

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

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.

1. YÊU CẦU CƠ BẢN VỀ TÍNH NĂNG AN TOÀN THÔNG TIN

Tên tính năng	Tiêu chí, chỉ tiêu kỹ thuật
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.
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.
Tích hợp điều khiển truy cập dựa trên vai trò - RBAC (Role-Based Access Control)	<p>Giải pháp cung cấp 03 tính năng sau:</p> <p>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).</p> <p>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.</p> <p>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.</p>

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

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.
Hỗ trợ TLS tự kí (Self-signed TLS)	Giải pháp cung cấp 02 tính năng sau: Cho phép quản trị viên tạo các chứng thư điện tử tự kí (Self-signed) TLS để đẩy nhanh quá trình triển khai. Cho phép các chứng thư điện tử được tạo bởi một đơn vị cấp chứng thư (CA) tin cậy (trusted certificate authority).
Tích hợp giao diện công thông tin quản trị hỗ trợ sử dụng kênh TLS	Giải pháp cung cấp tính năng tích hợp giao diện công 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.
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 công thông tin trên và dùng các phiên HTTP không mã hóa giống như là một lựa chọn dự phòng
Ghi log hoạt động của các hành động	Giải pháp cung cấp 03 tính năng sau: Ghi log hoạt động của các hành động thực hiện trên tất cả các thành phần. Cho phép quản trị viên xem xét, kiểm tra log thu được thông qua thành phần báo cáo. Chuyển log thu thập được cho bên thứ ba cung cấp giải pháp bảo mật để xem xét, kiểm tra kỹ hơn.
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.
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.
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

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

	được tính hợp lệ của cấu hình phần mềm giám sát máy ảo.
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.
Tách biệt các máy ảo với nhau	Giải pháp cung cấp tính năng tách biệt hoàn toàn các máy ảo với nhau về logic.
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: 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). 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. 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.

Tính năng	Tiêu chí, chỉ tiêu kỹ thuật
Dịch vụ xác thực	
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: Tệp tin /etc/keystone/keystone.conf được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone.

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

	<p>Tệp tin /etc/keystone/keystone-paste.ini được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone.</p> <p>Tệp tin /etc/keystone/policy.json được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone.</p> <p>Tệp tin /etc/keystone/logging.conf được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone.</p> <p>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.</p> <p>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.</p> <p>Tệp tin /etc/keystone/tls/certs/ca.pem được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone.</p> <p>Thư mục /etc/keystone/ được gán quyền sở hữu cho tài khoản là keystone và nhóm tài khoản là keystone</p>
Cấp quyền truy cập phù hợp cho các tệp tin cấu hình dịch vụ xác thực	<p>Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:</p> <p>Tệp tin /etc/keystone/keystone.conf được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin /etc/keystone/keystone-paste.ini được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin /etc/keystone/policy.json được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin /etc/keystone/logging.conf được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin /etc/keystone/tls/certs/signing_cert.pem được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin /etc/keystone/tls/private/signing_key.pem được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin /etc/keystone/tls/certs/ca.pem được gán quyền truy cập tối thiểu là 640.</p>

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

	Thư mục /etc/keystone/ được gán quyền truy cập tối thiểu là 750.
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
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.
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.
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: Tham số admin_token ở phần [DEFAULT] trong tệp tin /etc/keystone/keystone.conf được vô hiệu hóa (được gán giá trị rỗng). Tham số AdminTokenAuthMiddleware ở phần [filter:admin_token_auth] trong tệp tin /etc/keystone/keystone-paste.ini được xóa đi.
Ấn 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.
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:

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

	- Tham số provider ở phần [token] trong tệp tin /etc/keystone/keystone.conf được gán giá trị là fernet.
Dịch vụ quản trị giao diện dashboard	
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.
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.
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.
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.
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.
Phòng chống lấy cắp session ID thông qua	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:

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

tấn công XSS (Cross-Site Scripting)	Tham số SESSION_COOKIE_HTTPONLY trong tệp tin /etc/openstack-dashboard/local_settings.py được gán giá trị là True.
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.
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.
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.
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": '.*'.
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'.
Dịch vụ tính toán	
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:

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

	<p>Tệp tin <code>/etc/nova/nova.conf</code> được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là nova.</p> <p>Tệp tin <code>/etc/nova/api-paste.ini</code> được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là nova.</p> <p>Tệp tin <code>/etc/nova/policy.json</code> được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là nova.</p> <p>Tệp tin <code>/etc/nova/rootwrap.conf</code> được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là nova.</p> <p>Thư mục <code>/etc/nova/</code> được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là nova.</p>
Cấp quyền truy cập phù hợp cho các tệp tin cấu hình dịch vụ tính toán	<p>Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:</p> <p>Tệp tin <code>/etc/nova/nova.conf</code> được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin <code>/etc/nova/api-paste.ini</code> được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin <code>/etc/nova/policy.json</code> được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin <code>/etc/nova/rootwrap.conf</code> được gán quyền truy cập tối thiểu là 640.</p> <p>Thư mục <code>/etc/nova/</code> được gán quyền truy cập tối thiểu là 750.</p>
Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ tính toán	<p>Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <ul style="list-style-type: none"> - Tham số <code>auth_strategy</code> trong tệp tin <code>/etc/nova/nova.conf</code> được gán giá trị là <code>keystone</code>.
Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ tính toán	<p>Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <p>Tham số <code>www_authenticate_uri</code> ở phần <code>[keystone_authtoken]</code> trong tệp tin <code>/etc/nova/nova.conf</code> được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ keystone bắt đầu với xâu <code>https://</code>.</p> <p>Tham số <code>insecure</code> ở phần <code>[keystone_authtoken]</code> trong tệp tin <code>/etc/nova/nova.conf</code> được gán giá trị là <code>False</code>.</p>

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ tính toán và dịch vụ quản lý máy chủ ảo	<p>Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <p>Tham số <code>api_</code> máy chủ ở phần [glance] trong tệp tin <code>/etc/nova/nova.conf</code> được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ glance bắt đầu với xâu <code>https://</code>.</p> <p>Tham số <code>api_insecure</code> ở phần [glance] trong tệp tin <code>/etc/nova/nova.conf</code> được gán giá trị là <code>False</code>.</p>
Dịch vụ lưu trữ	
Cấp quyền sở hữu phù hợp cho các tệp tin cấu hình dịch vụ lưu trữ	<p>Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:</p> <p>Tệp tin <code>/etc/cinder/cinder.conf</code> được gán quyền sở hữu cho tài khoản là <code>root</code> và nhóm tài khoản là <code>cinder</code>.</p> <p>Tệp tin <code>/etc/cinder/api-paste.ini</code> được gán quyền sở hữu cho tài khoản là <code>root</code> và nhóm tài khoản là <code>cinder</code>.</p> <p>Tệp tin <code>/etc/cinder/policy.json</code> được gán quyền sở hữu cho tài khoản là <code>root</code> và nhóm tài khoản là <code>cinder</code>.</p> <p>Tệp tin <code>/etc/cinder/rootwrap.conf</code> được gán quyền sở hữu cho tài khoản là <code>root</code> và nhóm tài khoản là <code>cinder</code>.</p> <p>Thư mục <code>/etc/cinder/</code> được gán quyền sở hữu cho tài khoản là <code>root</code> và nhóm tài khoản là <code>cinder</code>.</p>
Cấp quyền truy cập phù hợp cho các tệp tin cấu hình dịch vụ lưu trữ	<p>Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:</p> <p>Tệp tin <code>/etc/cinder/cinder.conf</code> được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin <code>/etc/cinder/api-paste.ini</code> được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin <code>/etc/cinder/policy.json</code> được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin <code>/etc/cinder/rootwrap.conf</code> được gán quyền truy cập tối thiểu là 640.</p> <p>Thư mục <code>/etc/cinder/</code> được gán quyền truy cập tối thiểu là 750.</p>

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ lưu trữ	<p>Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <ul style="list-style-type: none"> - Tham số <code>auth_strategy</code> trong tệp tin <code>/etc/cinder/cinder.conf</code> được gán giá trị là <code>keystone</code>.
Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ lưu trữ	<p>Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <p>Tham số <code>www_authenticate_uri</code> ở phần <code>[keystone_authtoken]</code> trong tệp tin <code>/etc/cinder/cinder.conf</code> được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ keystone bắt đầu với xâu <code>https://</code>.</p> <p>Tham số <code>insecure</code> ở phần <code>[keystone_authtoken]</code> trong tệp tin <code>/etc/cinder/cinder.conf</code> được gán giá trị là <code>False</code>.</p>
Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ lưu trữ và dịch vụ tính toán	<p>Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <ul style="list-style-type: none"> - Tham số <code>nova_api_insecure</code> ở phần <code>[DEFAULT]</code> trong tệp tin <code>/etc/cinder/cinder.conf</code> được gán giá trị là <code>False</code>.
Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ lưu trữ và dịch vụ quản lý máy chủ ảo	<p>Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <p>Tham số <code>glance_api_máy chủ</code> ở phần <code>[glance]</code> trong tệp tin <code>/etc/cinder/cinder.conf</code> được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ glance bắt đầu với xâu <code>https://</code>.</p> <p>Tham số <code>glance_api_insecure</code> ở phần <code>[glance]</code> trong tệp tin <code>/etc/cinder/cinder.conf</code> được gán giá trị là <code>False</code>.</p>
Thiết lập cơ chế đảm bảo an toàn vận hành các thiết bị NAS (Network - Attached Storage)	<p>Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <p>Tham số <code>nas_secure_file_permissions</code> ở phần <code>[DEFAULT]</code> trong tệp tin <code>/etc/cinder/cinder.conf</code> được gán giá trị là <code>auto</code>.</p> <p>Tham số <code>nas_secure_file_operations</code> ở phần <code>[DEFAULT]</code> trong tệp tin <code>/etc/cinder/cinder.conf</code> được gán giá trị là <code>auto</code>.</p>
	Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

Phòng chống tấn công DoS (Denial- of- Service)	- Tham số max_request_body_size ở phần [oslo_ middleware] trong tệp tin /etc/cinder/cinder.conf được gán giá trị là 114688.
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: Tham số backend ở phần [key_manager] trong tệp tin /etc/cinder/cinder.conf được gán giá trị. Tham số backend ở phần [key_manager] trong tệp tin /etc/nova/nova.conf được gán giá trị.
Dịch vụ quản lý máy chủ ảo	
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 truy cập tối thiểu là 640. Tệp tin /etc/glance/glance-api.conf được gán quyền truy cập tối thiểu là 640. Tệp tin /etc/glance/glance-cache.conf được gán quyền truy cập tối thiểu là 640. Tệp tin /etc/glance/glance-manage.conf được gán quyền truy cập tối thiểu là 640. Tệp tin /etc/glance/glance-registry-paste.ini được gán quyền truy cập tối thiểu là 640. Tệp tin /etc/glance/glance-registry.conf được gán quyền truy cập tối thiểu là 640. Tệp tin /etc/glance/glance-scrubber.conf được gán quyền truy cập tối thiểu là 640. Tệp tin /etc/glance/glance-swift-store.conf được gán quyền truy cập tối thiểu là 640. Tệp tin /etc/glance/policy.json được gán quyền truy cập tối thiểu là 640. Tệp tin /etc/glance/schema-image.json được gán quyền truy cập tối thiểu là 640. Tệp tin /etc/glance/schema.json được gán quyền truy cập tối thiểu là 640.

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

	12. Thư mục /etc/glance/ được gán quyền truy cập tối thiểu là 750.
Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ quản lý máy chủ ảo	<p>Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <p>Tham số auth_strategy ở phần [DEFAULT] trong tệp tin /etc/glance/glance-api.conf được gán giá trị là keystone.</p> <p>Tham số auth_strategy ở phần [DEFAULT] trong tệp tin /etc/glance/glance-registry.conf được gán giá trị là keystone.</p>
Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ quản lý máy chủ ảo	<p>Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <p>Tham số www_authenticate_uri ở phần [keystone_authtoken] trong tệp tin /etc/glance/glance-registry.conf được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ keystone bắt đầu với xâu https://.</p> <p>Tham số insecure ở phần [keystone_authtoken] trong tệp tin /etc/glance/glance-registry.conf được gán giá trị là False.</p>
Phòng chống tấn công quét thăm dò port	<p>Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <p>- Tham số copy_from trong tệp tin /etc/glance/policy.json được gán giá trị (ví dụ: role:admin).</p>
Dịch vụ chia sẻ lưu trữ	
Cấp quyền sở hữu phù hợp cho các tệp tin cấu hình dịch vụ chia sẻ lưu trữ	<p>Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:</p> <p>Tệp tin /etc/manila/manila.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là manila.</p> <p>Tệp tin /etc/manila/api-paste.ini được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là manila.</p> <p>Tệp tin /etc/manila/policy.json được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là manila.</p> <p>Tệp tin /etc/manila/rootwrap.conf được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là manila.</p> <p>Thư mục /etc/manila/ được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là manila.</p>

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

Cấp quyền truy cập phù hợp cho các tệp tin cấu hình dịch vụ chia sẻ lưu trữ	<p>Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:</p> <p>Tệp tin /etc/manila/manila.conf được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin /etc/manila/api-paste.ini được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin /etc/manila/policy.json được gán quyền truy cập tối thiểu là 640.</p> <p>Tệp tin /etc/manila/rootwrap.conf được gán quyền truy cập tối thiểu là 640.</p> <p>Thư mục /etc/manila/ được gán quyền truy cập tối thiểu là 750.</p>
Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ chia sẻ lưu trữ	<p>Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <ul style="list-style-type: none"> - Tham số auth_strategy ở phần [DEFAULT] trong tệp tin /etc/manila/manila.conf được gán giá trị là keystone.
Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ chia sẻ lưu trữ	<p>Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <p>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://.</p> <p>Tham số insecure ở phần [keystone_authtoken] trong tệp tin /etc/manila/manila.conf được gán giá trị là False.</p>
Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ chia sẻ lưu trữ và dịch vụ tính toán	<p>Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <ul style="list-style-type: none"> - Tham số nova_api_insecure ở phần [DEFAULT] trong tệp tin /etc/manila/manila.conf được gán giá trị là False.
Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ chia sẻ lưu trữ và dịch vụ quản lý mạng	<p>Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <ul style="list-style-type: none"> - Tham số neutron_api_insecure ở phần [DEFAULT] trong tệp tin /etc/manila/manila.conf được gán giá trị là False.

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

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 <code>cinder_api_insecure</code> ở phần [DEFAULT] trong tệp tin <code>/etc/manila/manila.conf</code> được gán giá trị là False.
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 <code>max_request_body_size</code> ở phần [oslo_middleware] trong tệp tin <code>/etc/manila/manila.conf</code> được gán giá trị là 114688.
Dịch vụ quản lý mạng (networking)	
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: Tệp tin <code>/etc/neutron/neutron.conf</code> được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là neutron. Tệp tin <code>/etc/neutron/api-paste.ini</code> được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là neutron. Tệp tin <code>/etc/neutron/policy.json</code> được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là neutron. Tệp tin <code>/etc/neutron/rootwrap.conf</code> được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là neutron. Thư mục <code>/etc/neutron/</code> được gán quyền sở hữu cho tài khoản là root và nhóm tài khoản là neutron.
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: Tệp tin <code>/etc/neutron/neutron.conf</code> được gán quyền truy cập tối thiểu là 640. Tệp tin <code>/etc/neutron/api-paste.ini</code> được gán quyền truy cập tối thiểu là 640. Tệp tin <code>/etc/neutron/policy.json</code> được gán quyền truy cập tối thiểu là 640. Tệp tin <code>/etc/neutron/rootwrap.conf</code> được gán quyền truy cập tối thiểu là 640. Thư mục <code>/etc/neutron/</code> được gán quyền truy cập tối thiểu là 750.

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ quản lý mạng	<p>Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <ul style="list-style-type: none"> - Tham số <code>auth_strategy</code> ở phần [DEFAULT] trong tệp tin <code>/etc/neutron/neutron.conf</code> được gán giá trị là <code>keystone</code>.
Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ quản lý mạng	<p>Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <p>Tham số <code>www_authenticate_uri</code> ở phần [keystone_authtoken] trong tệp tin <code>/etc/neutron/neutron.conf</code> được gán giá trị là đường dẫn API đầu cuối đến máy chủ cung cấp dịch vụ keystone bắt đầu với xâu <code>https://</code>.</p> <p>Tham số <code>insecure</code> ở phần [keystone_authtoken] trong tệp tin <code>/etc/neutron/neutron.conf</code> được gán giá trị là <code>False</code>.</p>
Thiết lập cơ chế giao tiếp qua kênh TLS giữa dịch vụ quản lý mạng và các đối tượng khác	<p>Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <ul style="list-style-type: none"> - Tham số <code>use_tls</code> ở phần [DEFAULT] trong tệp tin <code>/etc/neutron/neutron.conf</code> được gán giá trị là <code>True</code>.
Dịch vụ quản lý thông tin mật	
Cấp quyền sở hữu phù hợp cho các tệp tin cấu hình dịch vụ quản lý thông tin mật	<p>Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:</p> <p>File <code>/etc/barbican/barbican.conf</code> được gán quyền sở hữu cho tài khoản là <code>root</code> và nhóm tài khoản là <code>barbican</code>.</p> <p>File <code>/etc/barbican/barbican-api-paste.ini</code> được gán quyền sở hữu cho tài khoản là <code>root</code> và nhóm tài khoản là <code>barbican</code>.</p> <p>File <code>/etc/barbican/policy.json</code> được gán quyền sở hữu cho tài khoản là <code>root</code> và nhóm tài khoản là <code>barbican</code>.</p> <p>Directory <code>/etc/barbican/</code> được gán quyền sở hữu cho tài khoản là <code>root</code> và nhóm tài khoản là <code>barbican</code>.</p>
Cấp quyền truy cập phù hợp cho các tệp tin cấu hình dịch vụ quản lý thông tin mật	<p>Các tệp tin cấu hình với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) bao gồm:</p> <p>File <code>/etc/barbican/barbican.conf</code> được gán quyền truy cập tối thiểu là <code>640</code>.</p> <p>File <code>/etc/barbican/barbican-api-paste.ini</code> được gán quyền truy cập tối thiểu là <code>640</code>.</p>

	VIETTEL AI RACE	Public 606
	TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT AN TOÀN THÔNG TIN CHO HẠ TẦNG ĐIỆN TOÁN Đám Mây	Lần ban hành: 1

	<p>File /etc/barbican/policy.json được gán quyền truy cập tối thiểu là 640.</p> <p>Directory /etc/barbican/ được gán quyền truy cập tối thiểu là 750.</p>
Thiết lập cơ chế xác thực bằng dịch vụ xác thực đối với những kết nối đến dịch vụ quản lý thông tin mật	<p>Tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <ul style="list-style-type: none"> - Tham số auth_strategy được liệt kê ở phần [pipeline:barbican-api-keystone] trong file /etc/barbican/barbican-api-paste.ini.
Thiết lập cơ chế xác thực qua kênh TLS đối với những kết nối đến dịch vụ quản lý thông tin mật	<p>Các tham số được thiết lập với nền tảng OpenStack (thực hiện tương tự đối với các nền tảng khác) như sau:</p> <p>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://.</p> <p>Tham số insecure ở phần [keystone_authtoken] trong file /etc/barbican/barbican.conf được gán giá trị là False.</p>