OpenStack 진단결과 (페이지 1)

구분	진단코드	진단항목	취약도	점검결과
파일 권한 관리	OT-01	Identity 설정파일 소유권 설정	상	취약
파일 권한 관리	OT-02	Identity 설정파일 접근권한 설정	상	취약
파일 권한 관리	OT-03	Dashboard 설정파일 소유권 설정	상	N/A
파일 권한 관리	OT-04	Dashboard 설정파일 접근권한 설정	상	N/A
파일 권한 관리	OT-05	Compute 설정파일 소유권 설정	상	취약
파일 권한 관리	OT-06	Compute 설정파일 접근권한 설정	상	양호
파일 권한 관리	OT-07	블록 스토리지 서비스 설정파일 소유권 설정	상	취약
파일 권한 관리	OT-08	블록 스토리지 서비스 설정파일 접근권한 설정	상	양호
파일 권한 관리	OT-09	이미지 스토리지 설정파일 소유권 설정	상	취약
파일 권한 관리	OT-10	이미지 스토리지 설정파일 접근권한 설정	상	양호
파일 권한 관리	OT-11	공유파일 시스템 설정파일 소유권 설정	상	N/A
파일 권한 관리	OT-12	공유파일 시스템 설정파일 접근권한 설정	상	N/A
파일 권한 관리	OT-13	네트워킹 서비스 설정파일 소유권 설정	상	취약
파일 권한 관리	OT-14	네트워킹 서비스 설정파일 접근권한 설정	상	양호
암호화	OT-15	Identity TLS 활성화	상	취약
암호화	OT-16	PKI토근의 강력한 해시 알고리즘 사용	상	양호
암호화	OT-17	Dashboard의 SECURE_PROXY_SSL_HEAEDER 설정	상	N/A
암호화	OT-18	Compute 인증을 위한 보안프로토콜 사용	상	취약
암호화	OT-19	Nova와 Glance의 안전한 통신	상	취약
암호화	OT-20	블록 스토리지 서비스 인증을 위한 TLS 활성화	상	취약

OpenStack 진단결과 (페이지 2)

구분	진단코드	진단항목	취약도	점검결과
암호화	OT-21	cinder와 nova의 TLS 통신	상	취약
암호화	OT-22	cinder와 glance의 TLS 통신	상	취약
암호화	OT-23	이미지 스토리지 서비스 인증을 위한 TLS 활성화	상	취약
암호화	OT-24	공유 파일 시스템 인증을 위한 TLS 활성화	상	N/A
암호화	OT-25	TLS를 이용한 공유 파일 시스템과 Compute 통신	상	N/A
암호화	OT-26	TLS를 이용한 공유 파일 시스템과 네트워킹연결	상	N/A
암호화	OT-27	TLS를 이용한 공유 파일 시스템과 블록 스토리지 서비스와의 연결	상	N/A
암호화	OT-28	네트워킹 서비스의 인증을 위한 안전한 프로토콜 사용	상	취약
암호화	OT-29	Neutron API 서버의 TLS 활성화	상	취약
보안설정	OT-30	Identity 서비스 max_request_body_size 설정	상	양호
보안설정	OT-31	admin 토큰 비활성화	상	N/A
보안설정	OT-32	Dashboard의 DISALLOW_IFRAME_EMBED 설정	상	N/A
보안설정	OT-33	Dashboard의 CSFR_COOKIE_SECURE 설정	상	N/A
보안설정	OT-34	Dashboard의 SESSION_COOKIE_SECURE 설정	상	N/A
보안설정	OT-35	Dashboard의 SESSION_COOKIE_HTTPONLY 설정	상	N/A
보안설정	OT-36	Dashboard의 PASSWORD_AUTOCOMPLE 설정	상	N/A
보안설정	OT-37	Dashboard의 DISABLE_PASSWORD_REVEAL 설정	상	N/A
보안설정	OT-38	Dashboard의 ENFORCE_PASSWORD_CHECK 설정	상	N/A
보안설정	OT-39	Dashboard의 PASSWORD_VALIDATOR 설정	상	N/A
보안설정	OT-40	Compute의 인증을 위한 keystone 사용	상	취약

OpenStack 진단결과 (페이지 3)

구분	진단코드	진단항목	취약도	점검결과
보안설정	OT-41	블록 스토리지 서비스의 인증을 위한 keystone 사용	상	취약
보안설정	OT-42	안전한 환경에서의 NAS 운영	상	N/A
보안설정	OT-43	블록 스토리지 서비스에서 요청 본문 최대 크기 설정	상	양호
보안설정	OT-44	블록 스토리지 볼륨 암호화	상	N/A
보안설정	OT-45	이미지 스토리지 서비스 인증을 위한 keystone 설정	상	N/A
보안설정	OT-46	공유파일 시스템 인증을 위한 오픈스택 Identity 사용	상	N/A
보안설정	OT-47	공유파일 시스템에서 요청 본문 최대 사이즈 설정	상	N/A
파일 권한 관리	OT-01	Identity 설정파일 소유권 설정	상	취약
파일 권한 관리	OT-02	Identity 설정파일 접근권한 설정	상	취약
파일 권한 관리	OT-03	Dashboard 설정파일 소유권 설정	상	N/A
파일 권한 관리	OT-04	Dashboard 설정파일 접근권한 설정	상	N/A
파일 권한 관리	OT-05	Compute 설정파일 소유권 설정	상	취약
파일 권한 관리	OT-06	Compute 설정파일 접근권한 설정	상	양호
파일 권한 관리	OT-07	블록 스토리지 서비스 설정파일 소유권 설정	상	취약
파일 권한 관리	OT-08	블록 스토리지 서비스 설정파일 접근권한 설정	상	양호
파일 권한 관리	OT-09	이미지 스토리지 설정파일 소유권 설정	상	취약
파일 권한 관리	OT-10	이미지 스토리지 설정파일 접근권한 설정	상	양호
파일 권한 관리	OT-11	공유파일 시스템 설정파일 소유권 설정	상	N/A
파일 권한 관리	OT-12	공유파일 시스템 설정파일 접근권한 설정	상	N/A
파일 권한 관리	OT-13	네트워킹 서비스 설정파일 소유권 설정	상	취약
파일 권한 관리	OT-14	네트워킹 서비스 설정파일 접근권한 설정	상	양호
암호화	OT-15	Identity TLS 활성화	상	취약

OpenStack 조치사항 (페이지 1)

진단코드	진단항목	조치방법
OT-01	Identity 설정파일 소유권 설정	Identity 설정파일 소유자 소유그룹을 keystone/keystone로 변경
OT-02	Identity 설정파일 접근권한 설정	Identity 설정파일의 퍼미션을 최소 640으로 설정
OT-05	Compute 설정파일 소유권 설정	Compute 설정파일의 소유자 소유그룹을 root/nova로 변경
OT-07	블록 스토리지 서비스 설정파일 소유권 설정	블록 스토리지 서비스 설정파일의 소유자 소유그룹을 root/cinder로 변경
OT-09	이미지 스토리지 설정파일 소유권 설정	이미지 스토리지 설정파일의 소유자 소유그룹을 root/glance로 변경
OT-13	네트워킹 서비스 설정파일 소유권 설정	네트워킹 서비스 설정파일의 소유자/소유그룹을 root/netutron로 변경
OT-15	Identity TLS 활성화	SSL 설정을 활성화한 뒤에 TLS 프로토콜을 활성화
OT-18	Compute 인증을 위한 보안프로토콜 사용	/etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 시작하도록 설정 또는 /etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 insecure 설정 값을 false로 설정
OT-19	Nova와 Glance의 안전한 통신	/etc/nova/nova.conf 파일에서 [glance] 섹션의 api_servers 값을 https://로 시작하도록 설정 또는 /etc/nova/nova.conf 파일에서 [glance] 섹션의 api_insecure 값을 false로 설정
OT-20	블록 스토리지 서비스 인증을 위한 TLS 활성화	/etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 시작하도록 설정 또는 /etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 insecure 값을 false로 설정

OpenStack 조치사항 (페이지 2)

진단코드	진단항목	조치방법
OT-21	cinder와 nova의 TLS 통신	/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nova_api_insecure 설정값을 False로 설정
OT-22	cinder와 glance의 TLS 통신	/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api_insecure 값을 False로 설정 또는 /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api_servers 값을 https://로 설정
OT-23	이미지 스토리지 서비스 인증을 위한 TLS 활성화	/etc/glance/glance-api.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 설정 또는 /etc/glance/glance-api.conf 파일에서 [keystone_authtoken] 섹션의 섹션의 insecure 값을 false로 설정
OT-28	네트워킹 서비스의 인증을 위한 안전한 프로토콜 사용	/etc/neutron/neutron.conf [keystone_authtoken] 섹션의 auth_uri 값을 https://로 설정 또는 /etc/neutron/neutron.conf [keystone_authtoken] 섹션의 insecure 값을 False로 설정
OT-29	Neutron API 서버의 TLS 활성화	/etc/neutron/neutron.conf 파일에서 [DEFAULT] 섹션의 use_ssl 값을 True로 설정
OT-40	Compute의 인증을 위한 keystone 사용	/etc/nova/nova.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 값을 keystone으로 설정
OT-41	블록 스토리지 서비스의 인증을 위한 keystone 사용	/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 값을 keystone으로 설정
OT-01	Identity 설정파일 소유권 설정	Identity 설정파일 소유자 소유그룹을 keystone/keystone로 변경
OT-02	Identity 설정파일 접근권한 설정	Identity 설정파일의 퍼미션을 최소 640으로 설정
OT-05	Compute 설정파일 소유권 설정	Compute 설정파일의 소유자 소유그룹을 root/nova로 변경

OpenStack 조치사항 (페이지 3)

진단코드	진단항목	조치방법
OT-07	블록 스토리지 서비스 설정파일 소유권 설정	블록 스토리지 서비스 설정파일의 소유자 소유그룹을 root/cinder로 변경
OT-09	이미지 스토리지 설정파일 소유권 설정	이미지 스토리지 설정파일의 소유자 소유그룹을 root/glance로 변경
OT-13	네트워킹 서비스 설정파일 소유권 설정	네트워킹 서비스 설정파일의 소유자/소유그룹을 root/netutron로 변경
OT-15	Identity TLS 활성화	SSL 설정을 활성화한 뒤에 TLS 프로토콜을 활성화
OT-18	Compute 인증을 위한 보안프로토콜 사용	/etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 시작하도록 설정 또는 /etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 insecure 설정 값을 false로 설정
OT-19	Nova와 Glance의 안전한 통신	/etc/nova/nova.conf 파일에서 [glance] 섹션의 api_servers 값을 https://로 시작하도록 설정 또는 /etc/nova/nova.conf 파일에서 [glance] 섹션의 api_insecure 값을 false로 설정
OT-20	블록 스토리지 서비스 인증을 위한 TLS 활성화	/etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 시작하도록 설정 또는 /etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 insecure 값을 false로 설정
OT-21	cinder와 nova의 TLS 통신	/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nova_api_insecure 설정값을 False로 설정
OT-22	cinder와 glance의 TLS 통신	/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api_insecure 값을 False로 설정 또는 /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api_servers 값을 https://로 설정
OT-23	이미지 스토리지 서비스 인증을 위한 TLS 활성화	/etc/glance/glance-api.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 설정 또는 /etc/glance/glance-api.conf 파일에서 [keystone_authtoken] 섹션의 섹션의 insecure 값을 false로 설정

OpenStack 조치사항 (페이지 4)

진단코드	진단항목	조치방법
OT-28	네트워킹 서비스의 인증을 위한 안전한 프로토콜 사용	/etc/neutron/neutron.conf [keystone_authtoken] 섹션의 auth_uri 값을 https://로 설정 또는 /etc/neutron/neutron.conf [keystone_authtoken] 섹션의 insecure 값을 False로 설정
OT-29	Neutron API 서버의 TLS 활성화	/etc/neutron/neutron.conf 파일에서 [DEFAULT] 섹션의 use_ssl 값을 True로 설정
OT-40	Compute의 인증을 위한 keystone 사용	/etc/nova/nova.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 값을 keystone으로 설정
OT-41	블록 스토리지 서비스의 인증을 위한 keystone 사용	/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 값을 keystone으로 설정

OpenStack 취약점 진단 점검 결과