng.

Hệ thống của nhà cung cấp dịch vụ cần cung cấp các tính năng mã hóa, xác thực, chống chối bỏ cho phép khách hàng quản lý và lưu trữ dữ liệu của mình an toàn trên nền tảng ĐTĐM của nhà cung cấp dịch vụ.

Cơ quan, tổ chức tham khảo yêu cầu an toàn dữ liệu tại tiêu chuẩn quốc gia TCVN 11930:2017 để có phương án thiết kế, thiết lập giải pháp bảo đảm an toàn dữ liệu phù hợp.

***4.3.8. Quản lý vận hành hạ tầng ĐTĐM***

Sau khi thiết kế, thiết lập hạ tầng ĐTĐM đáp ứng các yêu cầu an toàn thì việc quản lý, vận hành hệ thống nhằm duy trì tính ổn định và bảo đảm an toàn thông tin cho hệ thống trong quá trình vận hành khai thác là rất cần thiết.

Việc quản lý, vận hành nhằm bảo đảm an toàn thông tin cho hạ tầng ĐTĐM cơ bản bao gồm nhưng không giới hạn các hoạt động sau:

+ Xây dựng và thực thi chính sách bảo đảm an toàn thông tin cho hệ thống như: quản lý cấu hình, nâng cấp bản vá, đánh giá bảo mật, ứng phó sự cố và đảm bảo việc này được thực thi đáp ứng các yêu cầu an toàn thông tin cơ bản và tuân thủ các quy định của pháp luật và hợp đồng giữa các bên.

+ Giám sát, kiểm tra, đánh giá tính hiệu quả phương án bảo đảm an toàn thông tin của nhà cung cấp dịch vụ để phát hiện và cảnh báo sớm các nguy cơ có thể xảy ra làm ảnh hưởng đến các khách hàng.

Trong trường hợp chính sách bảo mật của nhà cung cấp dịch vụ cần thay đổi để đáp ứng các yêu cầu theo quy định và thực tế thì việc thay đổi này cần thông báo cho tất cả các khách hàng và các bên liên quan.

Cơ quan, tổ chức tham khảo yêu cầu an toàn cơ bản về quản lý tại tiêu chuẩn quốc gia TCVN 11930:2017 để có phương án xây dựng và thực thi chính sách bảo đảm an toàn thông tin phù hợp nhằm bảo đảm an toàn thông tin cho hạ tầng điện toán đám mây trong quá trình quản lý, vận hành, khai thác, sử dụng.

***4.3.9. Xây dựng phương án ứng cứu sự cố và khôi phục sau thảm họa***

Bất kỳ hệ thống nào dù được triển khai giải pháp bảo mật, tổ chức quản lý vận hành tốt đến đâu đều phải đối mặt với các nguy cơ, rủi ro mất an toàn thông tin. Do đó, mỗi hệ thống cần xây dựng phương án ứng cứu sự cố và khôi phục sau thảm họa để bảo đảm tính sẵn sàng và có phương án phù hợp khi có sự cố xảy ra.

Cơ quan, tổ chức thực hiện việc xây dựng hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng theo quy định tại Quyết định số 05/QĐ-TTg ngày 16/3/2017 và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017.

***4.3.10. Kiểm tra, đánh giá an toàn thông tin cho hạ tầng ĐTĐM***

Hạ tầng ĐTĐM phải được kiểm tra, đánh giá an toàn thông tin định kỳ hoặc đột xuất theo quy định của pháp luật tại Thông tư 03/2017/TT-BTTTT. Theo đó, nội dung kiểm tra đánh giá bao gồm: (1) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ; (2) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin; (3) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

Theo chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam, việc kiểm tra đánh giá an toàn thông tin cần được thực hiện bởi một đơn vị độc lập với đơn vị giám sát bảo vệ. Do đó việc thực hiện kiểm tra, đánh giá an toàn thông tin cho nền tảng ĐTĐM của một nhà cung cấp dịch vụ cần để bên thứ ba và cơ quan có thẩm quyền thực hiện.

Các tiêu chí đánh giá cụ thể được xác định căn cứ vào các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ, tiêu chuẩn, quy chuẩn quốc gia hoặc tiêu chuẩn quốc tế tương đương và các cam kết giữa nhà cung cấp dịch vụ và khách hàng.

Kết quả kiểm tra, đánh giá an toàn thông tin là cơ sở để các khách hàng đánh giá, lựa chọn nhà cung cấp dịch vụ phù hợp để sử dụng dịch vụ.

# 4.4. Tiêu chí, chỉ tiêu kỹ thuật an toàn thông tin cho hạ tầng ĐTĐM

Các yêu cầu được mô tả dưới đây là các tiêu chí, chỉ tiêu kỹ thuật an toàn thông tin cho cơ sở hạ tầng ĐTĐM. Cơ quan, tổ chức khi triển khai xây dựng, cung cấp, sử dụng cần lựa chọn nền tảng ĐTĐM đáp ứng các tiêu chí, chỉ tiêu kỹ thuật trong tài liệu này, tiêu chuẩn quốc gia TCVN 11930:2017 và các tiêu chuẩn, quy chuẩn kỹ thuật khác liên quan.

Yêu cầu về các tiêu chí, chỉ tiêu kỹ thuật cụ thể với từng tính năng và phương pháp đánh giá được mô tả chi tiết tại Phụ lục 2 tài liệu này.

***4.4.1. Yêu cầu tối thiểu về tính năng an toàn thông tin***

*a) Bảo vệ thông tin cá nhân của người dùng*

Cung cấp tính năng phòng chống việc mất mát, rò rỉ, giả mạo, thay đổi, lợi dụng thông tin cá nhân của người dùng trong cả quá trình truyền tin và lưu trữ.

*b) Tích hợp dịch vụ xác thực người dùng*

Cung cấp tính năng xác thực người dùng thông qua các dịch vụ bên thứ ba có thể được tích hợp vào (dựa trên, LDAP hoặc OpenID / SAM) trước khi người dùng truy cập vào các giao diện gồm cổng thông tin quản trị, danh mục dịch vụ và quản trị.

*c) Tích hợp điều khiển truy cập dựa trên vai trò - RBAC (Role-Based Access Control)*

Cho phép tích hợp điều khiển truy cập như tích hợp sẵn các quyền truy cập đã được định nghĩa trước; định nghĩa các quyền truy cập đối với các thao tác mà nhà cung cấp thực hiện trên tất cả các thành phần của nền tảng nhằm phục vụ mục đích quản trị; định nghĩa các quyền truy cập đối với các thao tác mà người sử dụng sử dụng dịch vụ điện toán đám mây thực hiện trên những thành phần của nền tảng mà người sử dụng muốn sử dụng và tuân theo thỏa thuận giữa hai bên.

*d) Giao tiếp giữa các thành phần qua kênh TLS*

Cho phép các thành phần giao tiếp qua kênh TLS.

*đ) Hỗ trợ TLS tự ký (Self-signed TLS)*

Hỗ trợ TLS tự ký như cho phép quản trị viên tạo các chứng thư điện tử tự ký (Self-signed) TLS; các chứng thư điện tử được tạo bởi một đơn vị cấp chứng thư (CA) tin cậy (trusted certificate authority).

*e) Tích hợp giao diện cổng thông tin quản trị hỗ trợ sử dụng kênh TLS*

Cung cấp tính năng tích hợp giao diện cổng thông tin quản trị hỗ trợ sử dụng kênh TLS dành cho người dùng đầu cuối và quản trị viên khi muốn kết nối qua kênh TLS.

*g) Chuyển hướng kết nối qua sử dụng TLS*

Cho phép quản trị viên cấu hình để áp dụng chính sách phải sử dụng kênh TLS đối với mọi kết nối truy cập vào giao diện cổng thông tin trên và dùng các phiên HTTP không mã hóa giống như là một lựa chọn dự phòng

*h) Ghi log hoạt động của các hành động*

Cho phép ghi log hoạt động của các hành động như ghi log hoạt động của các hành động thực hiện trên các thành phần; cho phép quản trị viên xem xét, kiểm tra log thu được.

*i) Tách biệt máy ảo với phần mềm giám sát máy ảo*

Cung cấp tính năng đảm bảo máy ảo được giám sát bởi một phần mềm giám sát máy ảo không gây ảnh hưởng đến phần mềm giám sát đó.

*k) Phân quyền cho máy ảo truy cập đến tài nguyên*

Cung cấp tính năng đảm bảo phần mềm giám sát máy ảo phân quyền cho máy ảo mà nó giám sát truy cập đến tài nguyên đúng theo chính sách quản trị nền tảng.

*l) Cấu hình cho phần mềm giám sát máy ảo*

Cho phép quản trị viên cấu hình cho phần mềm giám sát máy ảo và xác nhận tính hợp lệ của cấu hình phần mềm giám sát máy ảo.

*m) Bảo vệ dữ liệu*

Cung cấp tính năng phòng chống việc mất mát, rò rỉ, thay đổi dữ liệu trong cả quá trình lưu trữ trên các bộ nhớ dùng chung và truyền tin qua các mạng chia sẻ.

*n) Tách biệt các máy ảo với nhau*

Cung cấp tính năng tách biệt hoàn toàn các máy ảo khác nhau về logic (CPU, RAM, Network…).

*o) Đảm bảo các API của hệ thống có ít nhất 02 mức quyền truy cập đã định nghĩa sẵn cho các API của client.*

Cung cấp tính năng bảo đảm các chức năng quản trị và vận hành của hệ thống định nghĩa sẵn có các mức quyền truy cập đối với các API của client (ví dụ: quyền root và quyền user, trong đó quyền root cao hơn quyền user); chức năng quản trị và vận hành của hệ thống xác thực được client dựa trên các tiêu chí được định nghĩa trước bởi quản trị viên.

***4.4.2. Yêu cầu thiết lập cấu hình bảo mật cho cơ sở hạ tầng điện toán đám mây***

*a) Thiết lập cấu hình bảo mật đối với dịch vụ xác thực*

Yêu cầu thiết lập cấp hình: (1) Cấp quyền sở hữu các file cấu hình dịch vụ xác thực cho đúng user và group; (2) Kích hoạt kênh TLS trên server cung cấp dịch vụ xác thực; (3) Kích hoạt kênh TLS trên server cung cấp dịch vụ xác thực; (4) Sử dụng hàm băm mạnh cho các token tạo bởi hạ tầng khóa công khai PKI của dịch vụ xác thực; (5) Phòng chống tấn công DoS; (6) Phòng chống lợi dụng token admin để chiếm quyền quản trị; (7) Ẩn những thông tin nhạy cảm trong quá trình xác thực; (8) Thiết lập cơ chế đảm bảo an toàn cho quá trình sinh token.

*b) Thiết lập cấu hình bảo mật đối với dịch vụ quản trị giao diện dashboard*

Yêu cầu thiết lập cấp hình: (1) Cấp quyền sở hữu file cấu hình dịch vụ dashboard cho đúng user và group; (2) Cấp quyền truy cập file cấu hình dịch vụ dashboard; (3) Phòng chống tấn công XFS, CSRF, MitM, XSS; (4) Vô hiệu hóa tính năng tự động điền mật khẩu; (5) Vô hiệu hóa tính năng hiển thị bản rõ của mật khẩu; (6) Thiết lập cơ chế chỉ cho phép quản trị viên thay đổi mật khẩu; (7) Định nghĩa biểu thức chính quy kiểm tra mật khẩu; (8) Định nghĩa giá trị cho header X-Forwarded-Proto đối với các kết nối đến dịch vụ dashboard qua proxy và kênh TLS.

*c) Thiết lập cấu hình bảo mật đối với dịch vụ tính toán*

Yêu cầu thiết lập cấu hình: (1) Cấp quyền sở hữu các file cấu hình dịch vụ tính toán cho đúng user và group; (2) Cấp quyền truy cập các file cấu hình dịch vụ tính toán; (3) Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ tính toán; (4) Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ tính toán; (5) Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ tính toán và dịch vụ quản lý file ảnh của máy chủ ảo.

*d) Thiết lập cấu hình bảo mật đối với dịch vụ lưu trữ*

Yêu cầu thiết lập cấu hình: (1) Cấp quyền sở hữu các file cấu hình dịch vụ lưu trữ cho đúng user và group; (2) Cấp quyền truy cập các file cấu hình dịch vụ lưu trữ; (3) Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ lưu trữ; (4) Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ lưu trữ; (5) Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ lưu trữ và dịch vụ tính toán; (6) Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ lưu trữ và dịch vụ quản lý file ảnh của máy chủ ảo; (7) Thiết lập cơ chế đảm bảo an toàn vận hành các thiết bị NAS; (8) Phòng chống tấn công DoS; (9) Kích hoạt tính năng mã hóa phân vùng.

*đ) Thiết lập cấu hình bảo mật đối với file ảnh của của máy chủ ảo*

Yêu cầu thiết lập cấu hình: (1) Cấp quyền sở hữu các cấu hình file ảnh của máy chủ ảo cho đúng user và group; (2) Cấp quyền truy cập các cấu hình file ảnh của máy chủ ảo; (3) Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến file ảnh của máy chủ ảo; (4) Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến file ảnh của máy chủ ảo; (5) Phòng chống tấn công quét thăm dò cổng.

*e) Thiết lập cấu hình bảo mật đối với dịch vụ chia sẻ lưu trữ*

Yêu cầu thiết lập cấu hình: (1) Cấp quyền sở hữu các file cấu hình dịch vụ chia sẻ lưu trữ cho đúng user và group; (2) Cấp quyền truy cập các file cấu hình dịch vụ chia sẻ lưu trữ; (3) Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ chia sẻ lưu trữ; (4) Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ chia sẻ lưu trữ; (5) Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ chia sẻ lưu trữ và dịch vụ tính toán; (6) Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ chia sẻ lưu trữ và dịch vụ quản lý mạng; (7) Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ chia sẻ lưu trữ và dịch vụ lưu trữ; (8) Phòng chống tấn công DoS.

*g) Thiết lập cấu hình bảo mật đối với dịch vụ quản lý mạng*

Yêu cầu thiết lập cấu hình: (1) Cấp quyền sở hữu các file cấu hình dịch vụ quản lý mạng cho đúng user và group; (2) Cấp quyền truy cập các file cấu hình dịch vụ quản lý mạng; (3) Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ quản lý mạng; (4) Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ quản lý mạng; (5) Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ quản lý mạng và các đối tượng khác.

*h) Thiết lập cấu hình bảo mật đối với dịch vụ quản lý thông tin mật*

Yêu cầu thiết lập cấu hình: (1) Cấp quyền sở hữu các file cấu hình dịch vụ quản lý thông tin mật cho đúng user và group; (2) Cấp quyền truy cập các file cấu hình dịch vụ quản lý thông tin mật; (3) Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ quản lý thông tin mật; (4) Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ quản lý thông tin mật.

PHỤ LỤC 1
TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT TỐI THIỂU
CHO CƠ SỞ HẠ TẦNG ĐIỆN TOÁN ĐÁM MÂY

Bảng dưới đây mô tả tính năng và tiêu chí, chỉ tiêu kỹ thuật đối với từng tính năng cụ thể. Đối với tính năng có một tiêu chí, chỉ tiêu kỹ thuật thì việc đánh giá là đạt khi giải pháp cung cấp được tính năng đó, không đạt nếu giải pháp không cung cấp được tính năng đó.

Đối với tính năng có nhiều tiêu chí, chỉ tiêu kỹ thuật khác nhau thì tính năng đó đạt khi tất cả các tiêu chí, chỉ tiêu kỹ thuật đều đạt, không đạt khi một trong các tiêu chí, chỉ tiêu kỹ thuật không đạt.

| **STT** | **Tên tính năng** | **Tiêu chí, chỉ tiêu kỹ thuật** |
| --- | --- | --- |
| **I** | **Máy ảo** |
| 1 | Tạo máy ảo | Giải pháp cung cấp 03 tính năng sau:1. Tạo máy ảo mới thông qua giao diện đồ họa (GUI).2. Tạo máy ảo mới thông qua giao diện dòng lệnh (CLI).3. Tạo máy ảo mới thông qua giao diện lập trình ứng dụng (API) tích hợp với hệ thống khác. |
| 2 | Tạo nhiều máy ảo cùng một lúc | Giải pháp cung cấp 02 tính năng sau:1. Cho phép người dùng tạo nhiều máy ảo một lúc với số lượng tối thiểu 02 máy / 1 lần tạo.2. Cho phép người dùng tạo nhiều máy ảo một lúc với số lượng loại hệ điều hành khác nhau, tối thiểu 02 hệ điều hành khác nhau / 1 lần tạo. |
| 3 | Tùy biến máy ảo | Giải pháp cung cấp 04 tính năng sau:1. Cho phép người dùng tạo máy ảo từ tệp tin hệ điều hành mà hệ thống hỗ trợ.2. Cho phép người dùng tùy biến máy ảo muốn tạo và lưu lại máy ảo sau khi tùy biến thành tệp tin hệ điều hành.3. Lưu trữ tệp tin hệ điều hành do người dùng tạo ra trong nhóm tệp tin hệ điều hành tùy biến.4. Cho phép người dùng chọn tệp tin hệ điều hành trên giao diện cổng thông tin quản trị (web portal) để tạo máy ảo tùy ý. |
| 4 | Nhập / xuất máy ảo | Giải pháp cung cấp 03 tính năng sau:1. Cho phép người dùng tải lên và tạo máy ảo từ những tệp tin hệ điều hành có định dạng là VHD, VMDK, QCOW2 hoặc tương đương.2. Lưu lại máy ảo đang chạy thành các tệp tin hệ điều hành có định dạng là VHD, VMDK, QCOW2 hoặc tương đương.3. Cho phép người dùng tải xuống các tệp tin hệ điều hành. |
| 5 | Chuyển đổi định dạng tệp tin hệ điều hành | Giải pháp cung cấp tính năng cho phép người dùng chuyển đổi qua lại các định dạng tệp tin hệ điều hành là VHD, VMDK, QCOW2 hoặc tương đương cùng một lúc. |
| 6 | Triển khai máy ảo có cấu hình cao | Giải pháp cung cấp 02 tính năng sau:1. Hỗ trợ triển khai các máy ảo có số lượng lớn nhân xử lý và có bộ nhớ kích thước lớn mà nặng về bộ nhớ (memory-intensive) hoặc nặng về nhân xử lý (processor-intensive).2. Hỗ trợ ít nhất 64 vCPU và 128 GB RAM. |
| 7 | Thay đổi cấu hình phần cứng máy ảo | Giải pháp cung cấp 02 tính năng sau:1. Cho phép người dùng thay đổi cấu hình phần cứng máy ảo trong khi các máy ảo đang chạy, không yêu cầu đối với trường hợp giảm kích thước ổ cứng.2. Thông báo cho người dùng ngay lập tức khi cần phải khởi động lại máy ảo để áp dụng thay đổi. |
| 8 | Di chuyển máy ảo giữa các máy chủ vật lý | Giải pháp cung cấp tính năng di chuyển dữ liệu của một máy ảo đang chạy từ máy vật lý này sang máy vật lý khác mà không phải tắt hoặc khởi động lại máy ảo. |
| 9 | Di chuyển dữ liệu máy ảo giữa các bộ lưu trữ khác nhau  | Giải pháp cung cấp tính năng di chuyển dữ liệu của một máy ảo đang chạy từ thiết bị lưu trữ này sang thiết bị lưu trữ khác mà không phải tắt hoặc khởi động lại. |
| 10 | Khôi phục máy ảo sau khi có lỗi xảy ra | Giải pháp cung cấp tính năng khôi phục / khởi động lại tự động máy ảo (khi cơ sở hạ tầng vật lý phát sinh lỗi) mà phải thỏa mãn 02 điều kiện sau:1. Phát hiện được có lỗi đã xảy ra khi hệ thống gặp sư cố.2. Tự động khởi động lại máy ảo khi phát hiện lỗi. |
| 11 | Tính năng phân bổ máy ảo trên các máy vật lý khác nhau (anti-affinity) | Giải pháp cung cấp tính năng cho phép người dùng cấu hình các thông số trên máy ảo để xác định vị trí triển khai các máy ảo khác nhau trên các máy vật lý hoặc trung tâm dữ liệu khác nhau (nhằm phòng tránh sự ảnh hưởng của vấn đề nào đó về phần cứng hoặc cơ sở hạ tầng đối với tất cả các máy ảo cùng một lúc). |
| 12 | Tính năng hỗ trợ tự động thay đổi cấu hình hệ thống mức cơ bản | Giải pháp cung cấp 02 tính năng sau:Tính năng hỗ trợ tự động thay đổi theo chiều ngang thông qua 03 cách bao gồm bật / tắt máy ảo; tạo ra các máy ảo mới dựa theo kế hoạch được lập thủ công trước đó; thiết lập cấu hình tài nguyên cho máy ảo theo cấu hình được định nghĩa trước. |
| 13 | Tính năng phân bổ máy ảo trên cùng máy vật lý (affinity) | Giải pháp cung cấp 02 tính năng sau:1. Cho phép người dùng định nghĩa các quy tắc hợp tác trao đổi dữ liệu giữa các máy ảo.2. Hỗ trợ triển khai các máy ảo thường xuyên trao đổi dữ liệu với nhau trên cùng một máy vật lý. |
| 14 | Truy cập vào máy ảo thông qua giao diện bảng điều khiển (console) | Giải pháp cung cấp 02 tính năng sau:1. Cho phép người dùng truy cập vào máy ảo thông qua giao diện bảng điều khiển (console)2. Cung cấp giao diện bảng điều khiển (console) tương thích với các trình duyệt phổ biến. |
| 15 | Gắn các tệp tin định dạng ISO trên máy ảo | Giải pháp cung cấp tính năng Gắn các tệp tin định dạng ISO trên máy ảo (các tệp tin định dạng ISO có thể nằm trên một kho dữ liệu riêng của giải pháp). |
| 16 | Sao lưu/khôi phục máy ảo | Giải pháp cung cấp 05 tính năng sau:1. Cho phép người dùng sao lưu máy ảo thành các bản chụp (snapshot) theo kế hoạch được lập thủ công hoặc định kỳ trước đó.2. Lưu trữ bản chụp (snapshot) được tạo ra dựa theo thông tin về thời điểm tạo.3. Cho phép người dùng sao lưu máy ảo thông qua cổng thông tin quản trị hoặc CLI.4. Cho phép người dùng sao lưu ít nhất 07 phiên bản khác nhau của một máy ảo.5. Cho phép người dùng khôi phục máy ảo từ bản chụp (snapshot). |
| 17 | Giới hạn IOPS và băng thông ổ đĩa của máy ảo | Giải pháp cung cấp 02 tính năng sau:1. Cho phép người quản trị và người dùng giới hạn IOPS của máy ảo.2. Cho phép người quản trị và người dùng giới hạn băng thông ổ đĩa của máy ảo. |
| 18 | Giới hạn băng thông mạng của máy ảo | Giải pháp cung cấp tính năng cho phép người dùng giới hạn băng thông mạng của máy ảo cho cả hai luồng lưu lượng mạng vào / ra. |
| 19 | Triển khai máy ảo cần sử dụng các công nghệ tăng tốc (accelerator) | Giải pháp cung cấp tính năng hỗ trợ cấu hình NUMA and Transparent Hugepage, PCI Pass through, SR-IOV, OVS-DPDK, CPU pinning, DPDK và Direct I/O, khi triển khai các máy ảo cần sử dụng các công nghệ tăng tốc (accelerator). |
| 20 | Tự động chọn máy chủ vật lý khi tạo một máy ảo mới | Giải pháp cung cấp tính năng cho phép tự động chọn máy chủ vật lý để triển khai máy ảo mới tạo nhằm cân bằng tải giữa các máy chủ vật lý. |
| 21 | Thiết lập hoặc thiết lập lại mật khẩu cho tài khoản quản trị của máy ảo | Giải pháp cung cấp tính năng cho phép quản trị viên nhập mật khẩu cho tài khoản quản trị của máy ảo. |
| 22 | Định nghĩa, cấu hình và khởi tạo cụm gồm nhiều máy ảo | Giải pháp cung cấp tính năng cho phép người dùng định nghĩa một cluster mới tùy ý.- Ví dụ: một cụm máy chủ ảo 3 tầng gồm 06 máy ảo (02 máy chạy ứng dụng ở mạng công cộng, 02 máy chạy các dịch vụ backend ở mạng cục bộ và 02 máy chạy cơ sở dữ liệu ở mạng cục bộ) có thể được tích hợp với tính năng tự động thay đổi cấu hình hệ thống. |
| **II** | **Thiết bị lưu trữ** |
| 1 | Tích hợp các thiết bị lưu trữ truyền thống và giải pháp lưu trữ bằng phần mềm | Giải pháp cung cấp 02 tính năng sau:1. Hỗ trợ giải pháp lưu trữ bằng phần mềm (SDS-Software-Defined Storage).2. Hỗ trợ tích hợp các thiết bị SAN (Storage Area Network) và NAS (Network-Attached Storage). |
| 2 | Tích hợp các dịch vụ lưu trữ | Giải pháp cung cấp 02 tính năng sau:1. Hỗ trợ lưu trữ dạng khối (block storage)2. Hỗ trợ lưu trữ dạng đối tượng (object storage) và lưu trữ dạng tệp tin (file storage) |
| 3 | Áp dụng chính sách đối với các dịch vụ lưu trữ phân tầng | Giải pháp cung cấp tính năng cho phép người dùng thiết lập chính sách đối với các dịch vụ lưu trữ phân tầng.- Ví dụ: một quản trị viên về việc lưu trữ dữ liệu có thể lập kế hoạch lưu những dữ liệu không thường xuyên sử dụng trên thiết bị SATA chậm hơn và ít tốn kém hơn. |
| 4 | Gắn bộ nhớ trên nhiều máy ảo  | Giải pháp cung cấp 02 tính năng sau:1. Gắn một ổ cứng ảo (từ SAN hoăc SDS) trên nhiều máy ảo ổ cứng ảo có thể ở chế độ chỉ đọc.2. Gắn một hệ thống tệp tin chia sẻ dùng chung trên nhiều máy ảo. |
| 5 | Quản lý, phân bổ các tham số hiệu năng của ổ cứng ảo | Giải pháp cung cấp tính năng cho phép người dùng chọn một phân lớp hiệu năng cho các ổ cứng ảo.- Ví dụ: IOPS hoặc băng thông (đo bằng Mbps). |
| 6 | Tự động phân bổ dữ liệu trên vùng lưu trữ | Giải pháp cung cấp tính năng tự động phân bổ dữ liệu trên vùng lưu trữ để phân tải cho các ổ đĩa. |
| 7 | Mở rộng vùng lưu trữ | Giải pháp cung cấp tính năng cho phép người dùng tăng dung lượng của một vùng lưu trữ đã có sẵn. |
| 8 | Mở rộng các ổ cứng ảo | Giải pháp cung cấp tính năng cho phép người dùng tăng kích thước của một ổ cứng ảo (ổ cứng ảo của thiết bị SAN hoặc SDS) đã có sẵn mà không phải cấp thêm ổ cứng ảo mới hoặc sao chép dữ liệu sang ổ cứng ảo mới. |
| 9 | Di dời dữ liệu giữa các vùng lưu trữ khi hệ thống đang vận hành | Giải pháp cung cấp tính năng cho phép quản trị viên di chuyển dữ liệu giữa các vùng lưu trữ khi hệ thống đang vận hành. |
| 10 | Sao lưu ổ cứng ảo | Giải pháp cung cấp 03 tính năng sau:1. Cho phép người dùng sao lưu ổ cứng ảo tại một thời điểm bất kỳ thành các bản chụp (snapshot) thông qua các cách thức tự thao tác (self-service.)2. Sử dụng các bản chụp (snapshot) thông qua cách thức tự thao tác (self-service) với mục đích để cấp thêm máy ảo mới. |
| 11 | Khả năng cung cấp lưu trữ dạng đối tượng (Object storage) | Giải pháp cung cấp tính năng hỗ trợ khả năng cung cấp lưu trữ dạng đối tượng (Object storage) mà phải thỏa mãn các điều kiện sau:1. Lưu trữ và truy xuất dữ liệu thông qua API trên dịch vụ web.2. Hỗ trợ khả năng thay đổi đối với từng đối tượng đơn lẻ và toàn bộ lưu trữ dạng đối tượng (Object storage). |
| 12 | Mã hóa dữ liệu | Giải pháp cung cấp tính năng cho phép người dùng mã hóa dữ liệu hoặc cấu trúc dữ liệu. |
| 14 | Sao lưu đối tượng  | Giải pháp cung cấp 02 tính năng sau:1. Cho phép người dùng sao lưu đối tượng thành nhiều phiên bản tại những thời điểm khác nhau nhằm mục đích phòng ngừa việc mất mát dữ liệu do ghi đè hoặc xóa đối tượng.2. Cho phép người dùng cấu hình việc sao lưu thông qua CLI, GUI hoặc API đối với từng đối tượng. |
| **III** | **Mạng và mạng định nghĩa bằng phần mềm (Software-Defined Networking - SDN)** |
| 1 | Quản lý hiệu năng mạng | Giải pháp cung cấp tính năng cho phép người dùng quản lý hiệu năng đối với từng mạng mà máy ảo kết nối đến bao gồm việc giới hạn băng thông, độ trễ, quản lý chất lượng dịch vụ (QoS).  |
| 2 | Tích hợp nhiều cổng giao tiếp mạng ảo trên vNIC một máy ảo | Giải pháp cung cấp 04 tính năng sau:1. Cho phép nhiều địa chỉ IP khác nhau được gán cho một máy ảo thông qua tích hợp nhiều cổng giao tiếp mạng ảo trên vNIC với địa chỉ MAC khác nhau cho máy ảo đó.2. Cho phép người dùng sử dụng kết hợp cả địa chỉ IP public và địa chỉ IP private để gán cho máy ảo, ngoại trừ trường hợp hệ điều hành máy ảo mà không hỗ trợ.3. Cho phép người dùng định nghĩa nhiều phân đoạn mạng ảo mà không cần dùng phần mềm bên thứ ba.4. Cho phép người dùng định nghĩa nhiều mạng con cho mỗi mạng ảo. |
| 3 | Hỗ trợ khả năng dự phòng từ mức vật lý cho các mạng mà máy ảo kết nối đến  | Giải pháp cung cấp tính năng hỗ trợ kiến trúc thiết kế đảm bảo khả năng dự phòng mà phải thỏa mãn 02 điều kiện sau:1. Hỗ trợ từ mức vật lý (ít nhất ở mức cổng vật lý – NIC) cho các mạng mà máy ảo kết nối đến (ví dụ: nếu một máy chủ vật lý có 02 cổng / 1 NIC thì khi một cổng gặp sự cố cũng không ảnh hưởng đến kết nối mạng của máy ảo).2. Hoạt động ở mức active-active hoặc active-standby để cải thiện băng thông và bảo đảm tính sẵn sàng. |
| 4 | Cấp phát địa chỉ IP  | Giải pháp cung cấp 02 tính năng sau:1. Cho phép một máy ảo được gán địa chỉ IP động và địa chỉ IP này phải luôn không đổi giá trị trong suốt quá trình hoạt động của máy ảo.2. Cho phép một máy ảo được gán địa chỉ IP tĩnh (bao gồm cả địa chỉ IP public và private).  |
| 5 | Liên kết với bộ chuyển mạch và bộ định tuyến thông thường | Giải pháp cung cấp tính năng SDN hoặc Liên kết với các bộ chuyển mạch và bộ định tuyến thông thường của nhiều hãng khác nhau. |
| 6 | Phòng chống tấn công giả mạo địa chỉ IP và giả mạo gói tin ARP | Giải pháp cung cấp tính năng phòng chống tấn công giả mạo địa chỉ IP và giả mạo gói tin ARP đối với mạng nội bộ của máy ảo hoặc các mạng mà máy ảo và máy vật lý kết nối đến. |
| 7 | Hỗ trợ VLAN và VXLAN | Giải pháp cung cấp tính năng cho phép người dùng định nghĩa các mạng ảo bao gồm cả VLAN và VXLAN. |
| 8 | Hỗ trợ bộ định tuyến ảo | Giải pháp cung cấp tính năng cho phép người dùng sử dụng các chức năng của bộ định tuyến (NAT, định tuyến giữa các VLAN,…) để quản lý kết nối giữa các mạng. |
| 9 | Tích hợp dịch vụ cân bằng tải | Giải pháp cung cấp tính năng cho phép người dùng sử dụng dịch vụ cân bằng tải đã được tích hợp sẵn (dịch vụ bao gồm các chức năng cấu hình giám sát, cấu hình cho thiết bị đầu cuối và tương thích với nhiều máy ảo đang kết nối với nhiều mạng ảo khác nhau). |
| 10 | Cấu hình chính sách truy cập cho từng cổng trên máy ảo | Giải pháp cung cấp tính năng cho phép người dùng cấu hình chính sách truy cập cho từng cổng (thuộc cổng giao tiếp mạng ảo trên vNIC) trên những máy ảo đang chạy. |
| 11 | Tích hợp dịch vụ tường lửa | Giải pháp cung cấp tính năng cho phép người dùng sử dụng dịch vụ tường lửa đã được tích hợp sẵn (dịch vụ phải hoạt động bình thường trên tầng IP và Domain). |
| 12 | Hỗ trợ IPv6 cho cả mạng vật lý và mạng ảo | Giải pháp cung cấp tính năng hỗ trợ máy ảo hoặc cổng kết nối (ví dụ: bộ cân bằng tải) sử dụng IPv6 trên cả mạng vật lý và mạng ảo. |
| 13 | Tách biệt các mạng ảo với nhau | Giải pháp cung cấp tính năng tách biệt hoàn toàn các mạng ảo khác nhau. |
| 14 | Đảm bảo sự hao phí băng thông đường truyền kết nối giữa các mạng không vượt quá 10% | Giải pháp cung cấp tính năng đảm bảo sự hao phí băng thông đường truyền kết nối giữa máy ảo với máy ảo và máy ảo với thành phần bên ngoài không vượt quá 10%.- Ví dụ: nếu thiết lập 02 mạng VXLAN cho 02 máy ảo khác nhau trong mạng vật lý có băng thông là 10 Gbps thì băng thông thực tế của đường truyền kết nối giữa các máy ảo này phải > 9 Gbps. |
| 15 | Đảm bảo hạ tầng kỹ thuật cho máy vật lý và máy ảo có tính sẵn sàng cao | Giải pháp cung cấp tính năng đảm bảo máy vật lý và máy ảo chạy trên hạ tầng kỹ thuật có tính sẵn sàng cao, đảm bảo tính nguyên vẹn và tính bí mật của dữ liệu. |
| 16 | Hỗ trợ cấu trúc liên kết mạng có tính phân cấp do người dùng định nghĩa | Giải pháp cung cấp tính năng cho phép người dùng tự thiết kế các thành phần và sơ đồ mạng bao gồm tường lửa ảo, VLAN / VXLAN / GRE, mạng con, NAT, bộ cân bằng tải ảo. |
| 17 | Hỗ trợ tính năng tạo bộ chuyển mạch ảo | Giải pháp cung cấp tính năng tạo bộ chuyển mạch ảo và bộ định tuyến ảo |
| 18 | Tách biệt các mặt phẳng SDN với nhau | Giải pháp cung cấp tính năng tách biệt các mặt phẳng điều khiển, mặt phẳng chuyển tiếp và mặt phẳng quản trị với nhau. |
| 19 | Hỗ trợ Open Flow hoặc tương đương | Giải pháp cung cấp tính năng hỗ trợ OpenFlow cho SDN hoặc tương đương. |
| 20 | Tính năng tích hợp nền tảng điện toán đám mây | Giải pháp cung cấp tính năng hỗ trợ API sử dụng nền tảng điện toán đám mây để tạo bộ chuyển mạch ảo và bộ định tuyến ảo |
| 21 | Quản trị và điều khiển bộ chuyển mạch ảo và bộ định tuyến ảo | Giải pháp cung cấp tính năng quản trị và điều khiển bộ chuyển mạch ảo và bộ định tuyến ảo |
| 22 | Tự động tạo và quản trị bộ chuyển mạch ảo và bộ định tuyến ảo | Giải pháp cung cấp tính năng tự động tạo và quản trị bộ chuyển mạch ảo và bộ định tuyến ảo |
| 23 | Hỗ trợ AAA | Giải pháp cung cấp tính năng cho phép xác thực, phân quyền, ghi log hoạt động (authenticate, authorize, account – AAA) người dùng. |
| 24 | Tính năng quản trị các thành phần trong mạng | Giải pháp cung cấp tính năng cho phép người dùng sử dụng SNMP, Netconf hoặc tương đương có chức năng quản trị các thành phần khác trong mạng. |
| 25 | Tính năng hỗ trợ đảm bảo bộ điều khiển có tính sẵn sàng cao | Giải pháp cung cấp tính năng đảm bảo bộ điều khiển cho SDN có tính sẵn sàng cao. |
| 26 | Tính năng hỗ trợ Jumbo Frame(khuyến nghị áp dụng) | Giải pháp cung cấp tính năng sử dụng Jumbo Frame trong việc truyền tải gói tin. |
| 27 | Tính năng tích hợp CLI và GUI | Giải pháp cung cấp tính năng cho phép người dùng cấu hình, quản lý các thành phần trong mạng, bộ điều khiển cho SDN thông qua CLI và GUI. |
| 28 | Tính năng hỗ trợ bộ chuyển mạch ảo và bộ định tuyến ảo | Giải pháp cung cấp 09 tính năng sau:1. Hỗ trợ SPAN, RSPAN hoặc tương đương.2. Hỗ trợ LACP (mode 1, 2, 3, 4) từ máy ảo, máy vật lý.3. Hỗ trợ 802.1Q VLAN with trunking. 4. Hỗ trợ multicast snooping.5. Hỗ trợ LLDP.6. Hỗ trợ STP, RSTP hoặc tương đương.7. Hỗ trợ quản lý chất lượng dịch vụ (QoS).8. Hỗ trợ áp dụng chính sách lưu lượng cho từng máy ảo.9. Hỗ trợ VXLAN. |
| **IV** | **Máy vật lý** |
| 1 | Tự động cài đặt hệ điều hành và phần mềm giám sát máy ảo (hypervisor) | Giải pháp cung cấp tính năng tự động cài đặt hệ điều hành và phần mềm giám sát máy ảo sau khi có những thiết bị (ảo hoặc vật lý) mới truy cập mạng. Cho phép người dùng hoặc các thiết bị khác trong mạng có thể sử dụng, giao tiếp với chúng. |
| 2 | Triển khai nhiều phiên bản hệ điều hành Windows và Linux cho máy vật lý | Giải pháp cung cấp 07 tính năng sau:1. Hỗ trợ triển khai các phiên bản hệ điều hành Windows 8 và 10.2. Hỗ trợ triển khai các phiên bản hệ điều hành Windows Server 2012 và 2016.3. Hỗ trợ triển khai các phiên bản hệ điều hành Ubuntu 14.04, 16.04 và 18.04.4. Hỗ trợ triển khai các phiên bản hệ điều hành CentOS 6.x và 7.x.5. Hỗ trợ triển khai các phiên bản hệ điều hành RHEL 6 và 7.6. Hỗ trợ triển khai các phiên bản hệ điều hành Oracle Linux 6 và 7.7. Hỗ trợ các phiên bản hệ điều hành windows, ubuntu, centos, rhel, oracle linux, linux hiện hành. |
| 3 | Quản trị qua kênh truyền tín hiệu riêng biệt | Giải pháp cung cấp tính quản trị qua kênh truyền tín hiệu riêng biệt thông qua giao diện quản lý nền tảng thông minh (IPMI), sử dụng một trong các giao diện: iRMC, iLO, IDRAC, UCS hoặc tương đương. |
| 4 | Truy cập vào máy vật lý thông qua giao diện bảng điều khiển(console) | Giải pháp cung cấp tính năng cho phép người dùng truy cập vào máy vật lý thông qua giao diện bảng điều khiển(console) |
| 5 | Cấu hình cơ chế dự phòng cho ổ cứng (RAID - Redundant Arrays of Independent Disks) trên máy vật lý | Giải pháp cung cấp tính năng cho phép người dùng cấu hình RAID trên máy vật lý. |
| **V** | **Quản trị và vận hành** |
| 1 | Định nghĩa các hành động sau khi tạo hoặc xóa máy ảo | Giải pháp cung cấp tính năng cho phép quản trị viên định nghĩa các hành động sau khi tạo hoặc xóa máy ảo. |
| 2 | Thực hiện một hành động do người dùng chỉ định sẵn sau khi quá trình khởi động hoàn thành | Giải pháp cung cấp tính năng thực hiện một hành động do người dùng chỉ định sẵn thông qua cách thức tự hành (self-service) sau khi quá trình khởi động lần đầu hoàn thành đối với máy ảo mới tạo. |
| 3 | Hỗ trợ quản trị cấu hình | Giải pháp cung cấp tính năng hỗ trợ quản trị cấu hình (thông qua Ansible, Puppet, Chef hoặc SaltStack) mà phải thỏa mãn 03 điều kiện sau:1. Hoạt động như một dịch vụ được tích hợp sẵn để cho phép người dùng quản lý, kiểm tra các cấu hình và quy trình triển khai.2. Tự động hóa toàn bộ quy trình triển khai, nâng cấp, cập nhật và vá lỗi. 3. Tích hợp các thành phần vận hành tự động có khả năng được cấu hình thông qua các ngôn ngữ lập trình (như YAML,…). |
| 4 | Quản lý tài nguyên | Giải pháp cung cấp 02 tính năng sau:1. Cho phép quản trị viên giám sát, đánh giá lịch sử sử dụng tài nguyên của các máy ảo.2. Đưa ra các khuyến nghị về việc cấp thêm tài nguyên khi cần thiết. |
| 5 | Quản lý bản vá | Giải pháp cung cấp 03 tính năng sau:1. Tự động tạo thống kê, báo cáo về các bản vá đã được cập nhật.2. Tự động áp dụng các bản vá lên nhiều máy chủ một lúc.3. Khôi phục các bản vá đã cập nhật. |
| 6 | Tích hợp giao diện cổng thông tin quản trị | Giải pháp cung cấp 02 tính năng sau:1. Tích hợp giao diện cổng thông tin quản trị có tính tự hành cho người dùng đầu cuối (để người dùng tự quản lý tài nguyên được cấp) và giao diện cổng thông tin quản trị cho quản trị viên.3. Hỗ trợ giao diện cổng thông tin quản trị tương thích ít nhất 02 loại trình duyệt web là Firefox và Chrome  |
| 7 | Tùy biến giao diện cổng thông tin quản trị | Giải pháp cung cấp tính năng cho phép người dùng tùy biến giao diện cổng thông tin quản trị về hiển thị các thông số, tiêu chí như trạng thái, hiệu năng, tính sẵn sàng của tập hợp các máy chủ, dịch vụ. |
| 8 | Quản lý, giám sát nền tảng hạ tầng dịch vụ điện toán đám mây | Giải pháp cung cấp tính năng cho phép người dùng quản lý, giám sát cơ sở hạ tầng vật lý và ảo mà phải thỏa mãn 05 điều kiện sau:1. Hiển thị theo thời gian thực các thông số giám sát về CPU (idle, used, iowait, stealth), RAM, thiết bị lưu trữ, mạng.2. Cho phép người dùng cấu hình tùy theo ý muốn về cảnh báo hoặc báo cáo khi có sự cố xảy ra.3. Cho phép người dùng cấu hình khoảng thời gian lấy mẫu các thông số giám sát.4. Hiển thị các giá trị về thời gian ít nhất với các mức là giây, phút, giờ, ngày.5. Giám sát được các thành phần của cơ sở hạ tầng vật lý bao gồm bộ chuyển mạch, bộ định tuyến, tủ chứa máy chủ và các thiết bị lưu trữ. |
| 9 | Cảnh báo khi có sự kiện / sự cố về cơ sở hạ tầng xảy ra | Giải pháp cung cấp tính năng gửi cảnh báo cho người dùng khi có sự kiện / sự cố về cơ sở hạ tầng xảy ra mà phải thỏa mãn 05 điều kiện sau:1. Gửi cảnh báo khi giá trị ngưỡng về giám sát hiệu năng được kích hoạt. 2. Tạo cảnh báo trong vòng một phút kể từ khi một giá trị ngưỡng được kích hoạt.3. Cho phép người dùng định nghĩa ít nhất 03 giá trị ngưỡng khác nhau dành cho việc cảnh báo.4. Giải pháp cho phép người dùng thiết lập các giá trị ngưỡng đối với từng thành phần một.5. Giải pháp cho phép gửi cảnh báo qua email, SMS. |
| 10 | Thu thập và lưu trữ log hệ thống | Giải pháp cung cấp tính năng thu thập, lưu trữ và xoay vòng định kỳ log hệ thống về các tác vụ tạo, đọc, cập nhật, xóa - CRUD (Create, Read, Update, Delete – tạo, đọc, cập nhật, xóa), tài nguyên được sử dụng,… |
| 11 | Tích hợp API giám sát dữ liệu | Giải pháp cung cấp tính năng tích hợp API dành cho giám sát dữ liệu để cho phép bên thứ 3 thực hiện giám sát, phân tích dữ liệu qua API. |
| 12 | Ghi log về các sự kiện liên quan đến tài khoản | Giải pháp cung cấp tính năng ghi log về các sự kiện liên quan đến tài khoản mà phải thỏa mãn 03 điều kiện sau:1. Ghi log về các thao tác đăng nhập tài khoản, quản lý tài khoản bao gồm tạo / xoá / lập nhóm / gắn thẻ cho tài khoản người dùng và các thao tác khác (ví dụ: gán quyền, thiết lập số lượng tài khoản người dùng, thay đổi mật khẩu của tài khoản người dùng,…).2. Cho phép người dùng xem các bản ghi log thông qua giao diện có tính tự hành và khả năng xuất các bản ghi log để lưu giữ lâu hơn. |
| **VI** | **Tích hợp** |
| 1 | Tích hợp giao diện tương tác với thành phần quản lý chức năng mạng ảo (Virtual Network Function – VNF) | Giải pháp cung cấp tính năng tích hợp giao diện tương tác với thành phần VNF từ các hãng khác nhau, tuân theo kiến trúc ETSI MANO để hỗ trợ quản lý vòng đời VNF cũng như khả năng mở rộng. |
| 2 | Hỗ trợ thư viện phục vụ cho lập trình, phát triển phần mềm tương tác với hệ thống | Giải pháp cung cấp tính năng hỗ trợ các thư viện (mã nguồn mở hoặc tự nhà cung cấp dịch vụ điện toán đám mây tạo) phục vụ cho lập trình, phát triển phần mềm tương tác với hệ thống mà phải thỏa mãn 03 điều kiện sau:1. Tương thích với ít nhất 03 trong số ngôn ngữ lập trình phổ biến bao gồm Java, .NET, Perl, Node.js, PHP, Python, Ruby và PowerShell.2. Bao gồm các dịch vụ cốt lõi là vận hành, tính toán, lưu trữ và kết nối mạng.3. Có tài liệu kỹ thuật và ví dụ về mã nguồn. |
| **VII** | **Các yêu cầu khác** |
| 1 | Hỗ trợ máy chủ có kiến trúc CPU x86\_64 | Giải pháp cung cấp tính năng hỗ trợ cài đặt, triển khai, vận hành hệ thống trên máy chủ có kiến trúc CPU x86-based (bao gồm bộ xử lý Intel và AMD) và những loại máy chủ có 2 hoặc 4 nhân của các hãng Dell, HP, IBM, Cisco. |
| 2 | Đồng bộ thời gian | Giải pháp cung cấp tính năng đồng bộ thời gian cho tất cả các thành phần trong hệ thống. |

PHỤ LỤC 2
TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN
CHO HẠ TẦNG ĐIỆN TOÁN ĐÁM MÂY

2.1. Yêu cầu cơ bản về tính năng an toàn thông tin

Bảng dưới đây mô tả tính năng và tiêu chí, chỉ tiêu kỹ thuật đối với từng tính năng cụ thể. Đối với tính năng có một tiêu chí, chỉ tiêu kỹ thuật thì việc đánh giá là đạt khi giải pháp cung cấp được tính năng đó, không đạt nếu giải pháp không cung cấp được tính năng đó.

Đối với tính năng có nhiều tiêu chí, chỉ tiêu kỹ thuật khác nhau thì tính năng đó đạt khi tất cả các tiêu chí, chỉ tiêu kỹ thuật đều đạt, không đạt khi một trong các tiêu chí, chỉ tiêu kỹ thuật không đạt.

| **STT** | **Tên tính năng** | **Tiêu chí, chỉ tiêu kỹ thuật** |
| --- | --- | --- |
| 1 | Bảo vệ thông tin cá nhân của người dùng | Giải pháp cung cấp tính năng phòng chống việc mất mát, rò rỉ, giả mạo, thay đổi, lợi dụng thông tin cá nhân của người dùng trong cả quá trình truyền tin và lưu trữ. |
| 2 | Tích hợp dịch vụ xác thực người dùng | Giải pháp cung cấp tính năng xác thực người dùng thông qua các dịch vụ bên thứ ba có thể được tích hợp vào (dựa trên, LDAP hoặc OpenID / SAM) trước khi người dùng truy cập vào các giao diện gồm cổng thông tin quản trị, danh mục dịch vụ và quản trị. |
| 3 | Tích hợp điều khiển truy cập dựa trên vai trò - RBAC (Role-Based Access Control) | Giải pháp cung cấp 03 tính năng sau:1. Tích hợp sẵn các quyền truy cập đã được định nghĩa trước bao gồm ít nhất 02 quyền mức quản trị dành cho nhà cung cấp dịch vụ điện toán đám mây (bên cung cấp) và người sử dụng sử dụng dịch vụ điện toán đám mây (bên sử dụng).2. Cho phép nhà cung cấp dịch vụ điện toán đám mây định nghĩa các quyền truy cập đối với các thao tác mà nhà cung cấp thực hiện trên tất cả các thành phần của nền tảng nhằm phục vụ mục đích quản trị.3. Cho phép nhà cung cấp dịch vụ điện toán đám mây định nghĩa các quyền truy cập đối với các thao tác mà người sử dụng sử dụng dịch vụ điện toán đám mây thực hiện trên những thành phần của nền tảng mà người sử dụng muốn sử dụng và tuân theo thỏa thuận giữa hai bên. |
| 4 | Giao tiếp giữa các thành phần qua kênh TLS | Giải pháp cung cấp tính năng cho phép các thành phần giao tiếp qua kênh TLS. |
| 5 | Hỗ trợ TLS tự kí (Self-signed TLS) | Giải pháp cung cấp 02 tính năng sau:1. Cho phép quản trị viên tạo các chứng thư điện tử tự kí (Self-signed) TLS để đẩy nhanh quá trình triển khai.2. Cho phép các chứng thư điện tử được tạo bởi một đơn vị cấp chứng thư (CA) tin cậy (trusted certificate authority). |
| 6 | Tích hợp giao diện cổng thông tin quản trị hỗ trợ sử dụng kênh TLS | Giải pháp cung cấp tính năng tích hợp giao diện cổng thông tin quản trị hỗ trợ sử dụng kênh TLS dành cho người dùng đầu cuối và quản trị viên khi muốn kết nối qua kênh TLS. |
| 7 | Chuyển hướng kết nối qua sử dụng TLS | Giải pháp cung cấp tính năng cho phép quản trị viên cấu hình để áp dụng chính sách phải sử dụng kênh TLS đối với mọi kết nối truy cập vào giao diện cổng thông tin trên và dùng các phiên HTTP không mã hóa giống như là một lựa chọn dự phòng |
| 8 | Ghi log hoạt động của các hành động | Giải pháp cung cấp 03 tính năng sau:1. Ghi log hoạt động của các hành động thực hiện trên tất cả các thành phần.2. Cho phép quản trị viên xem xét, kiểm tra log thu được thông qua thành phần báo cáo.3. Chuyển log thu thập được cho bên thứ ba cung cấp giải pháp bảo mật để xem xét, kiểm tra kỹ hơn. |
| 9 | Tách biệt máy ảo với phần mềm giám sát máy ảo | Giải pháp cung cấp tính năng đảm bảo máy ảo được giám sát bởi một phần mềm giám sát máy ảo không gây ảnh hưởng đến phần mềm giám sát đó. |
| 10 | Phân quyền cho máy ảo truy cập đến tài nguyên | Giải pháp cung cấp tính năng đảm bảo phần mềm giám sát máy ảo phân quyền cho máy ảo mà nó giám sát truy cập đến tài nguyên đúng theo chính sách quản trị nền tảng. |
| 11 | Cấu hình cho phần mềm giám sát máy ảo | Giải pháp cung cấp tính năng cho phép quản trị viên cấu hình cho phần mềm giám sát máy ảo và kiểm tra được tính hợp lệ của cấu hình phần mềm giám sát máy ảo. |
| 12 | Bảo vệ dữ liệu | Giải pháp cung cấp tính năng phòng chống việc mất mát, rò rỉ, thay đổi dữ liệu trong cả quá trình lưu trữ trên các bộ nhớ dùng chung và truyền tin qua các mạng chia sẻ. |
| 13 | Tách biệt các máy ảo với nhau | Giải pháp cung cấp tính năng tách biệt hoàn toàn các máy ảo với nhau về logic. |
| 14 | Đảm bảo các API của hệ thống có ít nhất 02 mức quyền truy cập đã định nghĩa sẵn cho các API của client | Giải pháp cung cấp 02 tính năng sau:1. Đảm bảo các chức năng quản trị và vận hành của hệ thống định nghĩa sẵn ít nhất 02 mức quyền truy cập cho các API của client (ví dụ: quyền root và quyền user, trong đó quyền root cao hơn quyền user).2. Đảm bảo các chức năng quản trị và vận hành của hệ thống xác thực được client dựa trên các tiêu chí được định nghĩa trước bởi quản trị viên. |

2.2. Yêu cầu thiết lập cấu hình bảo mật cho hạ tầng điện toán đám mây

Bảng dưới đây mô tả yêu cầu đối với việc thiết lập cấu hình bảo mật cho hạ tầng điện toán đám mây. Việc thiết lập cấu hình như dưới đây là yêu cầu áp dụng.

Các yêu cầu được đánh giá là “Đạt” khi việc thiết lập cấu hình như được mô tả (nội dung Mô tả tiêu chí) hoặc được thiết lập ở mức bảo mật cao hơn. Đánh giá là “Không đạt” việc thiết lập cấu hình ở mức thấp hơn tiêu chí được mô tả.

Nội dung mô tả tiêu chí ở bảng dưới đây trên cơ sở tham khảo thiết lập cấu hình bảo mật trên nền tảng OpenStack, cơ quan, tổ chức khi thực hiện đánh giá với nền tảng khác thì thực hiện tương tự như với nền tảng OpenStack.

| **STT** | **Tính năng** | **Tiêu chí, chỉ tiêu kỹ thuật** |
| --- | --- | --- |
| **I** | **Dịch vụ xác thực** |
| 1 | Cấp quyền sở hữu phù hợp cho các tệp tin cấu hình dịch vụ xác thực | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. Tệp tin /etc/keystone/keystone.conf được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone.2. Tệp tin /etc/keystone/keystone-paste.ini được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone.3. Tệp tin /etc/keystone/policy.json được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone.4. Tệp tin /etc/keystone/logging.conf được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone.5. Tệp tin /etc/keystone/tls/certs/signing\_cert.pem được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone.6. Tệp tin /etc/keystone/tls/private/signing\_key.pem được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone.7. Tệp tin /etc/keystone/tls/certs/ca.pem được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone.8. Thư mục /etc/keystone/ được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone |
| 2 | Cấp quyền truy cập phù hợp cho các tệp tin cấu hình dịch vụ xác thực  | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. Tệp tin /etc/keystone/keystone.conf được gán quyền truy cập tối thiểu là 640.2. Tệp tin /etc/keystone/keystone-paste.ini được gán quyền truy cập tối thiểu là 640.3. Tệp tin /etc/keystone/policy.json được gán quyền truy cập tối thiểu là 640.4. Tệp tin /etc/keystone/logging.conf được gán quyền truy cập tối thiểu là 640.5. Tệp tin /etc/keystone/tls/certs/signing\_cert.pem được gán quyền truy cập tối thiểu là 640.6. Tệp tin /etc/keystone/tls/private/signing\_key.pem được gán quyền truy cập tối thiểu là 640.7. Tệp tin /etc/keystone/tls/certs/ca.pem được gán quyền truy cập tối thiểu là 640.8. Thư mục /etc/keystone/ được gán quyền truy cập tối thiểu là 750. |
| 3 | Kích hoạt kênh TLS trên máy chủ cung cấp dịch vụ xác thực | Cho phép người quản trị kết nối, quản trị với nền tảng điện toán đám mây thông qua kết nối bảo mật TLS |
| 4 | Sử dụng hàm băm mạnh cho các token tạo bởi hạ tầng khóa công khai PKI (Public Key Infrastructure) của dịch vụ xác thực | Tham số thiết lập cho tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số hash\_algorithm ở phần [token] trong tệp tin /etc/keystone/keystone.conf được gán giá trị là SHA256. |
| 5 | Phòng chống tấn công DoS (Denial-of-Service) | Tham số thiết lập cho tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số max\_request\_body\_size trong tệp tin /etc/ keystone/keystone.conf được gán giá trị là 114688 (theo mặc định) hoặc được gán một giá trị hợp lý và phù hợp với môi trường triển khai thực tế. |
| 6 | Phòng chống lợi dụng token admin để chiếm quyền quản trị | Tham số thiết lập cho tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:1. Tham số admin\_token ở phần [DEFAULT] trong tệp tin /etc/keystone/keystone.conf được vô hiệu hóa (được gán giá trị rỗng).2. Tham số AdminTokenAuthMiddleware ở phần [filter:admin\_token\_auth] trong tệp tin /etc/keystone /keystone-paste.ini được xóa đi. |
| 7 | Ẩn những thông tin nhạy cảm trong quá trình xác thực | Tham số thiết lập cho tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số insecure\_debug ở phần [DEFAULT] trong tệp tin /etc/keystone/keystone.conf được gán giá trị là False. |
| 8 | Thiết lập cơ chế đảm bảo an toàn cho quá trình sinh token | Tham số thiết lập cho tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số provider ở phần [token] trong tệp tin /etc/ keystone/keystone.conf được gán giá trị là fernet. |
| **II** | **Dịch vụ quản trị giao diện dashboard** |
| 1 | Cấp quyền sở hữu phù hợp cho các tệp tin cấu hình dịch vụ dashboard | Tham số thiết lập cho tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tệp tin /etc/openstack-dashboard/local\_settings.py được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là horizon. |
| 2 | Cấp quyền truy cập phù hợp cho các tệp tin cấu hình dịch vụ dashboard | Tham số thiết lập cho tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tệp tin /etc/openstack-dashboard/local\_settings.py được gán quyền truy cập tối thiểu là 640. |
| 3 | Phòng chống tấn công XFS (Cross-Frame Scripting) | Tham số thiết lập cho tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số DISALLOW\_IFRAME\_EMBED trong tệp tin /etc/openstack-dashboard/local\_settings.py được gán giá trị là True. |
| 4 | Phòng chống tấn công CSRF (Cross-Site Request Forgery) | Tham số thiết lập cho tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số CSRF\_COOKIE\_SECURE trong tệp tin /etc/openstack-dashboard/local\_settings.py được gán giá trị là True. |
| 5 | Phòng chống lấy cắp session ID thông qua tấn công MitM (Man-in-the-Middle) | Tham số thiết lập cho tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số SESSION\_COOKIE\_SECURE trong tệp tin /etc/openstack-dashboard/local\_settings.py được gán giá trị là True. |
| 6 | Phòng chống lấy cắp session ID thông qua tấn công XSS (Cross-Site Scripting) | Tham số thiết lập cho tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số SESSION\_COOKIE\_HTTPONLY trong tệp tin /etc/openstack-dashboard/local\_settings.py được gán giá trị là True. |
| 7 | Vô hiệu hóa tính năng tự động điền mật khẩu | Tham số thiết lập cho tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số PASSWORD\_AUTOCOMPLETE trong tệp tin /etc/openstack-dashboard/local\_settings.py được gán giá trị là False. |
| 8 | Vô hiệu hóa tính năng hiển thị bản rõ của mật khẩu | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số DISABLE\_PASSWORD\_REVEAL trong tệp tin /etc/openstack-dashboard/local\_settings.py được gán giá trị là True. |
| 9 | Thiết lập cơ chế chỉ cho phép quản trị viên thay đổi mật khẩu | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số ENFORCE\_PASSWORD\_CHECK trong tệp tin /etc/openstack-dashboard/local\_settings.py được gán giá trị là True. |
| 10 | Định nghĩa biểu thức chính quy kiểm tra mật khẩu | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số PASSWORD\_VALIDATOR trong tệp tin /etc/openstack-dashboard/local\_settings.py được gán giá trị khác với giá trị mặc định là "regex": '.\*'. |
| 11 | Định nghĩa giá trị cho header X-Forwarded-Proto đối với các kết nối đến dịch vụ dashboard qua proxy và kênh TLS | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số SECURE\_PROXY\_TLS\_HEADER trong tệp tin /etc/openstack-dashboard/local\_settings.py được gán hai giá trị là 'HTTP\_X\_FORWARDED\_ PROTO', 'https'. |
| **III** | **Dịch vụ tính toán** |
| 1 | Cấp quyền sở hữu phù hợp cho các tệp tin cấu hình dịch vụ tính toán | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. Tệp tin /etc/nova/nova.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là nova.2. Tệp tin /etc/nova/api-paste.ini được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là nova.3. Tệp tin /etc/nova/policy.json được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là nova.4. Tệp tin /etc/nova/rootwrap.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là nova.5. Thư mục /etc/nova/ được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là nova. |
| 2 | Cấp quyền truy cập phù hợp cho các tệp tin cấu hình dịch vụ tính toán  | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. Tệp tin /etc/nova/nova.conf được gán quyền truy cập tối thiểu là 640.2. Tệp tin /etc/nova/api-paste.ini được gán quyền truy cập tối thiểu là 640.3. Tệp tin /etc/nova/policy.json được gán quyền truy cập tối thiểu là 640.4. Tệp tin /etc/nova/rootwrap.conf được gán quyền truy cập tối thiểu là 640.5. Thư mục /etc/nova/ được gán quyền truy cập tối thiểu là 750. |
| 3 | Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ tính toán | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số auth\_strategy trong tệp tin /etc/nova/nova. conf được gán giá trị là keystone. |
| 4 | Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ tính toán | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:1. Tham số www\_authenticate\_uri ở phần [keystone\_ authtoken] trong tệp tin /etc/nova/nova.conf được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ keystone bắt đầu với xâu https://.2. Tham số insecure ở phần [keystone\_authtoken] trong tệp tin /etc/nova/nova.conf được gán giá trị là False. |
| 5 | Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ tính toán và dịch vụ quản lý máy chủ ảo | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:1. Tham số api\_máy chủ ở phần [glance] trong tệp tin /etc/nova/nova.conf được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ glance bắt đầu với xâu https://.2. Tham số api\_insecure ở phần [glance] trong tệp tin /etc/nova/nova.conf được gán giá trị là False. |
| **IV** | **Dịch vụ lưu trữ** |
| 1 | Cấp quyền sở hữu phù hợp cho các tệp tin cấu hình dịch vụ lưu trữ | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. Tệp tin /etc/cinder/cinder.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là cinder.2. Tệp tin /etc/cinder/api-paste.ini được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là cinder.3. Tệp tin /etc/cinder/policy.json được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là cinder.4. Tệp tin /etc/cinder/rootwrap.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là cinder.5. Thư mục /etc/cinder/ được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là cinder. |
| 2 | Cấp quyền truy cập phù hợp cho các tệp tin cấu hình dịch vụ lưu trữ  | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. Tệp tin /etc/cinder/cinder.conf được gán quyền truy cập tối thiểu là 640.2. Tệp tin /etc/cinder/api-paste.ini được gán quyền truy cập tối thiểu là 640.3. Tệp tin /etc/cinder/policy.json được gán quyền truy cập tối thiểu là 640.4. Tệp tin /etc/cinder/rootwrap.conf được gán quyền truy cập tối thiểu là 640.5. Thư mục /etc/cinder/ được gán quyền truy cập tối thiểu là 750. |
| 3 | Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ lưu trữ | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số auth\_strategy trong tệp tin /etc/cinder/ cinder.conf được gán giá trị là keystone. |
| 4 | Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ lưu trữ | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:1. Tham số www\_authenticate\_uri ở phần [keystone\_ authtoken] trong tệp tin /etc/ cinder/cinder.conf được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ keystone bắt đầu với xâu https://.2. Tham số insecure ở phần [keystone\_authtoken] trong tệp tin /etc/cinder/cinder.conf được gán giá trị là False. |
| 5 | Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ lưu trữ và dịch vụ tính toán | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số nova\_api\_insecure ở phần [DEFAULT] trong tệp tin /etc/cinder/cinder.conf được gán giá trị là False. |
| 6 | Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ lưu trữ và dịch vụ quản lý máy chủ ảo | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:1. Tham số glance\_api\_máy chủ ở phần [glance] trong tệp tin /etc/cinder/cinder.conf được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ glance bắt đầu với xâu https://.2. Tham số glance\_api\_insecure ở phần [glance] trong tệp tin /etc/cinder/cinder.conf được gán giá trị là False. |
| 7 | Thiết lập cơ chế đảm bảo an toàn vận hành các thiết bị NAS (Network -Attached Storage) | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:1. Tham số nas\_secure\_file\_permissions ở phần [DEFAULT] trong tệp tin /etc/cinder/cinder.conf được gán giá trị là auto.2. Tham số nas\_secure\_file\_operations ở phần [DEFAULT] trong tệp tin /etc/cinder/cinder.conf được gán giá trị là auto. |
| 8 | Phòng chống tấn công DoS (Denial-of-Service) | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số max\_request\_body\_size ở phần [oslo\_ middleware] trong tệp tin /etc/cinder/cinder.conf được gán giá trị là 114688. |
| 9 | Kích hoạt tính năng mã hóa volume | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:1. Tham số backend ở phần [key\_manager] trong tệp tin /etc/cinder/cinder.conf được gán giá trị.2. Tham số backend ở phần [key\_manager] trong tệp tin /etc/nova/nova.conf được gán giá trị. |
| **V** | **Dịch vụ quản lý máy chủ ảo** |
| 1 | Cấp quyền sở hữu phù hợp cho các tệp tin cấu hình dịch vụ quản lý máy chủ ảo | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. Tệp tin /etc/glance/glance-api-paste.ini được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là glance.2. Tệp tin /etc/glance/glance-api.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là glance.3. Tệp tin /etc/glance/glance-cache.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là glance.4. Tệp tin /etc/glance/glance-manage.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là glance.5. Tệp tin /etc/glance/glance-registry-paste.ini được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là glance.6. Tệp tin /etc/glance/glance-registry.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là glance.7. Tệp tin /etc/glance/glance-scrubber.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là glance.8. Tệp tin /etc/glance/glance-swift-store. conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là glance.9. Tệp tin /etc/glance/policy.json được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là glance.10. Tệp tin /etc/glance/schema-image.json được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là glance.11. Tệp tin /etc/glance/schema.json được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là glance.12. Thư mục /etc/glance/ được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là glance. |
| 2 | Cấp quyền truy cập phù hợp cho các tệp tin cấu hình dịch vụ quản lý máy chủ ảo  | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. Tệp tin /etc/glance/glance-api-paste.ini được gán quyền truy cập tối thiểu là 640.2. Tệp tin /etc/glance/glance-api.conf được gán quyền truy cập tối thiểu là 640.3. Tệp tin /etc/glance/glance-cache.conf được gán quyền truy cập tối thiểu là 640.4. Tệp tin /etc/glance/glance-manage.conf được gán quyền truy cập tối thiểu là 640.5. Tệp tin /etc/glance/glance-registry-paste.ini được gán quyền truy cập tối thiểu là 640.6. Tệp tin /etc/glance/glance-registry.conf được gán quyền truy cập tối thiểu là 640.7. Tệp tin /etc/glance/glance-scrubber.conf được gán quyền truy cập tối thiểu là 640.8. Tệp tin /etc/glance/glance-swift-store.conf được gán quyền truy cập tối thiểu là 640.9. Tệp tin /etc/glance/policy.json được gán quyền truy cập tối thiểu là 640.10. Tệp tin /etc/glance/schema-image.json được gán quyền truy cập tối thiểu là 640.11. Tệp tin /etc/glance/schema.json được gán quyền truy cập tối thiểu là 640.12. Thư mục /etc/glance/ được gán quyền truy cập tối thiểu là 750. |
| 3 | Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ quản lý máy chủ ảo | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:1. Tham số auth\_strategy ở phần [DEFAULT] trong tệp tin /etc/glance/glance-api.conf được gán giá trị là keystone.2. Tham số auth\_strategy ở phần [DEFAULT] trong tệp tin /etc/glance/glance-registry.conf được gán giá trị là keystone. |
| 4 | Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ quản lý máy chủ ảo | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:1. Tham số www\_authenticate\_uri ở phần [keystone\_ authtoken] trong tệp tin /etc/glance/glanceregistry. conf được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ keystone bắt đầu với xâu https://.2. Tham số insecure ở phần [keystone\_authtoken] trong tệp tin /etc/glance/glance-registry.conf được gán giá trị là False. |
| 5 | Phòng chống tấn công quét thăm dò port | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số copy\_from trong tệp tin /etc/glance/policy. json được gán giá trị (ví dụ: role:admin). |
| **VI** | **Dịch vụ chia sẻ lưu trữ** |
| 1 | Cấp quyền sở hữu phù hợp cho các tệp tin cấu hình dịch vụ chia sẻ lưu trữ | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. Tệp tin /etc/manila/manila.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là manila.2. Tệp tin /etc/manila/api-paste.ini được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là manila.3. Tệp tin /etc/manila/policy.json được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là manila.4. Tệp tin /etc/manila/rootwrap.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là manila.5. Thư mục /etc/manila/ được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là manila. |
| 2 | Cấp quyền truy cập phù hợp cho các tệp tin cấu hình dịch vụ chia sẻ lưu trữ  | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. Tệp tin /etc/manila/manila.conf được gán quyền truy cập tối thiểu là 640.2. Tệp tin /etc/manila/api-paste.ini được gán quyền truy cập tối thiểu là 640.3. Tệp tin /etc/manila/policy.json được gán quyền truy cập tối thiểu là 640.4. Tệp tin /etc/manila/rootwrap.conf được gán quyền truy cập tối thiểu là 640.5. Thư mục /etc/manila/ được gán quyền truy cập tối thiểu là 750. |
| 3 | Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ chia sẻ lưu trữ | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số auth\_strategy ở phần [DEFAULT] trong tệp tin /etc/manila/manila.conf được gán giá trị là keystone. |
| 4 | Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ chia sẻ lưu trữ | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:1. Tham số identity\_uri ở phần [keystone\_authtoken] trong tệp tin /etc/manila/manila.conf được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ keystone bắt đầu với xâu https://.2. Tham số insecure ở phần [keystone\_authtoken] trong tệp tin /etc/manila/manila.conf được gán giá trị là False. |
| 5 | Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ chia sẻ lưu trữ và dịch vụ tính toán | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số nova\_api\_insecure ở phần [DEFAULT] trong tệp tin /etc/manila/manila.conf được gán giá trị là False. |
| 6 | Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ chia sẻ lưu trữ và dịch vụ quản lý mạng | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số neutron\_api\_insecure ở phần [DEFAULT] trong tệp tin /etc/manila/manila.conf được gán giá trị là False. |
| 7 | Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ chia sẻ lưu trữ và dịch vụ lưu trữ | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số cinder\_api\_insecure ở phần [DEFAULT] trong tệp tin /etc/manila/manila.conf được gán giá trị là False. |
| 8 | Phòng chống tấn công DoS (Denial-of-Service) | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số max\_request\_body\_size ở phần [oslo\_ middleware] trong tệp tin /etc/manila/manila.conf được gán giá trị là 114688. |
| **VII** | **Dich vụ quản lý mạng (networking)** |
| 1 | Cấp quyền sở hữu phù hợp cho các tệp tin cấu hình dịch vụ quản lý mạng | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. Tệp tin /etc/neutron/neutron.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là neutron.2. Tệp tin /etc/neutron/api-paste.ini được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là neutron.3. Tệp tin /etc/neutron/policy.json được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là neutron.4. Tệp tin /etc/neutron/rootwrap.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là neutron.5. Thư mục /etc/neutron/ được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là neutron. |
| 2 | Cấp quyền truy cập phù hợp cho các tệp tin cấu hình dịch vụ quản lý mạng  | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. Tệp tin /etc/neutron/neutron.conf được gán quyền truy cập tối thiểu là 640.2. Tệp tin /etc/neutron/api-paste.ini được gán quyền truy cập tối thiểu là 640.3. Tệp tin /etc/neutron/policy.json được gán quyền truy cập tối thiểu là 640.4. Tệp tin /etc/neutron/rootwrap.conf được gán quyền truy cập tối thiểu là 640.5. Thư mục /etc/neutron/ được gán quyền truy cập tối thiểu là 750. |
| 3 | Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ quản lý mạng | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số auth\_strategy ở phần [DEFAULT] trong tệp tin /etc/neutron/neutron.conf được gán giá trị là keystone. |
| 4 | Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ quản lý mạng | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:1. Tham số www\_authenticate\_uri ở phần [keystone\_ authtoken] trong tệp tin /etc/neutron/neutron.conf được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ keystone bắt đầu với xâu https://.2. Tham số insecure ở phần [keystone\_authtoken] trong tệp tin /etc/neutron/neutron.conf được gán giá trị là False. |
| 5 | Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ quản lý mạng và các đối tượng khác | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số use\_tls ở phần [DEFAULT] trong tệp tin /etc/neutron/neutron.conf được gán giá trị là True. |
| **VIII** | **Dịch vụ quản lý thông tin mật** |
| 1 | Cấp quyền sở hữu phù hợp cho các tệp tin cấu hình dịch vụ quản lý thông tin mật | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. File /etc/barbican/barbican.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là barbican.2. File /etc/barbican/barbican-api-paste.ini được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là barbican.3. File /etc/barbican/policy.json được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là barbican.4. Directory /etc/barbican/ được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là barbican. |
| 2 | Cấp quyền truy cập phù hợp cho các tệp tin cấu hình dịch vụ quản lý thông tin mật | Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:1. File /etc/barbican/barbican.conf được gán quyền truy cập tối thiểu là 640.2. File /etc/barbican/barbican-api-paste.ini được gán quyền truy cập tối thiểu là 640.3. File /etc/barbican/policy.json được gán quyền truy cập tối thiểu là 640.4. Directory /etc/barbican/ được gán quyền truy cập tối thiểu là 750. |
| 3 | Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ quản lý thông tin mật | Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:- Tham số auth\_strategy được liệt kê ở phần [pipeline:barbican-api-keystone] trong file /etc/ barbican/barbican-api-paste.ini. |
| 4 | Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ quản lý thông tin mật | Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:1. Tham số identity\_uri ở phần [keystone\_authtoken] trong file /etc/barbican/barbican.conf được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ keystone bắt đầu với xâu https://.2. Tham số insecure ở phần [keystone\_authtoken] trong file /etc/barbican/barbican.conf được gán giá trị là False. |